Data Center and Cloud Services Directives.

Table of Contents

1. INTRODUCTION

Data Center is a centralized dedicated place that provides the information-processing infrastructure specifically the IT and Telecommunications equipment such as servers, storage equipment and the core network infrastructure.
Considering the above critical functions of this equipment as it requires operating 24x7 with operational requirements such as cooling, ambient temperature; exceptional attention needs to be taken to ensure that the optimum environment exists for it operations.
Several factors need to be considered in setting up the Data Centre. This guideline provides the factors that need to be considered in setting up and managing a data center.

1.1.SCOPE

These guidelines provide best practices and implementation methods that complement TIA, CENELEC, ISO/IEC and other published data center standards and documents. It is primarily a design standard, with installation requirements and guidelines related to implementing a design. The standard includes other installation Requirements and guidelines for data centers where appropriate.

1.2. REFERENCES

Below standards and best practices have been referred to prepare this datacenter directive document

- ANSI-TIA 942 – Telecommunications Infrastructure standards for Datacenters
- BICSI - Data Center Design and Implementation Best Practices
- ASHRAE Thermal Guidelines or GR-3028-CORE

1.3. ACRONYM

EMI - Electromagnetic Interference
ITE - Information Technology Equipment
CRAC - computer room air conditioners
HVAC - Heating, ventilation, and air conditioning
SPD - Surge Protection Device
NFPA - Standard for Fire Protection of Information Technology Equipment
IBC - International Building Code

2. DATA CENTER DESIGN PROCESS

A Well thought DC design process is the mandatory consideration for any Data Center within Rwanda. As Data center is the nerve center of IT computing infrastructure. These requirements must be considered while designing Data center.
Datacenters need to meet the space requirements, ambient environment and necessary security controls to protect the critical IT infrastructure that resides within.
Following are some key considerations:

- Site location and space considerations
- Architectural and Structural loading considerations
- Electric Power and backup power considerations
- Fire protection and cooling considerations
- Redundancy / Business continuity considerations
- Green Data Center considerations
- Security Considerations
- Operational considerations

It is essential that the design of the telecommunications cabling system, equipment floor plan, electrical plans, architectural plan, HVAC, security, and lighting systems must be aligned to each other. Ideally, the design process should be able to give:

- Estimate telecommunications, space, power and cooling requirements of the data center at full capacity and scalability.
- Space, power, cooling, security, floor loading, grounding, electrical protection and other facility requirements should be designed by well-qualified architects and engineers.
- Plan adequate space for operations Center, loading dock, storage room, staging areas and support areas. Floor plan should include placement of entrance Rooms, main distribution areas, intermediate distribution areas, horizontal distribution areas, zone distribution areas and equipment distribution areas.
- Conduct a risk assessment and plan appropriate security controls. These controls should be included in each aspect of Datacenter.

2.1. Data center Tier

The data center operating within Rwanda should be above Tier three. There are four types of a tier and are defined by uptime standard.

Tier 1	99.671% Availability	Non-Redundant capacity components (Single uplink and servers)
Tier 2	99.741% Availability	Tier 1 + Redundant capacity components
Tier 3	99.982% Availability	Tier 1 + Tier 2 + Dual Powered equipment and multiple uplinks
Tier 4	99.995% Availability	Tier 1 + Tier 2 + Tier 3 + All components are fully fault tolerant including uplinks, storage, chiller, HVAC Systems, Servers and everything is dual powered

3. SELECTION AND EVALUVATION OF THE SITE

This section emphasizes the requirements for evaluating and selecting a suitable site for the Data center, whether the location is a new site that involves the construction of a new data center or reviewing the location of an existing building that will function as a data center, or the ranking of an already existing and operational data centers when considering closure or consolidation.

- The location of the datacenter should be unobtrusive so as not to attract any unnecessary attention and the site should not be located directly above water pipelines or any drainage piping as it has the risk of water leakage.
- The location where possible earthquakes and low level vibrations (less than rector scale 2) are likely to happen should be avoided and the Data center should not be located in or near an area with an active volcanoes.
- The Datacenter should not be placed near an urban development or protected natural areas where there are high chances to get wildfire. The history of location must be verified and certified by local district offices.
- The site location should be checked for the risk of a flood of a river or possible break of a lake and the site should not be located near/in an area where there is high possibility of intolerable levels of wind such as storms, tornadoes, hurricanes, cyclones and heavy rainfall.
- The quality and the stability of the soil should be tested and certified and any possibility of land sliding should be verified by local district offices.
- The site should be checked for acceptable levels of noise including the noise levels that will be produced by equipment.
- The equipment like generators, cooling towers should have silencers and sound attenuated enclosures. Outdoor equipment should incorporate sound barriers within the architectural screening.
- The impact of lightning must be verified, and the recommended flash rate of 10 or less is preferred and areas with a flash rate of 0.6 or less are to be considered as lightning free.
- Air quality of the site should be checked for the datacenter; fresh air intake for external mechanical components like cooling towers and heat exchangers and anything may be emitted from the site. Clean air quality is recommended so that emission of gases particle do not cause a problem. If there are existing quality problems, this should get verified by the air quality control and other local environmental authorities and compliance should be adhered to.
- The Location must be far away from any other location where protests and or riots are likely to take place.
- The Vibration and Electromagnetic Interference at the site should be tested if the location of datacenter is in proximity to railroad and the necessary mitigation should be taken if the vibration is not at or on the recommended level.
- The datacenter should not be placed above the train tunnel since train movements create above the recommended level vibration and Electromagnetic Interference

Below table should be referred to before the selection of the Datacenter location

Airports	8km
Auto body or other paint shops	1.6km
Canals	3.2km
Chemical plants and storage	8 Km
Conventional power plants (ex. coal, natural gas)	8Km
Embassies and political group properties	5km
Foundries and heavy industry operations	5km
Gas station and distributors	1.6km
Grain elevators	8km
Harbors and ports	3.2km
High voltage power transmission line	1.6km
Nuclear power plant	80km
Landfills and waste storage facilities	3.2km
Landing and takeoff flight paths for any airport	1.6km
Military installations and munitions storage	13km
Municipal water and sewage treatment plants	3.2km
Overflow areas for reservoirs and man-made lakes	1.6km
Quarries	3.2km
Radio/television transmitters/stations	5km
Railroads	1.6km
Research laboratories	5km
Self-storage facilities	1.6km
Stockyards and livestock feedlots	3.2km
Transportation corridors where hazardous material could be transported	1.6km
Water storage towers	1.6km
Weather or other radar installations	5km
Lakes, dams, reservoir	3.2km

3.1. Site Access

The data center site should not be close enough to the road or adjacent to the road which could result in vehicular contact with the building fabric or any building component of the datacenter which could cause potential fire. In case of proximity, proper protection of the building should be put in place.
The Site should be within a recommended distance between 3.2 km to 16km to a freeway or major arterial road. The site should have two or more accessible roads from the nearest major arterial road with each road having a minimum 4.3m length clearance for vehicles throughout.
If the datacenter is on a campus, then the campus should have redundant access roads with security checkpoints at all access points.
The datacenter should not be located near any buildings and facilities that have a risk of fire and it should not be located near a large campus or manufacturing plant which may cause traffic.
The datacenter should not be placed near some properties as mentioned below, which could potentially affect datacenter operations;

- Military
- Embassy/consulate
- Police

- Fire station
- Hospital
- Chemical plant
- Political target
- Research lab
- Publishing house/foreign press
- Adjacent vacant lots may cause future issues because of:
- Possible future development and disruption during construction
- Unknown tenant(s)

Distance between Primary and disaster recovery datacenter will be determined using primary site and whether the backup site must have synchronous or asynchronous replication with the primary datacenter. However, there should be a minimum of 50 KM between the primary and disaster recovery site.

3.2. Site Security

The site should not be placed in the area where high crime rate is registered; site perimeter security analysis should be done depending on risk and threat analysis as per the factor based on the users' needs. This would include building type, site location and neighborhood.
All emergency services are located within a reasonable distance such as Police stations, Fire Station and Hospital as below table,

Fire Station	10km
Police Station	8km
Hospital	16km

3.3. Water and Sanitary sewer

Datacenter should have adequate sanitary waste capacity from the site to the municipal sanitary waste sewer system. A private sanitary waste system should be required in regions where no national sanitary waste sewer system is available.
Sanitary systems or storm drainage systems (depending on local requirements) should be sized for expected water usage by cooling systems, including cooling tower blow down or filtration systems, which could be greater than 750 liters/min (200 gpm).
Holding tanks, traps and such requirements should be planned for during site design. A private sanitary waste system is recommended for critical facilities that require on-site operations personnel 24/7 to maintain uninterrupted services. This will help mitigate having to vacate the facility in the event the WASAC sanitary waste sewer system fails.

Data centers should have access to large volumes of water for other uses. Some uses of water that may be required are as follows:
Domestic water (e.g., drinking water, restrooms, kitchens)
Irrigation (e.g., lawn watering)
Fire suppression (e.g., sprinkler systems)
HVAC (e.g., cooling towers, air humidification)

Provide adequate water delivery to the site to meet the requirements of the data center. For Tier 3 or TIER 4 data centers, the ability of the water supply pumping station (s) to deliver water when there is a major power outage must be documented or mitigated.

The water should be tested for contaminants and particulates and water filtration systems might be required as per the testing report.

If ground water is to be utilized, make sure that there is adequate ground water delivery on the site to meet the requirements of the data center. It is necessary to first determine the volume and quality of water that will be consumed for all purposes (data center cooling, building plumbing and occupant use, lawn irrigation, etc.).

A hydrogeological risk assessment should be carried out. The assessment should be conducted by a licensed hydrology engineering firm. An environmental impact study might be required. A hydrogeological report can include information on:

- Groundwater
- Infiltration
- Soil moisture
- Surface water flow
- Precipitation and evaporation
- Uncertainty analysis
- Water quality
- Remote sensing
- Integrating measurement and modeling
- Prediction

The available on-site water (Ground water) should be tested for contaminants and particulates. Water filtration systems may be required for some or all the various water uses listed above.

3.4. Utility Services

Utility services are essential for any datacenter to run its regular operations without any interruption. It is recommended that a Datacenter site be in an area where it can acquire the necessary skilled personnel to perform maintenance and repair of IT Equipment and Facility equipment, it would be difficult to get support if the site is located far from the necessary support.

3.5. Natural Gas and Other fuels

Fuels (e.g., natural gas, propane, and diesel) may be used to support primary or back-up systems of a data center. On-site fuel (e.g., propane, diesel) storage tanks should be located outdoors on the ground or buried below ground.

If natural gas is selected to support the heating systems, cooling systems, or backup electricity generation that the site requires, provide properly sized natural gas feed from the local utilities.

Data center should have a proper arrangement to have full capacity natural gas delivery to the site for the duration of any prolonged power outage or disaster situation.

Redundant gas feeds from redundant gas sources is the most desirable although rarely available method for natural gas delivery to a site. Natural gas in combination with diesel fuel may also be considered if dual-fuel generators are incorporated into the design. Dual-fuel generators start on diesel but can run on either diesel or natural gas. For sites with natural gas generators sized 25 kW or less, on-site storage of natural gas should be considered.

The data center site should be carefully planned to support on-site fuel storage when it is required. On-site fuel storage should be located on the data center site and in a secure and aesthetically pleasing manner. Fuel should be stored as far away from the data center as practical. Blast containment (proximity to a building or actual structure) should always be planned for in the site.
Special containment or controls are usually required in case of any fuel leaks.
Controls for fuel transfer should be in a secure location, above worst-case flood levels, and protected from other natural disasters.

Other fuel or energy sources (e.g., wind, solar) may be used to support the site. Consider their continuous availability to determine if they can be primary or secondary energy sources. If other energy sources are used, their requisite equipment and system infrastructure (wind generator, photovoltaic panels) will require additional space and may affect building and structural requirements.
Careful consideration should be given to the visual intrusion on neighbors and any effects on the surrounding environment. Zoning, codes, and other governmental/municipal restrictions may not allow for alternate fuel/energy sources.

3.6. Regulations

Determine if local air quality regulations exist such as generator emission restrictions. These regulations may restrict the acceptable hours of operating backup generators.
Concerns that data centers may have for local authorities are the emissions of oxides of nitrogen (Nox), carbon monoxide (CO) and particulate matter (PM-10).

Determine if there are any local, regional, or International regulations that identify acceptable levels of noise from equipment operating within the data center facility that cannot be exceeded at or beyond the property line.

Determine if there are any local regulations that will restrict the height or proximity to other facilities for Communication towers; water tanks; cooling towers; and other tall structures.
Determine if there are any federal or local requirements to hide these structures from public view.
Determine if there are any local regulations that will require double-walled tanks or restrict the size or proximity to other facilities for fuel tanks.
Determine if there are local regulations that will allow above ground fuel tanks only.
Evaluate security of the fuel tanks.
Emission levels need to meet state and local emission requirements. Generator hours may be limited by local codes because of air quality emission control or noise abatement.

Determine if there are any road restrictions (permanent or seasonal) on the size of vehicular traffic or time of day restrictions for truck traffic.

Determine how the Rwanda Housing authority determines the required number of parking stalls for a new facility. Negotiations with the Rwanda housing Authority may be necessary to try to reduce the number of required stalls if the Rwanda Housing Authority treats the data center as a typical commercial office space.
Consideration should be given to disaster recovery scenarios, which may require additional parking for the respective personnel.

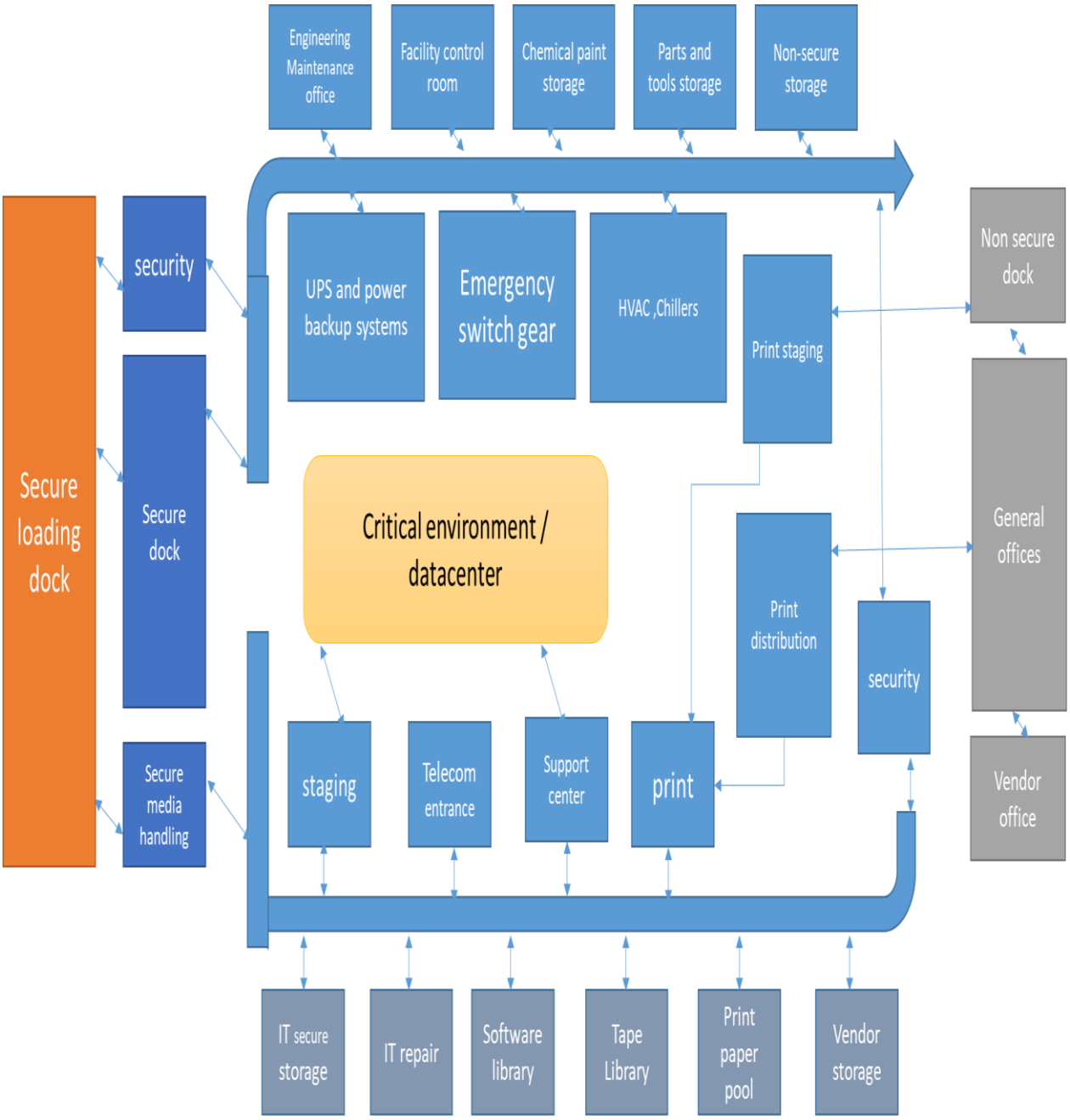
Determine the required setbacks from the property line for the building, parking, or perimeter security. Verify with the Rwanda Housing Authority that the target location does not have sight line restrictions that must be mitigated or that they can be done so economically.

An environmental assessment could include an environmental impact study if wetlands are impacted or if the site has any contaminants present. An environmental impact study may be required by Rwanda Environmental Management Authority. Ensure enough time prior to proceeding with the detailed design phase to allow completing the study and attend Rwanda Environmental Management Authority meetings as required to obtain approval.

4. SPACE PLANNING

Space planning is one of the key activities in the process of datacenter preparation. The size of the computer room space determines the capacity of datacenter to accommodate IT, Telecommunications equipment, power and cooling system. High-density data centers will have a higher capacity of power and/or cooling per unit of computer room floor space.

A balance between space and capacity needs to be determined at the outset when designing a new data center and when modifying an existing data center space. The balance will depend on the type of IT and telecommunications systems the data center is to support and the number/combination of those systems that are to be placed within each cabinet or rack.



4.1. Power Systems

The requirements of power systems should be considered when developing the space plan which includes electrical feeders, conduits and bus bar usage.

The type of UPS System should be decided before hand to plan the space accordingly and if the UPS system is centralized or distributed and the redundant power systems, replacement space, and equipment service area should be considered.

Necessary clearance should be provided for safety, access and maintenance for all electrical equipment as specified by the manufacturer, applicable codes and standards, and the applicable local approvals.

4.1.1. Electric Utility Service Feeds

Independent electric utility service feeds and associated switchgear should be in a dedicated space that is adjacent or in proximity to the primary data center electrical distribution space.

The electric utility service feeds and associated switchgear should be in a dedicated space that is equally distanced between or in proximity to the dual data center electrical distribution spaces.

Independent electric utility service feeds and associated switchgear should be in dedicated spaces separate from each other.

Utility entrance space A should be located adjacent to electrical distribution space A, and utility entrance space B should be located adjacent to electrical distribution space B. A catastrophic event affecting one should not affect the other.

4.1.2. Generator Power

The type of generator either indoors or outdoors is based on the site and the user requirements.

The indoor generators should have automated louvers, noise reduction/mitigation and exhaust management.

Outdoor generators will have increased exposure to physical and weather-related damage and generators installed outdoors should be installed within shelters.

Requirements for weight, vibration, lateral structure, and fire rating of surrounding surfaces of the space intended for a generator fuel tank capacity and location should be well planned for in the planning.

Generator exhaust systems should be located outside so that they do not flow into building ventilation air intakes, preferably on the prevailing downwind side from building ventilation air intakes.

Space planning will need to account for on-site fuel storage. The quantity of fuel that is required and can be stored will be affected by the following:

- Availability of backup or disaster recovery site for applications supported by the data center and expected time required to recover applications at the backup site.
- Proximity of the data center to locations or services, which provide fuel replenishment
- Priority status of the organization and response time for fuel replenishment during regional disasters, such as earthquakes, floods, and hurricanes
- Criticality of applications and regulatory requirements
- Business drivers requiring self-sustaining operations.
- Security considerations
- Protection from the elements (e.g., floods, storms)
- Location of fuel pumps
- Environmental requirements

- Storage of large amounts of fuel on site may trigger extensive jurisdictional and environmental permit reviews.
- Also, the permitting process may be more stringent for underground storage tanks (UST) than four aboveground storage tanks (AST).

4.1.3. Cooling Capacity

The space required to support the cooling systems will vary depending on the type of cooling system selected and the cooling systems should be selected based on the data center design and it can be one of – types below,

- central air handlers
- Perimeter CRAC units
- In row
- ceiling mount
- point of use cooling systems

4.2. Security

A security room should be located at or adjacent to the main personnel entrance to the facility.

A visitor sign-in area should be physically separated from the facility security operations.

The security rooms should include the security operations facility, including video monitoring and access control system database and front end-user interface. When planning this space consider:

- Video monitoring space requirements
- Access control system space requirements
- Access control storage requirements
- Unobstructed access to key storage
- Unobstructed access to access-card (temporary and blank) storage
- Fire/smoke alarm monitoring systems
- Restricted access to the security control room

4.3. Telecommunications Entrance Room

Provide a secure point where entering media from access providers can be converted from outdoor cable to indoor cable.

House the access provider-owned equipment such as their demarcation, termination, and provisioning equipment's.

The location for Main distribution Area, IDA and Horizontal distribution Area shall consider the maximum channel length of applications supported on the backbone cabling types to be installed.

The entrance room must be located with respect to the computer room and it should be designed to have the distance limitations of circuits to be provisioned from the entrance room.

The entrance room should be adjacent to or be in a secured space within the computer room.

The entrance room with the telecommunications main grounding bus bar (TMGB) should be close to the main electrical grounding bus bar to minimize the length of the bonding conductor for telecommunications (BCT), the conductor that interconnects the main electrical ground bar to the TMGB.

The distance limitations for T-1, T-3, E-1 and E-3 circuits and the type of media these circuits utilize and the number of DSX panels and patch panels in the channel and should refer TIA 942-A coaxial circuits for guidance.

4.4. Service Provider Considerations

The Service provider equipment and any associated cabling should be provided with adequate space. Separate or secured cable routes may be required between the entrance room and the access provider's equipment.

Access to the entrance room will be required by both the data center network operations staff and the access providers' technicians. Access to customer-owned equipment in the entrance room and the computer room should be secure from access provider technicians.

The entrance rooms should be sized to accommodate each anticipated access provider. The designer should meet with each access provider to determine their space requirements before sizing the entrance rooms. Additionally, cabinet and rack space will be required for customer-owned equipment and termination of cabling to the computer room and the rest of the building.

If there are multiple access providers, they may each request their own space. These requested spaces may be provided within the same room by using secure fencing, or they can be created by walls.

4.5. Command Center

The command center should have monitoring, but not control, a capability for all the data center building systems so that the network and system administrators are fully aware of all data center critical building system alerts or alarms.

The telecommunications room (TR) that supports the command center and other nearby data center support spaces should be outside the computer room.

The work area communications devices within the command center may need connectivity back to two different supporting cross-connect fields. Network monitoring may need connectivity directly to the core network hardware located in the Main Distribution Area space. Corporate LAN and telephone system will need connectivity to the general telecommunications cross-connect serving non-computer room communications.

4.6. Helpdesk

The helpdesk does not need to be located near the computer room and may be integrated into the general office space adjoining the data center. Alternatively, it may be acceptable to build the helpdesk and other general office space in a different building when there is no need for its location within the hardened portion of the data center facility.

Operator workstations for the helpdesk should be provided with critical electrical circuits fed from the backup generator and UPS systems to ensure that support functions are not disrupted by power fluctuations or blackouts.

4.7. Print

Printers should be located within a dedicated print room separate from the main computer room. The print room should have its own dedicated air handling system.

Power systems supporting the print functions should be considered critical and supported by the backup generator and UPS systems. Print storage may be located adjacent either to a loading dock or preferably the print room.

4.8. Loading Dock

A dedicated data center facility shall include a secure loading dock area.

Location of the loading dock should provide a step-free route through to the computer spaces with enough floor loading capacity to withstand material and equipment weights.

A dedicated data center facility should only have secure delivery capabilities such as a secure loading dock. A multi-purpose building with a data center should have a non-secure loading dock, separate from the data center, for general building deliveries.

4.9. Storage

A secured storage area for high-value equipment should be located adjacent to a secured loading dock.

The space required for secured high-value storage is recommended to be a ratio of 1:10 in comparison to the computer room space. The minimum space recommended is 23 m2 (250 ft2). The ratio may be reduced for large data centers depending on the specific operational practices.

The secured storage area should be monitored by the building CCTV security system or access controlled by the facility access control system. The system should generate a history of all access attempts.

A secured storage area should be provided for vendors' equipment. The space needed depends on the number and type of vendors who will be storing equipment on site.
The vendor storage area should be monitored by the building CCTV security system or located near or adjacent to a secured loading dock. The security requirements for vendor storage should be the same as the staging area.

4.10. Staging

All storage and unpacking activities should occur outside the computer room space, either in storage rooms or in staging areas. Preferably, a staging area should be located adjacent to the computer room. For high-value equipment, a staging area should be provided for unpacking and should be separate from any test-bench or lab space.

A staging area should have an air conditioning system separate from the computer room as cardboard boxes and packing materials can generate large amounts of particulates.

The staging area should be monitored by the building CCTV security system or access controlled by the facility access control system. The system should generate a history of all access attempts.

4.11. Administrative and engineering office

The engineering offices should be located near the electrical switchgear, UPS, generator, chiller, and HVAC rooms with enough space provided for power and cooling engineers and support staff.

The administrative or general office space may not require the same level of detailed construction as the data center and supporting back-of-house areas.
Items to be considered in the design of administrative space include:
• Disaster recovery and business continuity plans
• Operational policy during extreme weather conditions (e.g., what areas require staffing)
• Locations of emergency or “shelter in place” areas for personnel
• Future administrative space growth requirements, either as an expansion to the overall data center or as a stand-alone project
• Special function rooms such as a large conference or “war room” with wall-to-wall, floor-to-ceiling white Boards

4.12. Waste/Recycle

Recycling and compliance with local environmental initiatives is recommended. Local, state, or national incentive programs might be available to underwrite some cost.

As these facilities generate a large number of boxes, packing material, and other waste, adequate space should be allocated for its handling. Frequency of removal, fire prevention/protection, local authority requirements, and dumpster requirements, such as size, access, and location, should also be considered.

5. ARCHITECTURAL AND STRUCTURAL DESIGN

The purpose of this section is to provide information to assist a designer in the planning and specification of a computer room and related spaces.

This section will focus on the architectural and general construction elements of a data center. Some reference will be made to other elements as the purpose of the architectural elements of a data center is to provide a physical envelope that assists in meeting the needs of the end user.

The plan of the datacenter should involve the client facility in charge, IT People will have more insights about their resource and requirements.

IT, telecommunications, and other users collect data and turn it over to the facilities manager who then puts together a team that locates a site, designs, and constructs the data center.

5.1. Site Selection

The site should not have interfering elements.
The below interfering elements should be eliminated

- vibration
- air contamination
- security
- Flood
- electromagnetic interference
- Hazardous materials

The site should have enough space around the building to allow for complete security and it must have enough space for support equipment such as Generators, fuel tanks, HVAC Heat rejection systems and the site should have all electric service requirements.

The site should have the nearest prevailing ground floor for equipment access, upper floors can contribute to structural instability and mostly the upper floors are not designed for the floor loading required for a datacenter.

If the data center is on a floor above the first floor, ensure that access is provided for the equipment required in the data center.

The data center shall be located as close as possible to incoming power to reduce the power cabling lengths.

The building should be designed to meet design criteria for seismic and wind lateral conditions.

The computer room shall be located on a floor that has the structural capabilities to support the equipment. The computer rooms should be in proximity to the telecommunications entrance room(s) of the building.

The computer room is best located on the ground floor. It is generally desirable to locate the computer room away from exterior walls although it may be appropriate to design a data center where the computer rooms have an exterior wall with knock-out panels for future expansion or integration of certain free cooling options. Where knock-out panels are used, precautions against storm/blizzard damage and temperature extremes (e.g., condensation) should be taken.

Critical data centers shall be installed within a steel or concrete framed building such as a Type I, II, or III building as defined in the regulation of Rwanda Standards board. Under certain conditions, Type IV construction can be utilized if constructed in accordance with Rwanda standards board.

The exterior of buildings shall be nonflammable and of durable material, resistant to the foreseen weather conditions for the expected lifetime of the facility.

The building section shall allow a minimum clear access height of 3 mm (10 feet) from slab-to-slab.

The slab to structure above should be a minimum of 4.5 m (15 feet).

If datacenter is in multi-tenant building, it has to maintain the distance from hazards and mutual access points with other tenants.

All water lines, sprinkler lines, ductwork, and gas lines serving areas outside of the computer room shall not pass through the computer room area. No systems hazardous to the computer room shall be in or around the computer room.

All supply lines, ductwork, and telecommunication pathways serving the computer room shall not pass through the rooms of other tenants if comprehensive monitoring, protection against intrusion, and accessibility for maintenance cannot be guaranteed.

Services to the data center should be separate from services to other tenants.

5.2. 24/7 Operation of Data Center- Temperature and Relative Humidity Control

All Tier 3 and Tier 4 datacenter should have security personnel within the datacenter and security at arrival and departure locations.

At high security facilities, walls, windows and doors of rooms typically permanently staffed (i.e., command center, a guard station) should be hardened or bullet resistant.

Twenty-four-hour operations shall have break facilities within the building in the vicinity of the data center.

The design of the computer room shall include proper insulation and moisture control to maintain a steady temperature and relative humidity ranges within the data center and the computer room shall be monitored so that temperature and relative humidity can be maintained with minimum energy usage.

5.3. Materials

The computer room shall be designed and built with new materials, which are durable, of superior quality, and easy to maintain and operate. Where recycled materials will not affect the operation of the space, they may be considered for use.

5.4. General Paths of Access

All entries into the data center shall be secured. There should be a direct communication between control center and the building guard station and it should be both audio and visual for high sensitive sites.

The points of access include main data center personnel access, non-data center personnel access, vendor equipment - access, access to support equipment, such as UPS and batteries, HVAC equipment, miscellaneous electrical equipment repair access, telecommunications vendor access, and separate user group access.

The maximum slope for ramps is 8° from horizontal for movement of cabinets with equipment. However, some accessibility regulations specify a maximum rise of 1:12, or about 4.8°. Additionally, the ramp shall be at least 900 mm (36 in) clear width, have handrails on both sides, and have a 1.5 m (5 feet) clear landing at the top and bottom.

If the computer room has only one ramp, it shall meet Rwanda Information Society Authority accessibility requirements. One ramp for equipment and an elevator or ramp for wheelchair access is acceptable.

The main access to the data center should be secured via some form of access control. This control can be a combination of personnel and electronics or solely electronics. Each client should consider the level of security necessary for protection of the data being processed.

Sites without a building guard should have both audio and visual controls at the initial point of access to the data Center.

In data centers occupied 24/7; it is recommended that the initial main access route lead into a secure location outside the computer room that provides additional control prior to entrance into the computer room. Observe life safety code regarding egress.

The data center shall allow for the delivery of computer and telecommunications equipment to the facility. The computer/telecommunications equipment delivery pathway, including doors, shall allow for delivery of equipment as large as 3 m (10 feet) long by 1.2 m (4 feet) deep by 2.4 m (8 feet) high, weighing greater than 3400 kg (7500 lb).

The routes for mechanical and electrical equipment shall be large enough to permit installation of new equipment and removal of old equipment—a clear height of at least 2.7 m (9 ft) is typically required along routes from the loading docks to the electrical and mechanical rooms. Clear height requirements shall consider the height of equipment, packaging, and moving equipment.

The local access providers require access to the telecommunications entrance rooms, but they are generally restricted from access to the computer room unless:

- The entrance room is a portion of the computer room.
- The computer room houses equipment such as DWDMs, SONET multiplexers, or other circuit provisioning equipment.
- The carrier demarcation points (e.g., DS-1 or DS-3 DSX panels) reside in the computer room.

Access control shall allow access by essential vendors that support the processing equipment. The access control system may require that such vendors be escorted. This control shall allow the data center personnel to know when and where the vendors access the data center.

Support equipment that requires servicing should be serviced on the perimeter of the data center to prevent untrained personnel from inadvertently damaging the processing equipment.

5.5. Planning Detail

The entry to the computer room from non-computer room spaces shall lead into a controlled space within the data center, prior to providing access to the computer room areas.

Entry for equipment, if separate from main entry, shall be controlled by the data center personnel only.

The entry to the computer room should be positioned away from the direct access to the exterior.
Equipment entry should be located near a staging/storage area for unpacking and preparation of equipment prior to entry into a computer room.

The Command center should be near the main entrance and shall house environmental monitoring equipment, computer system monitors, and space for the number of data center operators present at any given time. A console is recommended to house all monitors.

The command center shall be located so that it has direct access to the computer room space.
As needed, office and conference facilities shall be provided adjacent to the command center for supervisory functions and to form a war room or emergency troubleshooting area.

The printer room shall be provided adjacent to the personnel areas. The printer room shall be self-contained with a filtration system on the return air leaving the room. Space shall be provided for paper staying within the printer room to ensure the stabilization of paper.

For facilities that produce in-house removable record storage media and store in-house for an extended time the media that has been removed from the library, a separate room shall be provided for media storage. A separate media room in not required when media is removed from the library and directly transferred to a permanent off-site storage location.

Storage of critical media shall be contained within a 2-hour fire rate enclosure.

Restroom and break room areas shall be provided with easy access to the operations and office areas. Restrooms shall be accessible, for both genders per the governing local codes and standards.

For 24/7 operations data centers, where practical, access to the restroom and break room should be within the security-controlled area of the data center.

5.6. Computer Room

The support equipment such as HVAC floor mounted air handlers, coolant distribution units, electrical PDU, static switches, fire suppression tank may require around 40% of overall space in the equipment area.

The cabinet and rack layout should be considered to allow for maximum flexibility. A data center may significantly change its ITE inventory every 3 to 5 years.

The data center planner should coordinate early on with mechanical and electrical systems designers. The computer rooms should be designed in a manner to provide adequate space for current equipment, growth, technology refresh, personnel and equipment circulation, and support equipment.

Production, development, and test systems should be in separate areas of the computer room, preferably in separate rooms served by dedicated networks.

Expansion should be planned into computer rooms. With the multitude of elements that affect the IT environment, it is difficult to plan for exact expansion needs.

The mechanical should be segregated from ITE in the computer room for class F3 and F4 facilities since installation; servicing and maintenance will typically be performed by different personnel.

The physical barrier is recommended to accomplish the segregation between the mechanical and ITE, permeable to the airflow or by installing the HVAC components in a separate room adjacent to the computer room with opening for the airflow.

5.7. Entrance Rooms

Class 3 and higher data centers shall have separate entrance rooms and the entrance room if separate from the computer room, shall be accessed without going through the computer room.

Class 2 and lower data centers may have a single entrance room. The entrance rooms should be attached with the computer room.

Entrance room should consider the cable termination hardware, protectors, splicing hardware, cabling pathways, space for cable pulling equipment, carrier equipment, electrical equipment, air conditioning equipment, security equipment, building automation systems and telecommunications equipment.

5.8. Mechanical Room

Outside of the computer room provide space for the heat ejection equipment and associated pumps, fuel tanks and controls.

Mechanical components within a computer room should be located separate from the ITE rows in order to provide maintenance access.

Cooling systems should be located separate from the ITE rows in order to provide for maintenance unless placement in or close to the ITE row is necessary for enhanced cooling effectiveness.

5.9. Electrical Room and UPS Room

A separate room shall be provided to contain the data center associated electrical equipment, including the switchboard, various electrical panels, generator automatic transfer switch, UPS systems, and input/output boards.

Electrical and UPS room should be as near as possible to both the main building electrical room and the generator.

The electrical room may require two exits, with doors opening in the outward direction from the room, and the doors and equipment with panic hardware as required by Rwanda Information Society authority. Secondary exit routes may pass through other associated spaces such as the battery room if permitted by Rwanda Information Society authority. .

Battery rooms with batteries containing liquid, free flowing electrolyte shall include electrolyte spill containment and exhaust systems as required by local codes.

If the batteries are in a dedicated battery room, the battery room should be adjacent to the associated electrical room.

The battery room should be located at grade level if feasible. Below grade can create a flooding hazard. Above grade can create a floor loading hazard.

The battery room should be designed to accommodate the anticipated maximum floor loading. The battery room should not be located above a computer room space.

5.10. Fire Suppression Room

A separate room shall be provided for the pre action sprinkler control valve system for class 4 datacenter and a separate room is recommended for critical or Class 3 data centers.

Space shall be provided for the placement of clean agent fire suppression tanks as required. Tanks shall be located to assist easy serviceability. Tanks shall not be in the ceiling area above equipment.

5.11. Circulation

Clear pathways allowing for the movement of racks, processing, and support equipment shall be provided throughout the space in a direct path.

Circulation pathways shall be a minimum of 1.2 m (4 ft) wide with a minimum clear overhead of 2.4 m (8 ft).

Rows should not exceed 20 cabinets or racks in length. Dead-end aisles should be avoided whenever possible for the safety of personnel. Where dead-end aisles are not avoidable, they should be no longer than 10 cabinets or racks in length.

5.12. Equipment Staging and Storage

Datacenter should have separate rooms to store arriving equipment and prepared in a room away from the computer room to prevent contaminants in the computer room and this room shall have filtration on the return air leaving the room.

The storage room can be part of a staging room or a separate room near the staging area for both arriving equipment and backup equipment such as boards, servers and other equipment.

A staging area should have the space for unpacking the preparing the arriving equipment and it should have space for large number of boxes and packing materials and consider fire protection requirements, frequency of removal and recycling to comply with local requirements.

A separate room for repair should be provided with easy access to both the equipment access and pathway to the computer room. An equipment repair room should have a work surface with multiple power and communications connections.

Caged areas should be provided for spare parts as necessary.

The building slab shall comply with all local building code requirements for protection against flooding, such as height above flood plain and setbacks from a flood plain.

All exterior openings and penetrations shall be sealed prior to work on interior walls or finishes in the computer room.

5.13. Floor Slab

Floor slabs shall be as per the calculations of the structural engineer, but no less than a floor loading of 7.2 kPa (150 lbf/ft2).

For elevated slabs, the concrete topping over metal deck flutes shall have a thickness of at least 100 mm (4 in) to allow for the adequate embedment of epoxy and anchor bolts.

The floor slab shall be leveled and sealed with a non-penetrating seal, such as epoxy, which is a moisture barrier and prevents dusting and particulate.

In order to accommodate initial or future high-density equipment (e.g., disk arrays, fully loaded server cabinets), a minimum floor loading of 12.0 kPa (250 lbf/ft2) is recommended.

5.14. Computer Room Wall Construction

The perimeter walls to the computer room shall be slab-to-slab and the perimeter walls of the computer room shall provide the appropriate level of airtightness suitable for a clean agent fire suppression system.

All wall penetrations shall be fire sealed and sealed to prevent chemical fire suppression leaks.
The thickness and shapes of wall structural elements shall meet local authority requirements for the specific wall height to be built.

Metal studs used in constructing interior walls shall have a minimum thickness of 0.64 mm (0.025 in / 22 Gauge) for wall up to a height of 3.5 m (11.5 ft) and a minimum thickness of 1.0 mm (0.039 in / 18 Gauge) for walls exceeding a height of 3.5 m (11.5 ft).

Studs shall have a minimum depth of 140 mm (5.5 in) to accommodate boxes and piping to be installed in the wall. Coordinate the thickness as all electrical and mechanical items shall be recessed or flush mounted.

Partitions touch a deck or vertical structural members; a joint isolator shall be provided to prevent transfer of vibration and structural loads.

Walls and other structural elements shall be designed for minimum deflection and securely fastened with isolation from all mechanical units and isolation pads or blocking at the top of the partitions.

For envelope walls separating the computer room from a non-conditioned or exterior space, insulation is to be provided as necessary to stabilize temperature migration. A minimum of R-3.3 $m^2 \cdot K/W$ (R-19 $ft^2 \cdot °F \cdot hr/BTU$) insulation is recommended.

Class 3 and Class 4 data centers may want to consider concrete masonry unit (CMU), concrete filled CMU, or tilt up concrete panels for the interior walls of the ITE, electrical, and mechanical space to provide additional structural integrity and high fire ratings.

In the interior of the computer room, partitions that are not required for rated separation shall be from top of access floor to the ceiling above unless additional height is required for security or environmental control. Nonrated walls shall be braced at a minimum of every 3 m (10 ft) and as required to meet lateral bracing requirements of the IBC.

Moisture/vapor seal should be provided completely around humidity-controlled spaces to prevent vapor Infiltration to and from the computer room.

Doors shall be large enough to move equipment between various data center rooms. Doors must be high enough to allow equipment entry on pallets without tilting.

Doors shall have a minimum thickness of 45 mm (1.75 in) and be a minimum of 1.1 m (3.67 ft) wide by 2.4 m (8 ft) high for a single door or 1.8 m (6 ft) wide by 2.4 m (8 ft) high for a pair of doors. Doors shall be mounted within steel frames, have a solid core, and be either wood or steel.

These doors shall have neither a center post nor doorsills.

All doors and frames within a rated partition assembly (1-hour or 2-hour) shall be rated at the code required rating of that assembly for occupancy rated separations (as per fire protection of Rwanda standards board requires fully rated doors). Doors shall have an air tight and fire-rated weather stripping all around the opening.

All doors along the entire route (i.e., from the loading dock to the computer room) should be a pair of doors.

Glazing within doors shall not exceed 0.065 m2 (100 in2). These requirements are for equipment and main exit doors to the computer rooms.
Glazing within rated doors shall be fire rate and set in metal frames. Glazed openings within rated partitions shall not exceed code limitations as set by the construction standards advised by Rwanda standards board.

Glazed openings within partitions shall be metal frame construction with glazing set in continuous stops (such as neoprene) to prevent vibration.

5.15. Fire-Rated Construction

Walls separating computer room, electrical rooms, battery rooms, mechanical rooms, and separate TRs from other areas within the building shall be a minimum of 1-hour separation or as required by applicable codes and regulations.

Doors and frames within a rated wall shall match the rating of the wall construction.

Glazing within a rated wall shall match the rating of the wall. Electrical rooms and battery rooms, as defined by IBC (International Building Code)Table shall have glazing within the doors only.

Floors above and below each of the spaces listed in below Table shall be a 2-hour rated, as defined in IBC (International Building Code). See below Table for the fire rating of spaces.

Area	Minimum Fire rating of walls
Computer room	1 Hour rating, slab to slab
Entrance Room	1 Hour rating, slab to slab
Main distributions Area	1 Hour rating, slab to slab
Horizontal distribution Area	1 Hour rating, slab to slab
IDA	1 Hour rating, slab to slab
Telecommunications	1 Hour rating, slab to slab
Command center	1 Hour rating, slab to slab
Printer room and supply storage room	1 Hour rating, slab to slab
Critical media storage	2 Hour rating, slab to slab
Electrical room	1 Hour rating, slab to slab
Battery room	1 Hour rating, slab to slab
Staging and storage room	1 hour rating , slab to slab
Loading dock	1 hour rating , slab to slab

5.16. Access Control Systems

Access control shall be provided at all entrances to the data center and all entrances to the computer room.

A system that allows for multiple levels of controls shall be installed to provide for different levels of security in different portions of the data center.

The access control system shall allow for easy modification of access control, be completely programmable, and provide a digital and hard copy of all access to the data center and its various components.

5.17. Airborne Particles

Non-conductive airborne particles can be minimized by:

- Doing all unpacking, cutting, and drilling outside the computer room
- Keeping cardboard boxes and manuals outside the computer room
- Prohibiting food or drink inside the computer room
- Avoiding carpets in computer rooms
- Using ceiling panels that have an impervious surface such as drywall panels with a vinyl covering
- Use of air filtration with regular replacement of filters
- Keeping printers, copiers, and tape media in separate rooms with separate HVAC systems
- Occasional professional cleaning of the access floor, subfloor, and overhead ducts
- Preventive maintenance cleaning of equipment, cabinets, and racks
- Place brushes, grommets, or other material in access floor openings to minimize loss of air pressure and airborne particulates.
- Fire marshals usually require that all combustible materials be stored outside the computer rooms and, in cases where aluminum floor tiles are used, keep printer toners out of the computer room to avoid thermite reactions.
- It is recommended that the designer verify that the manufacturer has tested for the resistance of zinc whisker development or has acted through the manufacturing process to mitigate whisker development. Some examples of mitigation include:
- Electroplated zinc coated or hot dip galvanized zinc coated with a special addition of other material preventing whisker growth.
- Powder coated with enough thickness
- Use of non-ferrous or stainless-steel materials

5.18. Access Flooring System

Underfloor concrete shall be cleaned and sealed after all major underfloor work has been done, including installation of the access floor system itself.

The access floor shall be a minimum of 450 mm (18 in) above the slab. When determining the minimum raised floor height for an air plenum, the mechanical designer shall analyze the height required achieving the desired air distribution.

Considerations shall include all under-floor airflow obstructions such as network cabling pathways, power systems and pathways, and cooling system piping.

Raised floor heights of 900 mm (36 in) are common.

Performance specification	Minimum	Recommended
Rolling Load (Access floor panel) Local surface deformation 0.5mm, total permanent set 1mm	567kg	680kg
Impact load Drop weight, dropped from 305mm height on 645mm local surface with deformation 1.5mm	68kg	79kg
Concentrated load Load on 645 mm2 point with maximum deflection 2mm anywhere on the panel	567kg	680kg
Uniform load Load rating of access floor system, including panels, pedestals and stringers	732kg/m2	1221kg/m2

The building's structural system supporting the access floor must support the access floor and all imposed loads.

The assembly shall be leveled and locked at a selected height, requiring deliberate action to change the height setting and preventing vibration displacement.

Pedestals shall be secured to the slab using a method acceptable to the access floor manufacturer and Rwanda Standard Board. This is typically performed using bolts, adhesives, or seismically isolated floor systems.

Stringers shall be used for all access floors exceeding the height of 500 mm (20 in).

All tiles shall be supported at all four sides/corners, and the tile surface shall have anti-static properties in accordance with IEC 61000-4-2(International Electro technical Commission's immunity standard on Electrostatic Discharge (ESD).

A structural engineer shall be consulted to provide a recommended maximum number of contiguous tiles and stringers that can be removed at any one time, and this information shall be incorporated into the operational guidelines for the data center.

For higher power density equipment where the underfloor space is used for cooling, the access floor should be a minimum of 900 mm (36 in) above the slab.

If the location has seismic activity, the access floor selected should be designed by the manufacturer for seismic applications, installed in accordance with the manufacturer’s instructions, and certified by a professional structural engineer.

Additional structural and operational criteria/factors to consider should include:

- Panel drop tests
- Maintaining panel integrity for a given cut-out size
- Pedestal axial loads
- Pedestal overturning moment
- Stringer mid span concentrated loads
- Permanent sets and deformations of any system components
- Pedestal bases should be glued directly to the concrete slab and not to the epoxied/painted slab

5. 19. Ceilings

In data center computer rooms and telecommunications spaces (e.g., entrance rooms, TRs), the minimum ceiling height should not be less than 3 m (10 ft) from the finished floor to any obstruction such as sprinklers, lighting fixtures, or cameras

Minimum 450 mm (18 in) clearance from sprinklers to raceways, cabinets, and racks shall be maintained to ensure that they do not disrupt the sprinkler distribution pattern subject to the Rwanda Information Society Authority.

The recommended ceiling height for computer room spaces (from slab-to-slab) is 4.5 m (15 ft or greater).

A suspended ceiling may not be required for computer rooms that do not use the ceiling space as an air-return. Benefits of an open ceiling (where not required for cooling) are the visibility of any technical problem and the ease of access to installations and pathways mounted underneath the ceiling slab.

Office-type ceilings should not be installed in new data center spaces. Depending on the design for the cabinets and the HVAC solution, there may be an HVAC solution design requirement to provide a ceiling return air plenum.

The materials used and the design of this type of ceiling shall consider any need to support cable trays or other cable pathways for overhead cabling in the data center.

Ceiling requirements should be developed taking into consideration non-flaking or dusting tiles, vapor resistance, and hold down clips for gaseous fire suppression discharge or high-volume airflow and acoustics. Materials known for metal whiskers (e.g., zinc, tin, cadmium), whether electroplated, pre-galvanized, or hot dip galvanized, should be excluded from ceilings.

5.20. Equipment Bracing System

Equipment cabinets and racks shall be braced in accordance with local codes. Cabinets braced at the top can utilize the cable ladder rack system, if present, with an attachment that provides rigid four-directional lateral bracing. Equipment mounted on access floors in seismic areas shall be braced to the underfloor slab with an approved method. The bases of cabinets and racks should be braced to the slab as appropriate for the seismic demand in accordance with local seismic codes or requirements.

5.21. Structural Building Code Compliance and Coordination

Local building codes shall be consulted in the planning and implementation of changes to the building and its mechanical, electrical, and life safety systems.

All loads on the structure are divided into various types:

- Dead loads, soil loads, hydrostatic pressure loads
- Live loads
- Flood
- Snow
- Rain
- Ice
- Seismic
- Wind

The magnitude of forces on any structure is a function of its geographic location. Rwanda Housing Authority identify the forces expected to be applied to buildings and nonstructural components. The applied forces are a function of probability at a given location for environmental loads (e.g., wind, ice, snow, flood, tsunami, and earthquake).

Critical facilities requiring higher performance should consider loads and performance requirements contained in the UFC 3-310-04(Seismic Design of Buildings) and UFC 3-301-01(structural engineering), or regional equivalent.

Additional loads that may warrant consideration for data centers include tsunami and ice impact loads because of shedding on adjacent structures such as telecommunication towers.

5.22. Structural Concerns Specific to Data Center Design

Floor loading (superimposed live load) shall be a minimum of 7.2 kPa2 (150 lbf/ft2) with 1.2 kPa (25 lbf/ft2) hanging dead load (weight that can be supported from the underside of the floor or roof). This floor load is adequate for most data center areas.

1.2 kPa (25 lbf/ft2) hanging dead load, the recommendation in this standard is a uniform load of 12.0 kPa (250 lbf/ft2) with 2.4 kPa (50 lbf/ft2) hanging dead load to provide flexibility in the location of higher floor loads such as large storage arrays, printing facilities, and densely populated blade server cabinets.

In specific regions of the access floor area where this equipment is located, the structural engineer should be notified of the specific operating weights.

Floors for battery rooms should be designed for a minimum superimposed live load of 12.0 to 23.9 kPa (250 to 500 lbf/ft2).

Roof areas over battery rooms should be designed to support a minimum suspended dead load of 1.4 kPa (30 lbf/ft2).

5.22.1. Raised Access Floors

Raised access floors are commonly used in data centers. When raised access floors are in use, all raised access floors shall meet Rwanda standards board special access floor requirements.

Raised access floors shall be designed and tested as a Designated Seismic System and shall have Special Certification Requirements as defined in the Rwanda standards board. The response spectra shall be calculated at the bottom and at the top of the raised access floor to determine the demand on the equipment mounted on the floor. The response spectra shall be computed for the in-structure response accounting for the structural support in addition to the response characteristics of the raised access floor.

The Rwanda standards board do not appropriately address seismic vertical ground motions and the amplifications of vertical ground motions in the structure. The nuclear industry and military industry require the calculation of the seismic demand because of vertical ground motions that is referred to as the seismic demand. UFC 3-310-04(Seismic Design of Buildings) can be used as a reference to determine a methodology to seismically qualify raised access floors.

Because of the importance of data centers, an in-structure response analysis should be used to compute the coupled response of a raised access floor. A coupled response can then be used to develop response spectra for equipment mounted on the raised access floor.

Equipment that is determined to be mission critical shall be designed and tested to determine the seismic demand and the equipment fragility. The seismic demand of mission critical equipment shall be determined at the point of attachment of the equipment.

Equipment determined to be mission critical shall specify the performance expectations. The seismic demand shall be determined at the point of attachment. The point of attachment may be a structural element, or it may be a nonstructural component (such as a raised access floor). If required, a coupled dynamic analysis may be required to determine seismic demand.

5.22.2. Wind

In the design of data centers, the implementation team should verify the wind-loading calculations with Rwanda Environment Management Authority for wind and it has to be considered in the project plan.

5.22.3. Earthquake

Data centers are placed in International building code Risk Category IV because of their criticality. The owner may elect to use a reduced Risk Category rating of II if the facility does not have to operate after an earthquake.

Designating a facility as Risk Category IV will still not necessarily ensure a data center will be functional following a major earthquake. If a facility is intended to be operational with a high degree of confidence following a major seismic event, it should be designed in accordance with the provisions of UFC 3-310-04(seismic design of building) for Risk Category V.

For data centers, special attention must be paid to the design of specific nonstructural components, such as raised access floors, that will have a direct impact on the survivability of the computer functions after an earthquake.

Depending on the height of the raised access floor and the amount of a mass supported as well as the magnitude of the earthquake, it may be necessary to isolate the access floor from the rest of the structure.

The process of isolation is generally referred to as base isolation. Base isolation is also a valid consideration for the entire building. Base isolation creates other concerns for elements that cross the plane of isolation. Care must be taken in the anchorage of generators, chillers, fans, switchgear, piping and conduit, and racks. The force on the support for these elements will be substantially increased as a function of their mass multiplied by the dynamic coefficients addressed in the code enforced earthquake design. The in-structure demand response spectra must be compared to the fragility of the nonstructural component.

5.22.4. Blast and Terrorist Attack

Many data centers are designed to resist the effects of a terrorist attack. Terrorist attacks can be in many forms, but the most prominent attack is in the form of a blast from some manner of vehicle-borne improvised explosive device (VBIED). Security experts and law enforcement should be consulted to quantify the size of an explosive device.

Security and physical site barriers should be constructed to maximize the distance that a VBIED can be from the data center. The blast dynamic pressures can be calculated and compared to the response of the data center structure and building envelope elements. Guidance for blast-resistant design may be found in the regulations of Rwanda standards board.

Smaller explosive devices can be mitigated by screening processes that place the threat at a defined distance from the facility.

Terrorist attacks can take many forms that can include introducing chemical, biological, or radiological agents into a facility. Protection should include screening for compounds that could be brought into a facility clandestinely and controlling air supply into a facility.

6. POWER AND ELECTRICAL SYSTEMS DESIGN

Electrical distribution systems for data centers are designed to power the center safely and reliably and this section will also address the power distribution and monitoring solutions that have been successful in meeting these demands, and how data centers can be designed to create sustainable IT environments that can satisfy evolving business, financial and regulatory goals.

The electrical system design should not have a single point of failure as it may lead to interruption in the service and business continuity.

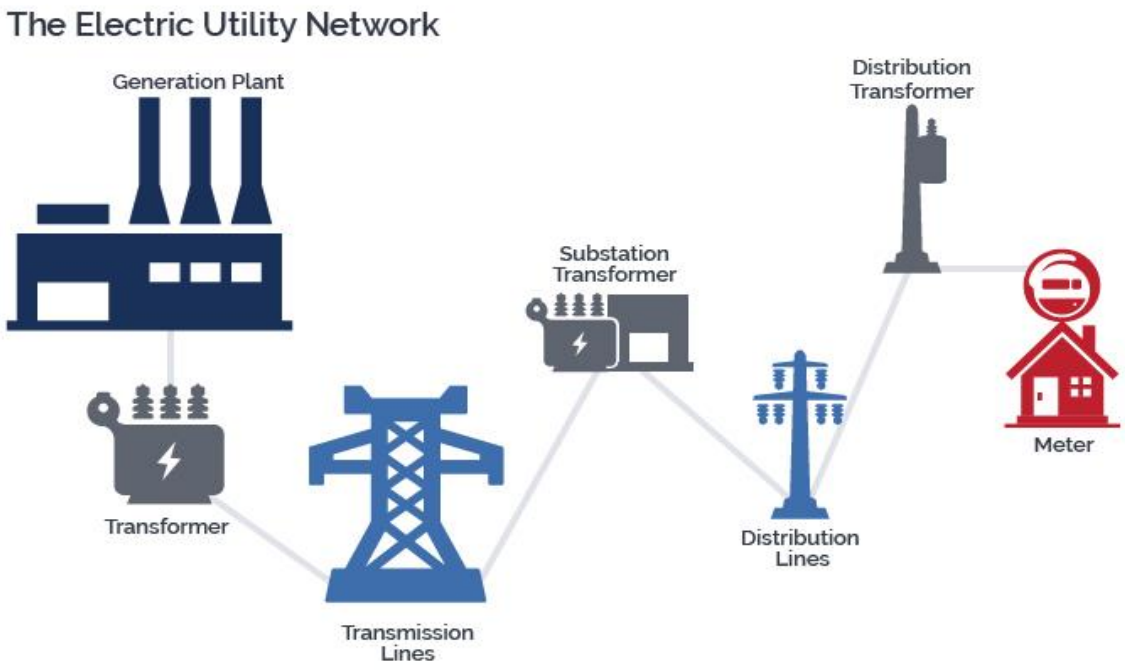
The site should be provided with enough electrical utility capacity to meet it is current and projected needs of the entire requirement of the datacenter.

The site should have multiple electrical source circuits with enough capacity to meet the entire site requirements.

The Datacenter should be in an area with easy sustainable circuit access to utility substations with a preference towards an area with utility circuits provided by two or more utility substations.

The site should have space for an electrical unit substation and its associated transformers and electrical utility circuit paths, and it should be located on the datacenter site in a secure way with accessibility.

Below Figure shows an overview of electrical transmission and distribution.



AC Electricity Distribution from Generation Stations to Data Centers

6.1. Transformers:

Transformers usually transform the utility's medium distribution voltage to a lower voltage for utilization by the data center.

The substation might transform voltage in excess of the site requirement and an on-site utility transformer might then transform the voltage to a lower voltage utilized by the building or facility.

The transformer size should be calculated based on the datacenter size, class and the load in the datacenter.

The Datacenter should have a dedicated transformers. The datacenter site should have considerable space for a minimum one electrical utility transformer and their associated electrical utility circuit paths and it must be located on the datacenter site in a secure and visible manner.

Datacenter is a critical infrastructure and it should have independent utility service to provide high availability services to the consumer.

Second power utility feed is advisable, but it depends on the uptime report of primary feed and benefits of a second power utility feed should be analyzed based on the mean time between failures (MTBF) to mean time to repair (MTTR) and power stability service to the data center.

A second power utility feed is recommended when the operational requirements of the data center results in an Operational Level 4, The availability requirements of the data center results in an Availability Ranking Level 4, The impact of downtime of the data center results in a Catastrophic classification, The reliability of the utility, based on the specific MTBF rates of the utility and the required mission time of the data center, is greater than 50%.

Electrical service entrance feed should have a minimum separation of 1.2 m (4 ft.) from other utilities along the entire route.

If redundant feeds are provided to the data center, it is recommended that the electrical service entrances to the facility have a minimum separation of 20 m (66 ft.) from the other electrical service entrances along the entire route.

At least two diversely routed electrical service feeds from different utility substations with each substation on separate power grids.

At least two diversely routed electrical service feeds from different utility substations with both Substations on the same power grid.

At least two diversely routed electrical service feeds from one utility substation. One electrical service feed from one utility substation.

Utility services should be underground to the facility as it will reduce the potential threat to system failure caused by overhead utility line damage. Overhead utility service is not recommended as it poses a risk to the vehicle accident, wind and some other weather conditions.

6.2. On Site Generation

Backup generators should be there as a backup to data center equipment in case of utility power failure. Emergency generators should be there to power the data center life safety systems (e.g., emergency lighting, fire pumps) if utility power fails.

The datacenter site should have considerable space for one or more emergency and backup generators and their associated electrical utility and life safety circuit paths, and it should be located on the datacenter site in a secure manner.

The datacenter should have necessary fuel pumps, piping and on-site storage and the space required can dictate performance for a minimum 48 hours without outside services.

6.3. Availability

All electrical equipment must have redundancy to increase both fault tolerance and it must be documented well to maintain to avoid the outage due to human error, and this helps to maintain the overall redundancy in data centers.

The capacity is kW required to serve the load and plus the design margin and growth factors.

Capacity is the power required by the load and is designated as "N". Higher levels of availability (based on the criticality of the activity supported by the data center) require higher levels of redundancy.
We recommend implementing below level of redundancy in Tier-3 and Tier 4 Datacenter.

6.3.1. 2N Redundancy

2N redundancy provides two complete units, modules, paths, or systems for everyone required for a base system. 2N is also referred to as "dual-path topology." Failure or maintenance of one entire unit, module, path, or system will not disrupt operations. For smaller fault-tolerant systems where a single module can accommodate the critical load, the 2N and N+ 1 model are synonymous.

6.3.2. 2(N+1) Redundancy

2(N+1) redundancy provides two complete (N+1) units, modules, paths, or systems. The failure or Maintenance of one unit, module, path, or system will still leave intact a system with full redundancy and will not disrupt operations.

6.3.3. Multi-N Redundancy (xN)

A multi-N system topology is used primarily in fault tolerant or large-scale power systems where more than two large systems are employed together. In such a system topology, the critical load connection at the PDU or the branch circuiting level is the primary means of achieving the redundancy and Class of the system.

Below table displays four different levels of design efficiencies for an N+1 topology. For example, if N is 100 kVA, N+1 redundancy can be achieved in any one of the following ways:

- 2 × 100 kVA modules (50%)
- 3 × 50 kVA modules (66%)
- 4 × 33 kVA modules (75%)
- 5 × 25 kVA modules (80%)

Design Efficiency Ratios -Topology UPS or power systems ratio Design efficiency
(Required kW/installed kW)

- N 1:1 100%
- N+1 2:1 50%
- N+1 3:2 66%
- N+1 4:3 75%
- N+1 5:4 80%
- 2N 2:1 50%

- 2(N+1) 6:2 33%
- N + 2 3:1 33%
- N + 2 4:2 50%
- N + 2 5:3 60%
- N + 2 6:4 66%

6.4. Electrical Class Ratings

The standard includes five Classes relating to various levels of reliability of the data center facility infrastructure. The Classes are completely performance related, and it is mandatory to implement Class F3 and F4. The five Classes are:

- Class F0 - a single path data center that meets the minimum requirements of the standard, but doesn't meet the requirements of an F1 or higher-level data center
- Class F1 - the single path data center
- Class F2 - the single path data center with redundant components
- Class F3 - the concurrently maintainable and operable data center
- Class F4 - the fault tolerant data center

6.4.1. Class F3

The Class F3 system possesses redundancy in the power paths to the critical load, but only one of those paths needs to be UPS powered.

The alternate path may be UPS powered, but this Class requires that it only be available and dedicated to the IT load.

On a dual-corded IT device, one input would be fed from the UPS power system, while the other input is fed from the non-UPS source.

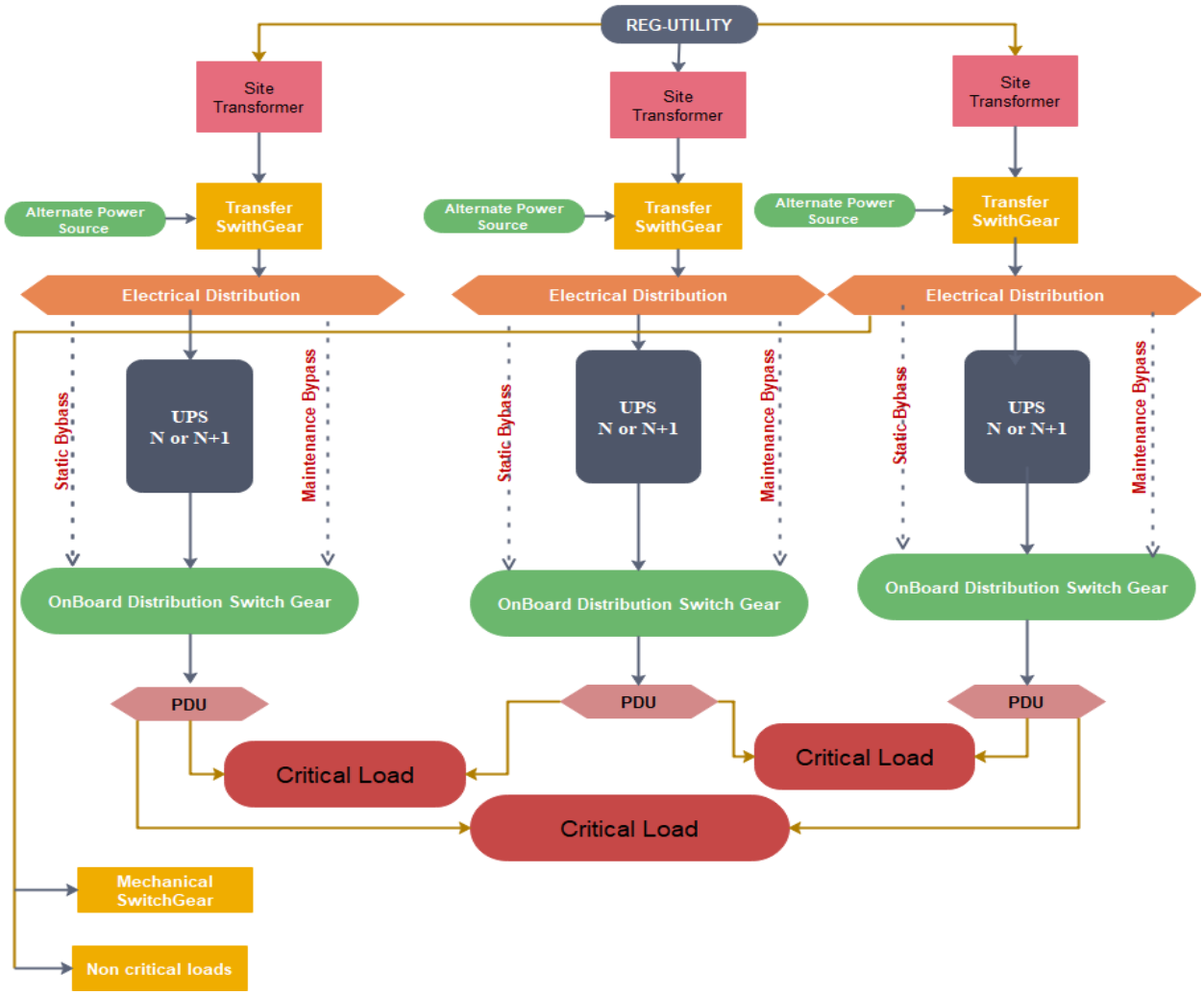
The Class F3 system allows for complete maintenance during normal operations (on a planned basis), but it loses redundancy during maintenance and failure modes of operations. STSs are required for single-corded loads to provide power redundancy where no IT component redundancy exists. STSs are not required for dual-corded loads.

All maintenance and failure modes of operation are transparent to the load.

Industry description	Concurrently maintainable and operable
Component redundancy	N+1, as a minimum
System redundancy	N
Number of utility sources	Once source with two inputs or one source with single input electrically diverse from backup generator input
Power sources available to critical load	TWO
UPS Sources available to the critical load	One UPS system with one UPS power path the load.
Ability to be maintained while under load	Yes, with a reduction of the system redundancy from N+1 or better to N during maintenance activities
Ability to recover from failures	At the plant and distribution level, but with a reduction of the system or distribution redundancy from N+1 or better to N after failure and prior to the recovery
Resulting definition	Multiple source/N rated single or multi module system/dual or multiple path

6.4.2. Class F4

A Class F4 system possesses redundancy in the power paths, and there may be more than two independent sources of UPS power to the critical load. The individual critical power systems are rated for the complete load for the 2(N+1)/system-plus-system option. For larger loads, the system may have multiple UPS systems where the system diversity is provided solely by the connection of the critical loads to the multiple UPS systems.



Each UPS system could be a multi-module UPS system or a single/high-kW UPS system. The fault tolerant system provides load source selection either via static transfer switches or by internal power supplies in the IT systems themselves.

There are no single points of failure in either the critical power system or the power systems supporting the mechanical or vital house/support loads. The Class F4 system allows for complete maintenance during normal operations and does not lose redundancy during either failure or maintenance modes of operations. All maintenance and failure modes of operation are transparent to the load.

Industry description	Fault tolerant
Component redundancy	Equal to or greater than N+1
System redundancy	Yes
Number of utility sources	One or more sources with two inputs
Power sources available to critical load	More than two
UPS sources available to the critical load	Yes with a reduction to no worse than N+1 during maintenance activities
Ability to recover from failures	Yes automatically with a reduction to no worse than N+1 after the failure and prior to the recovery
Resulting definition	Dual or multiple source(N+1 or better) power systems/multiple paths with redundant components

6.5. UPS SYSTEM

UPS and critical power system applications are focused on delivering quality power, whether originating from an electric utility or from internal energy storage, on an assured, 24/7 basis.

Datacenter should have reliable device to maintain the business continuity without any disruption. A UPS is usually required to provide stable power to sensitive active and passive equipment, and it can become single point of failure that affect multiple servers and business continuity disruption can be huge. So, resilience should be considered while planning the UPS for datacenter.

The primary concern of UPS system design for Class F3 and F4 systems is the maintenance of critical power services while accommodating known failures or allowing for safe and logical preventive maintenance.

Select a UPS that supports multiple power inputs, allowing two different sources to power the UPS unit. If one utility line fails, power from the other line can run the load and keep the UPS charged.

The Uptime Institute regards electricity from utility service providers as an unreliable source of power. Therefore, Tier 3 data center specifications require that the data center should have diesel generators as a backup for the utility power supply.

An automatic transfer switch (ATS) automatically should transfer the control to backup generator if the utility power supply goes down.

The Tier 3 data center specifications mandate two ATSs connected in parallel to ensure redundancy and concurrent maintainability.

Tier 3 data center specifications require the diesel generators to have a minimum of 12 hours of fuel supply as reserves. Redundancy can be achieved by having two tanks, each with 12 hours of fuel. In this case, concurrent maintainability can be ensured using two or more fuel pipes for the tanks. Fuel pipes can then be maintained without affecting flow of fuel to the generators.

Redundancy and concurrent availability can be achieved using separate power distribution panels for each ATS. This is because connecting two ATSs to a panel will necessitate bringing down both ATS units during panel maintenance or replacement.

The Tier 3 data center specifications require two or more power lines between each ATS and power distribution panel to ensure redundancy and concurrent maintainability.

Each power distribution panel and UPS should also have two or more lines for the same purpose.

Power from the distribution panel is used by the UPS and supplied to the power distribution boxes for server racks as well as a network infrastructure. For example, if a 20 KVA UPS is required for a data center, redundancy can be achieved by deploying two 20 KVA UPS or four 7 KVA UPS units. Redundancy can even be achieved with five 5 KVA UPS units.

The Tier 3 data center specifications require that each UPS be connected to just a single distribution box for redundancy and concurrent maintainability. This ensures that only a single power distribution circuit goes down, in case of a UPS failure or maintenance.

Each server rack must have two power distribution boxes in order to conform to Tier 3 data center specifications. The servers in each rack should have dual power supply features so that they can connect to the power distribution boxes.

A static switch can be used for devices which lack dual power mode features. This switch takes in supply from both power distribution boxes and gives a single output.

The static switch can transfer from a power distribution box to another in case of failures, within a few milliseconds.

A data center built according to Tier 3 data center specifications should satisfy two key requirements: redundancy and concurrent maintainability. It requires at least n+1 redundancy as well as concurrent maintainability for all power and cooling components and distribution systems.

A component's lack of availability due to failure (or maintenance) should not affect the infrastructure's normal functioning.

Class F3 Model provides multiple power paths as close to the critical load as possible and Class F4 Model include different number of UPS power plants versus the number of UPS Power delivery path.

The static bypass, the maintenance bypass, the output breaker, and any load bank testing connections can all have a direct impact on the maintenance and failure response of the UPS system.

Bypass configurations can affect UPS functionality as follows:

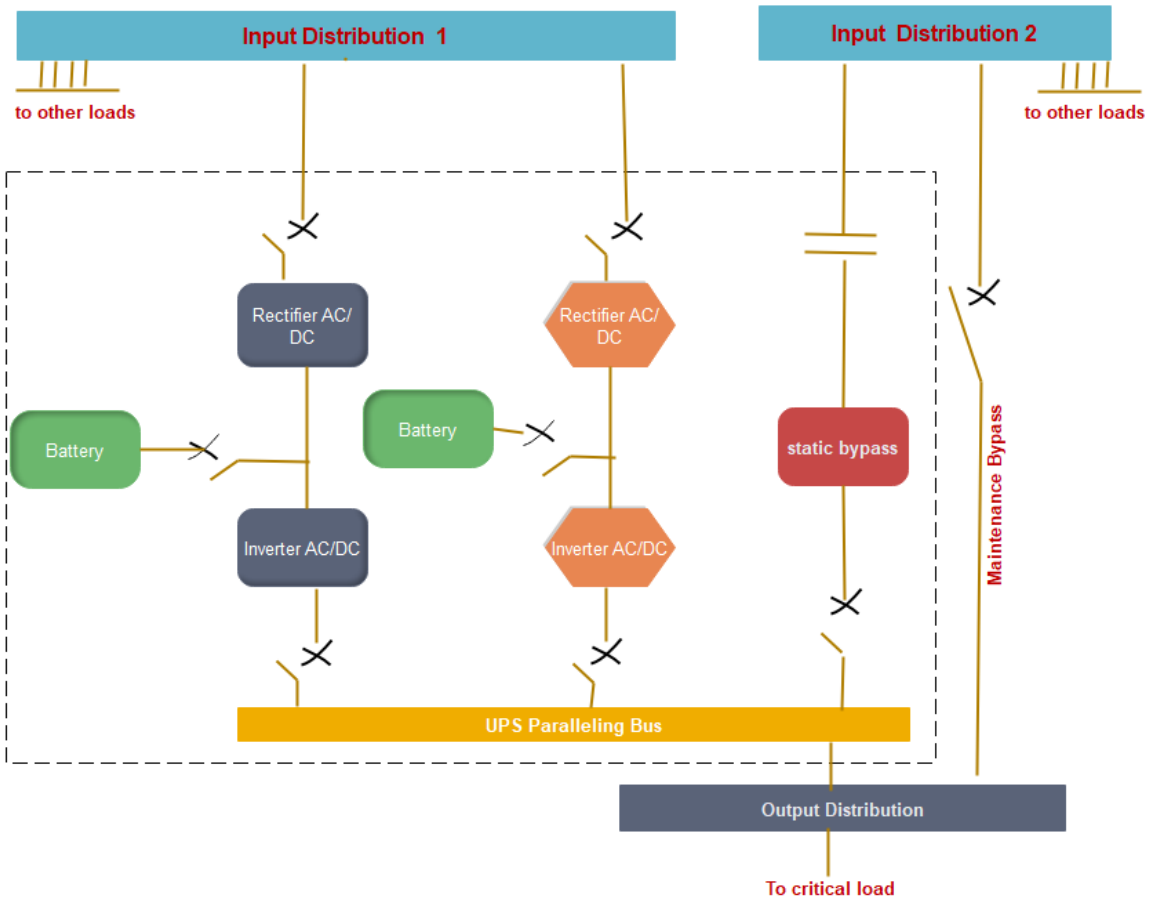
- Combining maintenance bypass and static bypass paths from a single input feeder will typically result in a lower Class because it reduces the ability to remove a module or system without interrupting the service to the downstream critical loads.

- Load bank connections that are independent of the UPS output source can contribute to a high Class because they allow for testing without interrupting the service to the downstream critical loads.

- Locating circuit breakers on the collector bus or on the output bus of paralleled UPS systems rather than Making them internal to a power module will contribute to a high Class by allowing a module to be removed from the service without shutting down the entire system. These are also known as isolation breakers.

- The presence of a maintenance bypass will allow for the removal or testing of a UPS module or for the replacement of a static switch in the event of a catastrophic failure. This has a dramatic effect on the mean time to repair (MTTR).

Maintenance bypass is mandatory for all Class F3 and F4 applications and for system control cabinets.



When the input to the rectifier and the static bypass originate from one bus (Input Distribution 1) and the maintenance bypass originates from a separate bus (Input Distribution 2), the critical load shall be transferred without interruption or disturbance to an isolated source, either utility or generator, depending on the design, while the UPS is repaired or tested.

When other loads are connected to the bus that support either the rectifier and static bypass (Input Distribution 1) or the maintenance bypass (Input Distribution 2), the designer shall also consider how any disturbance on the input bus could affect the critical load while operating in this mode and (how to minimize the disturbance). This type of design, including disturbances may be caused by:

- Testing of the UPS
- Testing of other loads connected to the same bus
- Turning on and off other loads connected to the same bus
- Fault conditions

Inputs to the static bypass and maintenance bypass shall not be derived from separate sources unless the two sources are synchronized in phase and frequency. Lack of synchronization will result in an unreliable design that should require open transition (i.e., shut down the loads and then restart from the alternate source.

Note that synchronization of sources is difficult because load imbalances and phase shifts (such as transformers introduced downstream) can force circuits out of synchronization. The best practice is to power both the static bypass and the maintenance bypasses from the same source.

The UPS system static bypass and maintenance bypass designs should consider using the same source or type of source for the closed transition transfer mechanisms.

This would require the power module inputs, static bypass input, and the maintenance bypass input to be synchronized to the same source.

Depending upon the configuration, some UPS could be exempted from this rule when the static bypass input and the output of the UPS are synchronized. For example, input to power module inputs could be fed from utility 480 VAC wye source “A” while the static bypass and maintenance bypass could be fed from utility (or generator) 480 VAC wye source “B”.

Other UPS configurations may have the maintenance bypass external to the UPS system to enable the UPS to be taken off-line for maintenance or replacement. It is acceptable to have the maintenance bypass internal to the UPS system in a Catcher system since the Standby UPS system can function as the external alternate path in the event the UPS system needs to be taken off-line for maintenance or replacement.

Attention shall be paid with respect to the configuration of disconnects external and internal to the UPS system to enable maintenance of rectifiers, inverters, or static bypass components in a safe manner.

A dedicated input to the static switch that is separate from the rectifier input allows the critical load to further sustain faults that could be associated with the rectifier. In Class F0 and Class F1 applications, a single source of input power for both the rectifier and the static bypass is permitted.

Static bypass switch input

Class	Description and input source
F0	Single power module with a single input to both rectifier and the static switch.
F1	Single power module with inputs to both the rectifier and the static bypass switch from the same upstream breaker.
F2	Single or multiple power modules, all power module from the same upstream distribution, static bypass switch input from separate upstream breaker than power module plants.
F3	Multiple power module, all power module inputs from the same source, static bypass switch input from a separate upstream breaker than power module inputs.
F4	Multiple power module, all power module inputs from the same source, static bypass switch input from a separate upstream breaker than power module inputs.

6.6. Synchronization

Synchronization can occur in one of two ways for UPS systems:

- Actively based on some form of external control system
- Passively by the management of the static switch inputs to the given modules or via active systems specific to the UPS manufacturer, depending upon the chosen UPS topology.

The active systems offer excellent synchronization functionality, especially when the UPS system uses batteries.

The passive system is important as vital system transfers are assured to be coordinated when the static inputs are managed and considered in the design. A lack of input or output synchronization could result in a failure of ASTS operation or an out-of-phase transfer, thereby resulting in a dropped load and possible equipment damage.

UPS systems shall be synchronized in one of two ways:
• Line-side (source) synchronization
• Load-side (output) synchronization

In either event, synchronization is vital and shall be required for a high-reliability system at the Class F3 and Class F4 levels. Since Class F0, Class F1, and sometimes Class F2 systems are single module/single plant systems, no external synchronization is required.

When system-level synchronization is not possible, static switching at the loads or critical power buses may be required.

6.7. UPS Output Switchboards

Output switchboards directly support the PDU and ASTS systems downstream of the UPS power plants. For Class F1, F2, and F3 systems, UPS outputs should be vertically organized to the UPS output distribution system downstream. Simpler electrical topologies may not have separate UPS output switchboards and critical power distribution switchboards.

For Class F3 systems, the second path may be derived from a non-UPS source. For Class F4 systems, there may be multiple power paths, but these are kept separated until they meet at the critical load.

6.8. Ties and Interconnections

If the UPS sources are synchronized and are not overloaded, UPS systems may transfer load between each other. Except on a plant level, the UPS is the foundation of the multi corded system for critical loads.

All transfers are done via closed-transition, and the control systems for this type of operation are typically redundant or offer some other form of manual operation if the control system fails.

System ties are common in system-plus-system configurations, and several UPS system manufacturers offer pre-engineered solutions for this design feature. For xN or other types of UPS topologies, the system designer shall engineer a solution for the given UPS module and plant configuration.

Ties and interconnections should also prevent the propagation of failures and should limit short circuit fault current.

6.9. UPS Output Distribution

UPS output distribution switchboards are located immediately downstream of the UPS power plants and extend to the PDU or data processing room levels.

One important consideration for these systems is that they do not have to follow the redundancy level or plant counts found in the UPS power plants.

Class F1 systems, the UPS output distribution switchboards are single units.
Class F2 systems, there may be module redundancy, but there may not be UPS power path redundancy. In both cases, UPS systems would match the total UPS power paths.

In a Class F3 system with a single UPS power plant, there are at least two UPS output powered critical distribution switchboards, one on the active path and one on the alternate, or non-UPS, path.
For a Class F4 system, there are at least two critical power switchboards, if not more.

UPS output distribution switchboards may come in numerous specifications and configurations, all depending on the maintenance and failure mode of the critical loads downstream and UPS systems upstream.

6.10. Power Distribution Units (PDUs)

PDUs with an isolation transformer create a separately derived neutral for downstream loads although this may not be necessary for 3-phase loads or for systems in which the load utilization voltage is created at the UPS.

PDUs with transformers convert the output voltage of the UPS system to the utilization voltage of the critical loads as needed.

The PDU should have output branch circuit panel boards or distribution circuit breakers that serve the downstream critical loads or subpanel boards serving downstream critical loads.

If the PDU has an isolation transformer, its inrush characteristics should be coordinated with the upstream UPS peak load tolerances for normal, failure, and maintenance modes of operation. Low inrush transformers may also be employed depending on the UPS system’s design.

Where PDUs are expected to run close to their rated loads or one or more loads will generate large harmonic currents, a K-factor transformer might be considered.

Harmonic currents can be created by the ITE (e.g., switched mode power supplies [SMPS]), but they can also be created by fans or drives that are connected to the PDU critical bus.

High harmonic currents, especially those caused by single-phase power supplies in the ITE that create triplen harmonics (odd multiples of the 3rd harmonic, such as 3rd, 9th, 15th, 21st), can cause PDU output voltage distortion and transformer overheating. This heating reduces the efficiency of the transformer and increases the load on cooling equipment. These problems can be exacerbated when the PDU's transformer is operated close to its rated capacity.

Transformers are frequently rated to K-9, but they may also be as high as K-13 to K-20. K-factor rated transformers are larger, more expensive, and less efficient than non-K-rated transformers, thereby increasing both capital and operating expenses, so they should be deployed judiciously.

For Class F3 and Class F4 facilities where the transformer seldom operates at greater than 40% of its rated load, K-factor rated transformers may not be necessary as harmonics can be tolerated up to a certain level.
• It may have a harmonic-tolerant (or K-rated) transformer.
• It may have a low inrush transformer to prevent unintended upstream circuit breaker trip.

6.11. Direct Current (DC) Power Systems

DC power systems that serve critical loads are common in two forms:

- The primary power source for access provider and carrier equipment.
- As an alternative to AC power in computer rooms because of energy efficiency, design simplification and ease of paralleling alternative energy sources DC power distribution systems function within the data center in the same way as the AC systems providing power to a variety of loads. However, DC-based systems can offer additional features that can be attractive to data center designers and operators. It is also possible to mix DC and AC systems in hybrid configurations, for example, providing DC to critical loads and AC to mechanical loads.

DC power system operating voltages are affected by several factors such as:

- Battery technology (e.g., lead-acid varieties, nickel-cadmium, nickel-metal-hydride, lithium-ion varieties, sodium varieties, flow varieties)
- Rectifier output regulation in maintaining constant voltage under dynamic loads
- Voltage drops in DC power conductors—cable sizes and lengths
- Operating voltage limits of various connected loads
- Derating for environmental conditions such as altitude
- All DC equipment shall be properly and clearly marked according to the applicable electrical or building codes and as required by the appropriate listing agency. DC equipment includes, but is not limited to:
- Cords
- Cables
- Raceways
- Bus ways
- Power connectors
- Junction boxes

- Batteries
- Generators
- Flywheels
- Circuit breakers
- PDUs
- Rectifiers
- DC-UPS

The design of all DC-powered ITE shall likewise comply with applicable sections of required electrical and building codes and shall be rated, listed, and marked for DC operation at the anticipated voltage range.

Electrical safety clearance rules are applicable to both AC and DC circuits. For DC circuits, the clearance requirements shall generally be the same as those for AC circuits having the same nominal voltage to ground.

Direct current systems should meet the same requirements for availability, reliability, maintenance, and safety as AC power systems.

DC-based critical power systems are an emerging and potentially viable option for mission-critical environments, it is advisable at the present time to work closely with the designers, equipment providers, and electrical contractors who have experience in the direct current applications.

Designers, operators and others involved in DC systems should refer to the appropriate standards such as:

- Over current protection devices (OCPD) and disconnect devices for DC power systems will need further investigation for higher voltage DC systems. AC-rated devices cannot automatically be used on a DC power system at the same rated voltage and current.
- The established 2:1 protection coordination scheme for DC fuses is not readily applicable since data centers typically utilize circuit breaker technology.
- Transients for other than 48 VDC systems are not well described.
- Battery disconnect or other DC disconnect usage at voltages above 50 VDC is not well established.
- Disconnects may not be required, depending upon local requirements. 2-pole or even 3-pole disconnects may be required, perhaps at multiple points within a system. Interrupting capacity and withstand ratings may need to be selectively coordinated.
- Conductor sizing regulations for DC are not well established; sizing per AC code requirements may be inappropriate for DC conductors.
- If the rectifier technology is switched mode power supply (SMPS), it may require use of electrical noise control via power line filters (possibly connected to the return or DC equipment ground conductor) and might create additional audible noise from cooling fans.
- Rectifier operation modes at the higher voltages, such as 380 VDC, may need verification for AC input power factor correction, load sharing, paralleling, voltage sensing, and current limitation.
- The DC power distribution topology is historically bus or cabling. Further, there may also be a need for an underfloor topology. Distribution (such as rigid bus bar) withstand under extreme fault current conditions (such as a direct short across the batteries [if batteries are used]) will probably vary considerably from that for telecommunications 48 VDC system.
- Voltage drop is a concern, especially if DC is run for distances longer than a few meters. Guidelines for calculating voltage drop can be found in IEEE 946.

- For metallic battery racks, determine the local authority requirements for sizing the bonding conductor. 13.3 mm2 (6 AWG), which is typically specified for telecommunications applications below 50 VDC, may not be acceptable for higher voltages (e.g., 380 VDC).
- Consult with the local authority regarding limitations for the location of centralized DC power systems in the computer room.
- Determine the grounding methods required by the ITE. The 380 VDC system might be operated as a positive grounded system (similar to the 48 VDC telecommunications system) as a negative grounded system (similar to the 24 VDC telecommunications system) or as an ungrounded system (similar to higher voltage UPS systems).

6.12. Computer Room Equipment Power Distribution

The distribution to the critical loads must be exactly mapped to the redundancy of those loads and the cord and circuit diversity that they require.

The upstream systems must be able to deliver the source diversity to the computer room circuiting under normal maintenance and failure modes of operation as prescribed in the Class performance descriptions.

At this level, the electrical system is downstream from the PDU or transformer level, and this system is typically operating at the utilization voltage level for the ITE or critical equipment. This distribution can be present in several forms such as bus way or individual circuits.

For high-density loads, a given design may separate the panel board branch circuit sections of the PDU into cabinets near the critical loads. This system may have either single or dual-inputs and is commonly known as a remote power panel (RPP). RPPs reduce installation labor and reduce the cable and circuit length to the load.

Distribution to the loads may be either overhead or underfloor. Underfloor power distribution is most commonly accomplished using liquid tight flexible metallic conduit, although in some jurisdictions, hard conduit may be required. IEEE 1100 recommends hard steel conduit with the Rwanda standards board approved insulated grounding wire for added safety, performance, and protection.

Power distribution should be located under the cold aisle and telecommunications cabling located under the hot aisle to minimize air blockages.

Overhead power distribution can frequently eliminate the cost of conduits (with the addition of cable tray or bus way) and can have the added benefit of eliminating cables as a cause of underfloor air blockage.

Overhead cabling, if used, should be planned to minimize blockage of airflow above the floor.

For future and high-density loads, traditional 20A circuits may not be enough for power strips in the IT cabinets, and in some installations, 3-phase power strips with appropriately sized circuit capacity may be required to support the load. To accommodate future power requirements, installation of three-phase cabling at a capacity of up to 50 or 60 A or at utilization voltages of around 400 VAC is recommended even if such power is not immediately required.

6.13. Load Management

Unused or abandoned cables not terminated at equipment or marked for future use shall be removed.

Load connection best practices for facilities are listed below:

- Twist-lock receptacles and plugs for all underfloor or overhead receptacles should be provided.
- Receptacles on the power strip within a cabinet or rack do not require locking-type receptacles.
- Some systems use a plug-in bus way system installed adjacent to the loads or cabinets. The bus way's design should allow new load taps to be installed while the bus is energized without creating any arcing or transients.

Locking receptacles should be used for connecting the input cords of the power strips and for larger ITE. For in-rack loads using straight-blade cords, anti-pullout tie downs should be used where cords plug into the power strips.

Power distribution cables originating from different source PDUs, RPPs, electrical phases, taps off the same PDU, or electrical panels should be clearly identified as to their source, phase, and load capacity.

If permitted or required by the Rwanda Standards Board, cables from different sources may have different color jackets and connectors.

Branch circuit overload protection devices should be de-rated by a design factor of 20% (e.g., be at least 25% larger than their connected ITE load) to ensure that circuits are not operating at the edge of their circuit breaker trip rating.

- For equipment and systems that require power feeds from more than one power source to provide availability (typically Class F3 or Class F4), the power cords should be split across two of the cabinet power strips. To provide availability for single-corded equipment and for equipment that utilizes multiple cords but is not power feed-fault tolerant, these items should be plugged into a rack-mounted power strip or receptacle fed by a larger upstream, automatic static transfer switch (ASTS), or some other point-of use ASTS.
- Equipment with three power cords should have one of the three plugs on a rack-mounted power strip or receptacle fed by a static transfer switch or point-of-use switch. The other two plugs should be plugged into receptacles supported by different PDUs. These other two receptacles should not be on static transfer switches.
- Power cords should be mechanically connected at the point of entry to the rack or a piece of ITE. This may be accomplished via the ITE manufacturer's cable tie downs, hook-and-eye straps, cable ties, or similar attachment that allow for the secure attachment of the power cable to the enclosure and would prevent the accidental disconnection or damage of cable. Provide slack loop, as appropriate, in the tie down to allow for some cable movement.

- UPS sources should be paired or grouped together and represented by individual panels or remote power panels for ease and clarity.
- Plugs and rack-mounted power strips should be located where thermos graphic testing can observe all critical connections and over-current protection devices while operating.

- Cable management should be used.

- Disruption to future operations should be minimized by locating distribution equipment to permit expansion and servicing with minimal disruption.

- All power receptacles and junction boxes should be labeled with the PDU/RPP/panel number and circuit breaker number. Each PDU/RPP/panel circuit breaker should be labeled with the name of the cabinet or rack, or the grid coordinates of the equipment that it supports.

- All power receptacles and junction boxes installed under an access floor system should be attached to the access floor or the structural floor per manufacturer's recommendations when required by the Rwanda Standards Board.

- Receptacles and junction boxes should be mounted on a channel to keep raceways and equipment above the subfloor. This attachment may be made mechanically via concrete anchors, brackets attached to the access floor pedestals, or even industrial hook-and-loop NRTL-listed fasteners, which make an excellent, dust-free alternative to drilling in an anchor or adhesives. Additionally, boxes and other electrical devices should be mounted at least 25 mm (1 in) above the subfloor to prevent water intrusion in the event of a leak.

- Every computer room, entrance room, access provider room, and service provider room circuit should be labeled at the receptacle with the PDU or panel board identifier and circuit breaker number.

- Receptacles on UPS power should be color coded, have a color-coded label, or have a colored dot to indicate the specific upstream UPS power source.

- Supply circuits and interconnecting cables identified for future use should be marked with a tag of enough durability to withstand the environment involved.

6.14. Automation and Control, Monitoring

Monitoring is defined as the telemetry and ability to view what is going on within a given system. In some cases, monitoring systems can integrate and manage alarm and trouble signals from the monitored systems.
For the purposes of this section, control is defined as any device that directly regulates a change in state in a given system. Controls are an active system, and may be either:

- Manually initiated and automatically operated based on human input or decision

- Automatically initiated and operated based on a predetermined script or response to a failure or external change of state.

Operators should be able to respond to failures or to determine the loading or operation of their systems.

Monitoring is mandatory for all Classes with increasing levels of observation scope and granularity with increasing Class.

As Class level increases, monitoring increases by replacing summary alarms with individual alarm points and by presenting systems virtually for the system operators.
For Class F4 systems, a virtual single line, which clearly shows system loading and power flow, should be provided. In some instances, a simulator is also provided where changes of state can be tried in a virtual setting to see the outcome prior to employing them in the live, working environment.

Electrical systems should disclose all changes in state, alarms, pre-alarms and positions of all breakers, and switches as well as general system information.

Power quality monitoring (PQM) for data centers is recommended since IT systems may be sensitive to power quality, transients, harmonics, and other types of waveform disruption.

Power monitoring is also vital as waveform disturbances offer a precise definition of experienced failures and outages. When addressing power system monitoring, there are three facets of observation:

- Power levels noting voltage, current, and frequency
- Harmonic content
- Waveform imaging and capture

Power monitoring offers a sampling of the power system's quality in a manner like a mechanical system's monitoring of temperature or water chemistry to the chiller/cooling system.

PQM should be located at portions of the electrical system that offer a complete view of the vital locations where power is being converted.

No favor is made over switchgear-integrated monitoring or stand-alone systems. The key element is how they are used.

6.15. Bonding, Grounding, Lightning Protection, and Surge Suppression

The comprehensive electrical protection required for the critical facility is achieved using a system approach to integrate lightning protection, overvoltage and surge suppression, bonding and grounding.

Grounding is addressed in three sections: electrical distribution, PDU, and within the computer room.
Electrical system grounding is consistently misunderstood and, for most facilities, not adequately maintained, changed or integrated to the ITE loads that it serves.

It is the intent of this standard to provide a bonding and grounding system that substantially equalizes any no transient potential differences so that all the enclosures, raceways, and all bonded metal found in the computer room are effectively at the same ground potential (substantially equalized).

Bonding and grounding of data centers relates most specifically to maintaining the facility's common electrical bonding and grounding system along with any desired supplementary bonding and grounding for the ITE.

Bonding and grounding also address vital issues such as harmonic current management and fault current mitigation.

Bonding and grounding also integrate voltage transient suppression by the application of SPD (surge protection device) systems as well as lightning protection systems.

The bonding and grounding system are one of the few electrical systems completely systemic to the entire critical facility.

If properly organized and installed, the ground system is essentially a radial system from the electrical service entrance. There are a few subtleties for critical facilities that vary from other buildings.

Where generators are not treated as separately derived sources, neutrals and grounds are routed with the associated phase wiring and carried back (without being switched) to the main service and terminated on the main service's neutral and ground buses.

Where generators are treated as separately derived sources, grounds are carried back to the main service and terminated on the main services ground bus.

Data center bonding and grounding addresses all bonding and grounding work within the critical environment.

These systems include:

- The separately derived system at the PDU
- Ground path to the load
- Critical environment grounding—supplementary at the ITE
- ITE bonding and grounding
- Personal grounding and static discharge.

Bonding and grounding for a data center involve several entities such as:

- A common grounding electrode system (GES) for the building, involving the intersystem bonding of a:
  - Grounding electrode system for the electrical power
  - Grounding electrode system for the lightning protection system (LPS)
  - Grounding electrode system for the telecommunications service provider cables and protectors
- Grounding electrode conductors for solidly grounding each power service entrance
- Grounding electrode conductors for solidly grounding each separately derived power source such as an engine-generator for standby power
- Grounding electrode conductors for solidly grounding each telecommunications service entrance

Bonding and grounding infrastructure for telecommunications utilizing components such as the BCT, TMGB, TBB, TGB, and GE as described in TIA-607-B

- Equipment grounding conductor for power distribution from the service/source to the load
- Structural metal
- Grounding conductors such as the down conductors for an LPS and SPDs
- The common bonding network (CBN) within the building
- Supplemental bonding and grounding structures for electronic equipment such as:
  - Mesh-bonding network (mesh-BN)
  - Isolated bonding network (IBN)
  - Supplementary bonding grid.

The common bonding network (CBN) is the set of metallic components that are intentionally or incidentally interconnected to form the bonding network (a mesh) in a building. The CBN always has a mesh topology and connects to the grounding electrode system via one or more grounding conductors.

Serving power systems and electronic equipment bonding and grounding primarily involves the serving power source and the power distribution to the IT and other electronic equipment.

This primary level of bonding and grounding is required to be in accordance with the NRTL product safety listing of the power system and the electronic equipment (load).

The entities of concern are the grounding electrode conductor (system) and equipment grounding (bonding) conductor (or green wire).

These dedicated circuit conductors are required for the safe operation of the equipment, including any ground faults.

In some instances, equipment may be designed as “double insulated,” whereby the NRTL requirements for the equipment grounding conductor may be eliminated (e.g., a two-prong plug or receptacle). Although data center electrical and electronic equipment may be considered “grounded” according to its NRTL requirements, supplementary bonding and grounding are recommended.

High-resistance/impedance grounding (HRG) systems can be used in lieu of solidly grounded systems. HRGs are typically designed to limit a ground fault current to 10 Amps or less. The advantages of using HRGs are:

- Safety enhancements because of mitigation of phase-to-ground fault currents
- Operational enhancements because of reduction of ground fault current trips
- Reduced cost because of the elimination of four-wire feeders

The HRGS (High Resistance Grounding System) are installed at the service transformer. They function down to the first separately derived source in the distribution system. Where used for ITE installations, consideration should be given to any impact on the resistance/impedance of the grounding systems.

HRGs (High Resistance Grounding System) may influence the level of electrical noise versus earth ground at higher frequencies such as for filters. The impact may occur because of reactance of the resistance/impedance devices such as an inductor or wire-wound resistor. Inductive/reactance grounded power systems are not recommended for low-voltage systems.

Check with the UPS system manufacturer if it is not connected to solidly ground neutral sources as they typically will provide “neutral” grounding kits for their UPSs.

The following considerations are important for understanding the complexities of bonding and grounding for a data center:

- All dead metal objects within the data center should be grounded (this includes empty cabinets and racks and ladder racks).

- Equipotential grounding becomes increasingly difficult across an expanse such as a building or larger data center.

- Distributed grounding (within a building or complex) cannot accomplish equipotential grounding.
- A dedicated and separate ground for data center equipment is NOT recommended and is entirely likely to be an electrical safety violation.

- Especially where multiple services (power and communications) enter the building at separated locations, a buried ground ring is recommended to provide equipotential bonding. Where multiple power service entrances are involved, the ground ring conductor should be sized at 107 mm2 (4/0 AWG) minimum bare copper.

- Where equipment is designed for double insulation, grounding that equipment may be a secondary concern (pending its product safety listing requirements and electromagnetic emissions compliance).

- Any electrical grounding infrastructure placed for the electrical power system should not replace the separate bonding and grounding infrastructure for telecommunications (TIA-607- B).

- The infrastructure described in TIA-607-B is better placed in the central portions of the building and away from exterior locations where lightning current activity is more likely.

- Supplementary bonding and grounding of data center equipment is recommended (this is over and above bonding and grounding of the serving power distribution) as it:
  - Provides for more locally grounded equipment
  - Maintains a level of grounding even if the serving power circuit grounding is interrupted
  - Provides dispersed path(s) for ESD currents to follow

- Provides conductive paths among interconnected equipment where common configurations include grids and planes.

- Further reduce the levels of inter-unit common-mode electrical noise on signal and power cabling, Provide a lower resistance and lower impedance inter-unit ground reference

- Reduce damage to inter-unit equipment during power fault and surge events
  - An isolated bonding network (IBN) may be utilized for certain telecommunications applications

- The electronic equipment system is only grounded via a single point connection window.

- This concept has been used by the telecommunications service providers (primarily for DC powered systems but may also be applicable for AC powered systems).

- Data circuits between data centers and different floors should be decoupled to prevent issues related to unwanted electrical transients. Fiber optic circuits and links are ideal for decoupling. Some types of circuits may utilize suitable transformer isolation for decoupling.

7.15.1. Lightning Protection

Lightning events can cause fires, damage to buildings, and breakdowns of electrical, telephone, and computer installations, which may result in considerable losses in operational revenues and increased customer dissatisfaction.

Damage results from electromagnetic fields from the lightning strike, voltage differentials in ground systems, and structural damage from ohmic heating or mechanical forces. This damage can be attributed to insufficient direct strike protection;

Deficient grounding; bonding and shielding techniques for the susceptibility level of the installed electronic equipment systems; and deficient selection and installation of surge protective devices.

Depending on the geographical location for the data center, there may be local guides available specific to the country or region, such as the risk analysis guide provided in fire protection by Rwanda standard board , which takes into account geographical location and building construction among other factors in determining the suitability of a lightning protection system.

If a lightning protection system is installed, it shall be bonded to the building grounding system as required by the prevailing standards and the local authority and as required for maximum equipment protection.

For some locations, lightning protection is required by local authority for basic building safety and protection.

If a lightning protection system is present, the lightning protection system shall be:

- Applied as a comprehensive system
- Integrated with properly sized and installed SPDs(Surge Protection Device)
- Implemented to cover all systems and buildings serving the critical environment.

Where protection from lightning-caused voltage fluctuations and transients is to be provided for protection of critical facilities, installation should be in accordance with industry recognized standards as per the local regulations authority.

Surge Suppression/Surge Protective Devices (SPDs)

Surge suppression, as used in this section, encompasses all surge protective devices or SPDs.

Within surge suppression for low voltage AC power circuits, the term surge protective device (SPD) has replaced the term transient voltage surge suppression (TVSS) with TVSS no longer in use.

Surges and transient power anomalies are potentially destructive electrical disturbances with the most damaging being overvoltage occurrences and short duration events.

High-energy transient power anomalies can arise from inductive load switching or other events within the power system or from capacitive and inductive coupling from environmental events such as nearby lightning activity.

Environmental and inductive power anomalies are wideband occurrences with a frequency range from close to DC to well into the RF high-frequency spectrum. It is critical that each point-of-entry (e.g., power, HVAC, telephone, LAN, signal/control, RF) into the equipment area be protected against these anomalies.

This protection is essential to reduce the risk of personal injury, physical equipment damage, and loss of operations. Although lightning can cause the most visible damage, it is not the predominant cause of transient voltages.

Sources of transient voltage include, but are not limited to:
Power Company switching

- Generator transfer
- Shared commercial feeders with poor line regulation
- Load switching
- Fault currents
- HVAC units
- Heating elements
- Power tools
- Electric motors
- Fluorescent lights.

SPDs and large-scale surge suppression are an integral part of the high voltage lightning protection for a facility.

Additional low voltage transient mitigation is typical for an information technology facility to protect against internally generated transient events.

For lower Classes of data centers, SPDs are located at the utility entrance with transients not being addressed further downstream unless the site demands -for-it. For higher reliability Classes, SPDs are prevalent throughout the power system. As the data center Class increases, SPDs may be found in the following locations:

- Utility service entrances
- Generator buses
- UPS inputs
- UPS outputs
- UPS power distribution switchboards
- PDUs and critical power distribution panels

The installation of surge protective devices is a requirement for all data centers Class F1 and higher. A lack of surge protective devices would result in a Class F0 rating.

SPDs shall not be mounted inside the switchgear (unless specifically designed, manufactured, NRTL listed, and properly installed for integral installation) and shall be installed with minimum lead lengths and separation of Input/output wiring in order to perform properly.

System	Class F0	Class F1	Class F2	Class F3	Class F4
Utilities Service Entrance	Recommended	Required	Required	Required	Required
Generator Buses	Recommended	Required	Required	Required	Required
UPS Rectifier inputs	Optional	Recommended	Required	Required	Required
UPS Static Bypass inputs	Optional	Recommended	Required	Required	Required
UPS Maintenance Bypass inputs	Optional	Recommended	Recommended	Required	Required
UPS Outputs	Optional	Optional	Optional	Optional	Optional
Critical switchboards (downstream from UPS)	Optional	Optional	Optional	Optional	Optional
PDU or RPP	Optional	Optional	Optional	Optional	Optional

6.16. Building Ground (Electrode) Ring

A building ground electrode ring shall be installed for facilities where a lightning protection system is installed or where there are multiple power service entrance locations along the periphery of the facility.

As required by local codes and standards, the ground ring shall be bonded to structural metal at every other column or more often. Concrete-encased electrodes (also known as Ufer electrodes) shall be used in new construction as a method of supplementing the grounding electrode system.

Concrete-encased electrodes improve the effectiveness of the grounding electrode system because of concrete having hygroscopic properties and by providing a much larger surface area in direct contact with the surrounding soil:

- Concrete-encased electrodes shall be encased by at least 51 mm (2 in) of concrete, located within and near the bottom of a concrete foundation or footing that is in direct contact with the earth.

- Concrete-encased electrodes shall be at least 6 m (19.7 ft) of bare copper conductor not smaller than 21.1 mm2 (4 AWG) or at least 6 m (19.7 ft) of one or more bare or zinc galvanized or other conductive coated steel reinforcing bars or rods at least 12.7 mm (0.5 in) in diameter.

- Concrete-encased electrodes shall be bonded to any other grounding electrode system at the site.

- This building grounding system shall be directly bonded to all major power distribution equipment, including all switchgear, generators, UPS systems, and transformers, as well as to the telecommunications systems and lightning protection system. The facility shall possess a building electrical main ground bus (MGB) where all the large-load feeder facility grounds terminate. This is the location, coupled with the telecommunications main grounding bus bar (TMGB), where the grounding system can be validated for both continuity and impedance.

A building ground electrode ring should be installed for all facilities.

Single or triplex ground rod fields as the only earthling vehicle are not adequate for a critical facility.
The direct burial connections should meet appropriate electrical testing requirements as set out in the applicable standards and codes to ensure durability.

Designs may vary according to the site parameters such as available real estate, earth resistivity, frost line level, and the depth of the water table.

Ground bus bars should be placed to facilitate bonding and visual inspection.

The ground ring should be 107 mm2 (4/0 AWG) minimum bare copper wire buried a minimum 800 mm (30 in) deep and a minimum 1 m (3 ft.) from the building wall. For larger sizes, stranded conductors are recommended.

Ground rings encircling buildings should be installed just beyond the roof drip line.

The size of the ground ring conductor is recommended to be the same as the largest size required by the Rwanda Standards Board for a grounding electrode conductor to promote the accomplishment of intersystem bonding.

The ground rods should be connected to the ground ring. Typical ground rods are 19 mm by 3 m (3/4 in by 10 ft) copper-clad steel ground rods spaced every 6 to 12 m (20 to 40 ft) along the perimeter ground loop.

Test wells for the building ground electrode ring should be provided at the four corners of the loop.

The common grounding electrode system should not exceed 5 ohms to true earth ground as measured by the fall of potential method (IEEE 81). As noted in the NEC, IEEE 1100, and IEEE142, common bonding of different systems plays a crucial role along with grounding.

Supplementary bonding and grounding methods are those provided in addition to the bonding and grounding measures typically required by the applicable electrical safety codes and product safety standards.

Supplementary bonding and grounding methods are intended to improve facility and equipment performance related to bonding and grounding. Examples of supplementary bonding and grounding entities may include metallic raceways, racks and cable trays; under the raised floor or above the cabinet and rack metallic grid work; metal plates and metal sheets; multiple bonding conductors from equipment to a grounding/bonding structure, etc.

An integral part of the bonding and grounding network in the access floor area or any critical environment is the grounding of the IT support equipment and static discharge management during ongoing operations. This includes the connection of a cabinet of ITE chassis to the mesh-BN, connections between various IT systems and cabinets, and personal grounding checks and static charge dissipation.

Rack Connections to the Mesh-BN It is common for cabinets to be physically connected for structural integrity, and they also may be logically, virtually, or network connected, acting as an integral platform.

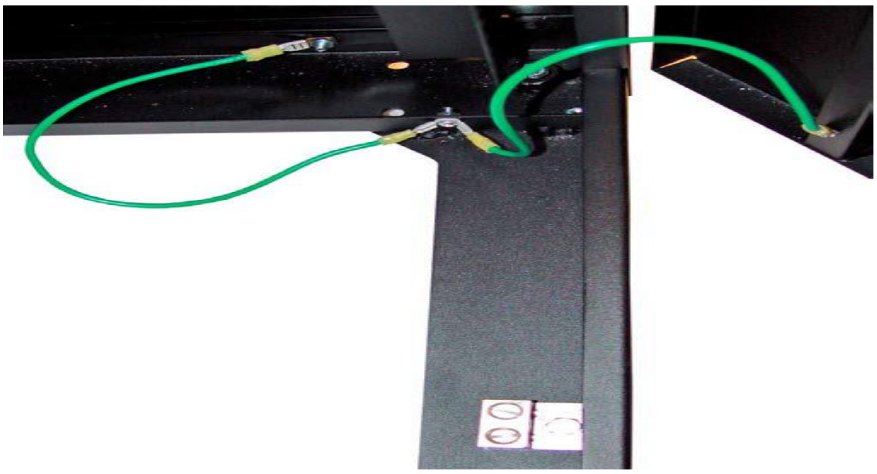
This is achieved by the manufacturer assembling the cabinet or rack in such a way that there is electrical continuity throughout its structural members. For welded racks, the welded construction serves as the method of bonding the structural members of the rack together.
All adjacent cabinets and systems should be bonded in order to form grounding continuity throughout the rack structure itself.

Electrical continuity cannot be assumed using a nut and bolt connections used to build or stabilize equipment cabinets and racks.

Bolts, nuts, and screws used for rack assembly may not be specifically designed for grounding purposes, and unless grounding bonding jumpers are installed, do not assume electrical continuity for the cabinet lineup.

Most cabinets and racks are painted, and as paint is nonconductive, this negates any attempt to accomplish desired grounding. Therefore, paint or cabinet coating must be removed in the bonding area for a proper bond to be formed.

Most power is routed over the top or bottom of the rack. Without a reliable bond of all four sides of the rack, a safety hazard exists from potential contact with live feeds.



6.16.1. Personal Grounding and Static Discharge

Electrostatic discharge (ESD) is the spontaneous transfer of electrostatic charge. The charge flows through a spark (static discharge) between two bodies at different electrostatic potentials as they approach each other.
Electrostatic discharge (ESD) may cause permanent damage or intermittent malfunction of networking hardware.

Anyone that touches network equipment or network cabling becomes a potential source of ESD as it relates to telecommunications equipment.

Network cabling that has been installed but not connected may become charged when these cables are un-spooled and slid over carpet or other surface that contributes to the buildup of ESD.

The charged cabling may become a source of ESD to the telecommunications equipment to which it connects. Charged cabling should be discharged to an earth ground prior to connection to network equipment.

ESD charges may remain for some time, especially in dry conditions.

Factors affecting ESD charge retention include:

- Cable design
- Dielectric materials
- Humidity
- Installation practices

Low humidity and static-generating building materials are the primary causes of ESD.

There should be no significant ESD charge retention difference between types of telecommunication cabling as all cables have a nearly identical ability to acquire a static charge.

It is important to follow all ESD specifications and guidelines provided by the applicable network equipment manufacturer.

Mitigation techniques, such as anti-static flooring and humidity control are important for critical installations.

The use of static discharge wrist straps when working on or installing network or computer hardware is specified in most manufacturers' installation guidelines.

Wrist strap ports should be attached to the rack by a means that ensures electrical continuity to ground.

Pedestrian static discharge mats may be required for certain access floor environments or spaces with standard resistance flooring.

6.17. Labeling and Signage

Labeling shall be integrated to the individual systems and shall provide the operator an understanding of system status under cursory examination. Labeling works hand in hand with the graphical user interface (GUI) and the physical organization of the equipment and systems themselves.

The GUI is typically a visual dashboard for the complete operation of the system. Information on the GUI typically include a color -coded power flow diagram, electrical performance, electrical characteristics, and alarm status.

Equipment may have a mimic bus display, indicating how power flows through the system and how the individual breaks are connected.

It may also be color-coded for the critical, utility, and generator power systems.

A critical power system with four distinct UPS systems could be labeled UPS-A, UPS-B, UPS-C, and UPS-D. Such a system could bear a unique color-coding where the system A might be red, the B system might be blue, the C system might be green, and the D system might be yellow. This color-coding would be carried all the way through the system.

All branch and data center circuits shall be marked with their individual circuit designations.

Conduit systems and junction boxes shall also be color-coded by system, and power feeders may also bear their specific designation (e.g., UPS A Input).

Conduit color-coding may be via a label, cladding, or painting.

Circuits that are on the output of an UPS or that support critical loads should be color-coded to readily distinguish them from non-critical circuits. This color-coding may be in the form of colored self-adhesive labels or nameplates.

Equipment labeling should possess all critical information concerning the system to which it is affixed. This information should include:

- Equipment nomenclature and designation (e.g., Generator AH54)
- System capacity rating in kVA and kW (e.g., 750 kVA/675 kW)
- Input voltage, phasing, and connection (e.g., 480V, 3-phase, 3-wire)
- Output voltage, phasing, and connection (e.g., 480V, 3-phase, 3-wire)
- Power factor (e.g., 0.9 lagging)
- System or switchboard serving this piece of equipment
- System, switchboard, or load that is being served by this equipment

7. MECHANICAL AND COOLING SYSTEM

Datacenters are critical, energy-hungry infrastructures that operate around the clock. They provide computing functions that are vital to the daily operations of top economic, scientific, and technological organizations around the world. Cooling must be one of the primary concerns of a Datacenter designer.

Effective heat removal from the datacenter equipment requires attention to the direction of airflow. An important part of thermal management of air-cooled electronic equipment is air management. All HVAC systems are not compatible with all data center, so the designer should select the appropriate HVAC System for specific datacenter. It is necessary to choose appropriate HVAC (Heating-Ventilation-Air Conditioning) system and equipment used is made based on many factors. Below a list of few factors to be considered while choosing datacenter cooling,

- Room size
- Overall cooling density (watts per square meter or watts per square foot), which is established by the maximum kW load for the computer equipment used in the electrical design. Cooling load should match actual operating load as opposed to nameplate load.
- kW per cabinet or module

- Number and capacity of HVAC units required to meet load and redundancy criteria and their location in the space relative to computer equipment layout
- Room location relative to mechanical support spaces
- Room location in the building relative to outdoors
- Ceiling height
- Absence or presence of access floor
- Access floor height
- Future expansion needs
- Reliability requirements
- Available maintenance personnel
- Local climate

Provide dual cooling and heating systems utilizing down flow discharge modular cooling units for most effective systems.

Design should consider maintaining a consistent temperature and humidity to counteract the hot dry air created by your equipment.

Design should consider that equipment density is constantly rising and along with it the heat and energy loads.

Ensure that you have adequate capacity for the future power and HVAC needs of your facility and potential future expansion without disrupting the business operations.

All environmental controls should be monitored with logging, trend projection and alarm notification.

Ensure that the location of equipment is critical, and the type must provide an easy but secure access for maintenance.

Ensure that the capability in facility design to replace all pieces of equipment without affecting operations of the facility.

7.1. Air conditioners and air handlers

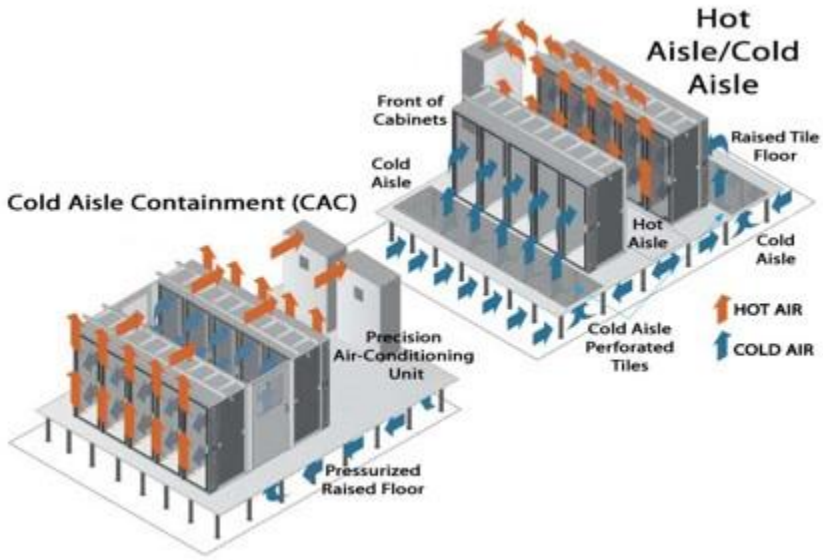
The most common types are air conditioner (AC) or computer room air handler (CRAH) units that blow cold air in the required direction to remove hot air from the surrounding area.

7.2. Hot aisle/cold aisle

The cold air (or aisle) is passed to the front of the server racks and the hot air comes out of the rear side of the racks. The main goal here is to manage the airflow in order to conserve energy and reduce cooling cost.

7.3. Hot aisle/cold aisle containment

Containment of the hot/cold aisles is done mainly to separate the cold and hot air within the room and remove hot air from cabinets. The image below shows detailed airflow movement of cold and hot containment individually.



The total of all server airflows in that row represents the total airflow through the racks from the cold aisle to the hot aisle.

This is not the same as the volume of air that must be supplied to the cold aisle by the HVAC system.

The HVAC system must supply more air since the temperature difference produced by the HVAC equipment will generally be lower than the temperature rise through the electronics equipment because of bypass air waste and related mixing of supply air and return air.

HVAC systems and cooling equipment must always be selected using a holistic approach. The choice of air distribution method should never be considered without evaluating other significant factors, such as whether or not an access floor is used, the return air path, location of CRAC units or air handling equipment relative to server racks, orientation of hot/cold aisles, ceiling height, methods for humidity control, and provisions for future expansion, to name just a few.

Each choice affects the others, and the overall performance of the data center cooling system will be dictated by the entire package of decisions.

It is recommended that to design the datacenter with access floor which assist to manage the hot aisle and cold aisle.

Airflow in the typical data center consists of two flow loops:

- CRAC units (a few big fans) circulate air within the entire room.
- Servers (many little fans) circulate air between cold and hot aisles.

Each of the two airflow loops described above operates with a different temperature difference between inlet and supply. However, the energy must balance between the two; all the heat rejected from the servers must be further rejected in the CRAC unit.

The type of air delivery method through an access flooring system should be consistent.

Do not mix perforated tiles with supply air grilles as the differences in flow/pressure drop characteristics will result in an inconsistent and unpredictable performance.

Large, relatively unobstructed openings in the access floor can have significant adverse effects on the underfloor pressurization and should be avoided as the larger the opening, the smaller the pressure drop corresponding to a cubic meters or feet per minute

Air takes the path of least resistance; large openings will starve the perforated floor tiles. Large means any opening that is large relative to a single perforation in an access floor tile. Many (relatively) small openings can begin to look to the HVAC system like a few very large openings.

An access floor system provides a flexible method of delivering cooling to data centers, allowing for numerous configurations.

Perforated panels can readily be moved to accommodate high heat load areas.

Floor height should be selected based on the combined needs for airflow, power distribution, network/communications cabling, and chilled water distribution, if used.

Access floor heights greater than 900 mm (36 in) introduce additional cost to the flooring system, may require special considerations for access and safety, and do not significantly enhance the uniformity of air distribution below power densities of 1350 W/m2 (125 W/f2).

For data centers with power densities in the 1610 to 2150 W/m2 (150 to 200 W/f2) range, a 1060 mm (42 in) access floor depth should be considered.

Chilled air should always be delivered into the cold aisle in front of the cabinets and not be delivered directly into the bottom of the cabinet. There are three main reasons for this:

- Openings provided below the racks for this purpose will generally be large compared to the tile perforations.
- Some air will bypass out through the back of the rack into the hot aisle.
- Air supplied directly into the bottom of a cabinet may be significantly below the minimum temperature.
- CRAC unit discharge air temperature is typically in the 13 to 16 °C (55 to 60 °F) range, and 80% to 90% RH at that temperature.

- With Underfloor distribution, the air coming out of the perforated tiles will usually be below 20 °C (68 °F).

Room temperature measurement points should be selected in conformance to ASHRAE Thermal Guidelines:

Temperature measurement sensors should be regularly calibrated.

A significant difficulty with temperature and humidity measurement point locations is the physical installation in meaningful locations.

Sensors typically must be mounted on a fixed surface, making the mid-aisle 1500 mm (60 in) above floor locations impractical for permanently installed devices.

Temperature and humidity sensors furnished with CRAC units are factory installed in the units at their inlet and do not indicate the conditions of the air at the computer equipment inlets.

Temperature-measuring points should ideally mimic the equipment inlet conditions since these conditions define the equipment comfort.

Floor plenums should be as airtight as possible relative to adjacent spaces and cleaned prior to being put into use.

Overhead ductwork must be closely coordinated with lighting, sprinklers, and power or network cabling in data centers where these utilities are not located below an access floor.

Overhead ducts wider than 1200 mm (48 in) will require sprinkler heads to be located below the ductwork.

Cabinets and racks shall be arranged in rows with fronts of cabinets/racks facing each other in a row to create hot and cold aisles.

Equipment should be placed in cabinets and racks with cold air intake at the front of the cabinet or rack and hot air exhaust out the back, top, or both.

Reversing the equipment in the rack will disrupt the proper functioning of hot and cold aisles.

Blank panels should be installed in unused cabinet and rack spaces to improve the functioning of hot and cold aisles.

When placed on an access floor, cabinets and racks shall be arranged to permit tiles in the front and rear of the cabinets and racks to be lifted.

Cabinets should be aligned with either the front or rear edge along the edge of the floor tile per TIA-942-A.

Cabinet size, location for air entry, location for cable entries, and access to front and rear should be planned for consistency according to ETSI EN 300-019.

CRAC units should be in the hot aisle path when the return air path is the free space in the room.

Return air should be positioned to capture the highest heat concentration such as return air intakes directly over the hot aisles or directly over equipment producing the highest heat.

Capturing the heat with return grilles and not entraining it in the supply air should be the goal of return and supply layouts.

When using a return air system to reduce recirculation, supply air temperature must be controlled to very near the lowest acceptable equipment inlet temperature.

A ceiling height of at least 3 m (10 ft.) above the access floor will allow for an effective hot air area above cabinets and racks and optimize the return air path. Rooms with high-density cooling loads should consider ceilings higher than 3 m (10 ft.).

The cold aisle plenum space should remain unobstructed by raceways in conformance to TIA-942-A.

Floor tile cutouts for cable egress to cabinets and damping around cables should conform to TIA-942-A.

When overhead cable systems are used in lieu of or in addition to underfloor cabling, placement and grouping of cable should be planned to minimize the effects on return air.

Obstructions in the return air path could contribute to higher levels of hot air recirculation to the cold aisles, depending on the configuration of the cable system relative to the rack layout.

HVAC availability and redundant power access should conform to the requirements of the Class that best satisfies the reliability goals of the enterprise.

Providing CRAC units and other mechanical cooling equipment with dual power sources to ensure continuous operation if one source of power is lost is to be considered for Class F3 and Class F4 but is not mandatory under the requirements of this standard and is not required for Class F2 or lower facilities.

8. FIRE PROTECTION

Data centers face many challenges from managing complexity to improving energy efficiency and meeting fire safety, security and business regulatory requirements. Human failure (e.g. non-observance of fire protection regulation) or technical reasons can lead to a fire incident.

It is important to have a fire-suppression system which is specifically designed for Datacenter to maintain the high uptime and maximum availability and get maximum protection. A comprehensive fire safety system is mandatory to ensure business continuity. High availability can only be achieved if all relevant influencing factors are planned, implemented and put into effect in the company in a coordinated and consistent way.

Appropriate incident response would also prevent or contain the risk due to the fire and assist to avail the system.

So the data centers have to be designed, implemented and operated in such a way that a high level of availability can be guaranteed in case of a fire.

The goals of fire protection are to efficiently protect people, assets, data and the environment from the dangers and effects of fire, and to minimize material damages, loss of data, operational interruptions and the consequent loss of business.

Fire risks result basically from the probability of occurrence and the effect caused by fire.

. There are four major reasons why there is a potential risk of fire in a data center:

- Heavy power load:
  Heavy power loads or a defective piece of equipment can very quickly lead to a short circuit or overheating.

- Electrical fire risk:
  Constant ignition source (electricity); and combustible materials such as plastics in printed circuit boards.

- Infrastructure:
  Extensive cabling; particularly below raised floors.

- Ventilation:
  Comprehensive air -cooling, resulting in a higher air exchange, increases risk of spreading the fire.

The objective of fire prevention in data centers is to minimize or eliminate the use of combustible materials.

The basic design elements of fire protection are:

- Fire detection
  Smoke, heat, and early warning detectors connected to an alarm and monitoring panel.

- Fire alarm system
  A system, including the fire detection systems, with a means to automatically send an alarm to the supervisor and trouble signals to a central station, security center, fire department, or other approved, constantly attended location, and warn occupants of the presence of smoke, heat, or fire using audible or visual alarms.

- Fire suppression
  Extinguishing systems to protect the data processing equipment.

8.1. Fire detection

Fire detection system detect and alert early and guarantee the protection of the datacenter from fire and relevant fire safety controls and measures helps to take necessary precautions and avoid any incident.

The fire detection system should include an early warning smoke detection system and a water leak protection system.

The sprinkler system should have an alternate water source to prevent a single point of failure and to allow maintenance.

Local codes may sometimes require that the suppression agent used below the access floor must be identical to the method used above the floor for the rest of the space or building.

If the entire facility is not protected with a gaseous clean agent system, it is a best practice to protect space under access floors with a dedicated inert gas clean agent system or a carbon dioxide total flooding system when the under-floor space contains combustible material.

Carbon dioxide should normally not be used above the access floor in computer rooms.

Data center personnel should be trained on the use and function of the fire detection and extinguishing systems of the computer room.

Paper should be stored outside the computer room with a fire suppression system separate from the one used by the computer room.

Penetrations through the walls and floor of the room shall be sealed with a fire-resistant material that provides a fire rating at least equal to the rating of the wall and floor.

Air ducts shall be provided with automatic fire and smoke dampers where the ducts pass through fire-rated structure.

All pass-through or windows are provided in the fire-rated walls should be provided with a fire-rated shutter or fire-rated window of rating equal to the wall.
Some clean agents such as the inert gas agents will require vents in the enclosure that open during the discharge of clean agent to prevent excessive pressure build up as a result of the influx of gas in the room.

Containment aisles or “hot collars” (e.g., equipment cabinet chimneys, vertical exhaust ducts) shall not be considered as being plenums.

Materials used to construct containment structures or barriers shall meet the requirements of the local authority. For locations where the local authority does not have requirements, materials used shall have a maximum flame spread index of 50 and a maximum smoke development index of 450 as measured by UL 723(Standard for surface burning characteristics of building materials)

Hinged doors used in hot aisles shall open in the direction of egress.

Sliding doors and hinged doors shall meet the requirements of the local authority and be operable from the inside without the use of hands (e.g., “panic hardware”) as allowed by the local authority.

8.2. Fire suppression

Fire Suppression systems used within a contained aisle shall meet or exceed the minimum requirements for suppression systems used in the surrounding space and shall comply with local regulations.

Where containment is introduced into existing data centers, fire suppression systems shall be modified when necessary to meet prevailing codes and standards.

Sprinkler head placement shall meet local code requirement for clearances to walls or other obstructions to dispersal.
The system may have to be retested to verify compliance.

Sprinkler or clean agent system dispersal modification requirements may be waived if:

- Obstructions are removable prior to an emergency dispersal event, Obstruction can be removed without compromising means of egress, and removal is initiated by an automatic means of smoke detection.

- Fusible links, shrinking panels or other heat-responsive triggers shall not be used as a means for triggering removal of barriers to code-required clearances for suppression systems.

- Automatic barrier removal, if used, shall remove all obstructions for the entire suppression zone.

For gaseous fire suppression systems:

- Any additional volumetric space constructed for contained closed loop return air shall be added to the calculated total volume requirement for gaseous agent.

- The concentration of the gaseous agent, when released, shall not be less inside a contained space than it is in the area outside the contained space.

Sprinkler piping should be centered at ceiling level within the contained aisle (not above cabinets).
Sprinkler heads should be high enough that spray can reach the top of the cabinets on either side of the aisle.

Clean agent nozzles that are too close to a wall or other obstruction can result in “frosting”, thereby reducing the effectiveness of the agent, before the agent has a chance to atomize. Placement of 1.2 – 1.8 m (4 – 6 ft.) from the nearest obstruction is recommended.

Fire suppression sprinkler pipes on eight-foot centers grids can be arrayed to meet clearance requirements of most local codes for hot aisle containment and cabinet hot collar containment.

Rows will fall on an eight-tile pitch from the center of cold aisle to the center of the adjacent cold aisle.

Fire extinguishers shall be clearly visible. Each fire extinguisher shall be labeled to describe clearly the type of fire on which it should be used.

Hand-held clean agent fire extinguishers are recommended and may be required by Rwanda Standard Board . Extinguishers that use dry chemical agents are not recommended because they can damage electronic equipment.

Switchgear rooms should have clean agent handheld fire extinguishers like those used in the computer room.

Recommended Sprinkler Systems for Data Center Spaces

Area	Sprinkler system
Computer Room	Pre-action sprinkler system
Network Operations Center	Pre-action sprinkler system
Entrance Room	Pre-action sprinkler system
Office	Wet sprinkler system
Electrical Switch Gear	Pre-action sprinkler system
Battery and UPS Room	Pre-action sprinkler system
Generator Room	Pre-action sprinkler system
Chiller Room	Wet sprinkler system
Other space not listed above	Wet sprinkler system

Labeling and signage practices for the fire protection system should include the following:

- Emergency procedures should be posted on all fire alarm control panels and annunciator panels.
- Fire alarm manual stations should be clearly labeled to avoid any confusion.
- Install a cover over these manual stations to avoid accidental triggering.

Pre-action sprinkler systems should be trip tested at least once every three years.

9. DATA CENTER CABLING SYSTEMS

Structure cabling is imperative for any datacenter and it should be performed well as per the standards. Below factors needs to be considered when choosing the media,

- The quality and the life of a span must be checked
- The quantity of the cable
- Trunking capacity of the cabling
- Vendor background must be checked.

Telecommunications distribution consists of two basic elements—the distribution pathways and related spaces and the distribution cabling system.

Datacenter cabling covers two major sections, network equipment and Server equipment.
Below list are comes under networking equipment

- Voice, modem, and facsimile telecommunications service

- Switching and other network equipment
- telecommunications management connections
- Keyboard/video/mouse (KVM) connections
- Intelligent infrastructure management (IIM)
- Wide area networks (WAN)
- Local area networks (LAN)

Below list comes under server equipment

- Storage area networks (SAN)
- Wireless systems utilized in the data center including wireless LANs

Other items require cabling, other building signaling systems (building automation systems such as fire, security, power, HVAC, and EMS)

Based on the capacity requirement planning, adequate copper conductor and optical fiber capacity to the site should be provided to meet the current and projected needs of the entire site,

Multiple connectivity paths with enough capacity should be provided based on the datacenter class requirements.

Connectivity capacity to the site should be planned and implemented very carefully. If the data center is designed for minimal initial capacity with large future capacity requirements, careful consideration should be given to the amount of capacity requested to be delivered to the site by the access providers.

The selection of the primary access provider should be carefully determined to ensure that the required availability requirements can be achieved.

To have a reliability of the communication services, Data centers should have redundant circuits from the primary access provider or adding services from alternate access providers.
The reliability of the overall communications services can be further increased if the redundant circuits are serviced from separate access provider offices following diverse routes.

Redundant telecommunications service cabling is planned, telecommunications service cabling pathways should maintain a minimum separation of 20 m (66 ft.) along the entire route.

At least two diversely routed telecommunications service feeds from different access provider central offices with each access provider central office connected to multiple higher-level access provider and multiple long-distance carrier offices.

At least two diversely routed telecommunications service feeds from different access provider central offices with both access provider central offices connected to the same higher-level access provider and long-distance carrier offices.

At least two diversely routed telecommunications service feeds from one access provider central office.
One telecommunications service feed from one access provider central office.

All telecommunications service cabling to the facility should be underground with a minimum separation of 1.2 m (4 ft.) from other utilities along the entire route.

The datacenter should not have overhead telecommunications cables especially if there is only one service entrance, in such a scenario, ensure that the entrance cables are well protected from physical damage at the drop pole.

If cables drop from service poles to underground, the drop pole should provide 100 mm (4 in) rigid conduits from below grade up to the elevation where the cables are suspended to protect the entrance cables from physical damage.

Data centers should be in an area with easy sustainable connectivity to the access provider central offices.

Datacenter should be in an area where connectivity is provided by two or more access provider for Tier 3 and higher datacenter.

Redundant data centers for disaster recovery (DR) purposes should be located with enough physical separation to reduce single modes of failure (natural or manmade) - within acceptable limits for the critical data.

The two locations should be on separate distribution systems to minimize the occurrence of one outage affecting both locations.

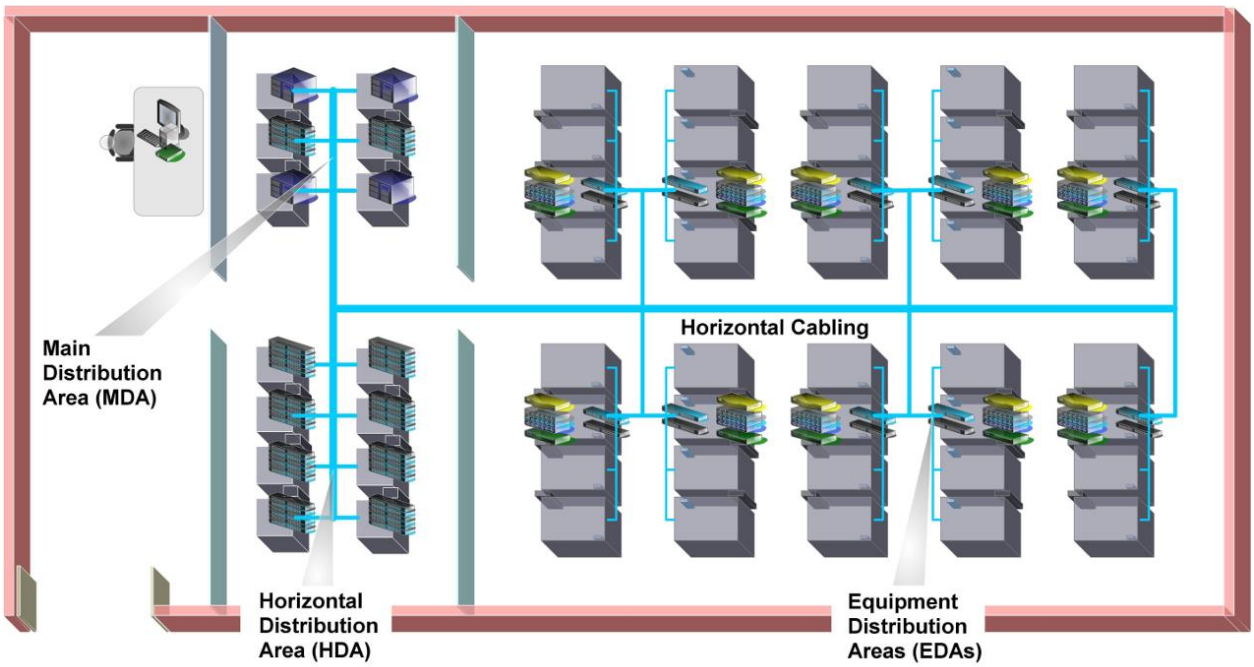
Telecommunications cabling is, therefore, one subset of telecommunications distribution and may be described as a specific system of balanced twisted-pair, unbalanced cabling (e.g., coaxial) and optical fiber cabling, equipment/patch cords, connecting hardware, and other components supplied as a single entity.

Cabling plan should reduce maintenance and relocation and expansion of additional equipment. It should ensure that cabling can be accessed for reconfiguration under the floor or overhead on cable pathway system.

9.1. Data center network cabling design

The datacenter cabling infrastructure layer contains, and the Data center spaces dedicated to supporting the telecommunications cabling system and related equipment are listed below. These spaces include:

- Entrance Room (ER)
- Main Distribution Area (MDA)
- Horizontal Distribution Area (HDA)
- Equipment Distribution Area (EDA)
- Zone distribution area (ZDA)



Data center telecommunications spaces such as the MDA and entrance room(s) shall be sized for full data center occupancy, including all anticipated expansions and planned applications.

All data center spaces for telecommunications shall have the same mechanical and electrical redundancy as the computer room(s). (Or even opposite) sides of the building.

Conduit duct banks and their associated maintenance holes and other pathways from the access provider central offices and service provider point-of-presences to the building's entrance facilities should be separated by at least 20 m (66 ft.) along their entire routes.

A conduit duct bank with appropriately placed maintenance holes that surrounds a data center and incorporates multiple building entrance facilities should be considered for the data center.

At least one conduit for replacement cables should be set aside for each internal and entrance pathway to facilitate rapid replacement of cables.

The use of inner duct, either conventional or fabric, is recommended aiding in cable management and increased utilization of available conduit space.

10.1.1. Entrance Rooms

Access providers that serve the building shall be contacted to ascertain the point(s) of entry to the property and the requirements for their telecommunications cabling, terminations, and equipment.

Class C2 and higher data centers shall have diverse entrance facilities, preferably with route diversity from the data center to different access providers.

A Class C2 data center may be served from multiple central offices and multiple service provider point-of-presences that enter the property at different locations.

The location of each building entrance facility shall be coordinated with routing of access provider pathways as well as internal pathways and shall not conflict with the location of other building facilities such as power, gas, and water.

Each building point-of-entry supporting an access provider's outside plant facilities should be located on different (or even opposite) sides of the building.

Conduit duct banks and their associated maintenance holes and other pathways from the access provider central offices and service provider point-of-presences to the building's entrance facilities should be separated by at least 20 m (66 ft.) along their entire routes.

A conduit duct bank with appropriately placed maintenance holes that surrounds a data center and incorporates multiple building entrance facilities should be considered for the data center.

At least one conduit for replacement cables should be set aside for each internal and entrance pathway to facilitate rapid replacement of cables. The use of inner duct, either conventional or fabric, is recommended aiding in cable management and increased utilization of available conduit space.

When using multiple entrance rooms, entrance rooms should be at least 20 m (66 ft) apart and be in separate fire protection zones. The two entrance rooms should not share power distribution units or air conditioning equipment.

Telecommunications entrance cabling for data centers should not be routed through a common equipment room unless cabling is segregated from common access via conduit or other means.

Entrance rooms should be outside the computer room - to improve security. However, they may be placed in the computer room or consolidated with the main distribution area if cabling distances for circuits is an issue, security is not an issue, or other security measures are used to ensure security (such as escorting and monitoring the activities of all technicians in the computer room).

10.1.2. Main Distribution Area (MDA)

The MDA includes the main cross-connect (MC), which is the central point of distribution for the data center structured cabling system. The main cross-connect is called the main distributor (MD)

Equipment typically located in the MDA includes:

- Core routers
- Core, spine, or interconnection layer LAN and SAN switches
- High-performance computing switches
- PBX or voice gateways
- T-3 (M13) multiplexers

The MDA may serve one or more IDAs, HDAs, and EDAs within the data center and one or more telecommunications rooms (TRs) located outside the computer room space to support office spaces, operations center, and other external support rooms.

All data center shall have at least one MDA. A second MDA shall be provided to meet the availability requirements of the telecommunications infrastructure (e.g., Class C4). If two MDAs are present, both shall meet all requirements of the MDA as specified in the applicable data center standard.

Access provider provisioning equipment (e.g., M13 multiplexers) may be in the MDA rather than in the entrance room to avoid the need for a second entrance room because of circuit distance restrictions.

A second MDA is recommended in Class C3 data centers. Each MDA should have fully diverse cable routes to access multiple entry points so that no single point of failure exists within the site.
When utilizing two MDAs, the MDAs should:

- Have core routers and switches distributed between the MDAs
- Distribute circuits between the two spaces
- Be in different fire protection zones
- Be served by different power distribution units and air conditioning equipment

9.1.3. Intermediate Distribution Area (IDA)

The intermediate distribution area (IDA) is the space that supports the intermediate cross-connect. The intermediate cross-connect is called the intermediate distributor.

It may be used to provide a second level cabling subsystem in data centers too large to be accommodated with only MDAs and HDAs. The IDA is optional and may include active equipment such as LAN and SAN switches.

The IDA may include the horizontal cross-connect (TIA) or zone distributor (ISO/CENELEC) for equipment areas served directly from the IDA.

The IDA may be inside the computer room but can be located in a dedicated room or a secure cage within the computer room for additional security.

9.1.4. Horizontal Distribution Area (HDA)

The HDA is used to serve equipment not supported by a horizontal cross-connect (HC) or zone distributor (ZD) in an IDA or MDA. The HDA is the distribution point for cabling to the EDAs.
Equipment typically located in the HDA includes:

- LAN switches
- SAN switches
- Keyboard/video/mouse (KVM) switches

This equipment is used to provide network connectivity to the end equipment located in the EDAs. A small data center may not require any HDAs as the entire data center may be able to be supported from the MDA. A typical data center will have several HDAs.

9.1.5. Zone Distribution Area (ZDA)

The ZDA is an optional interconnection point within the horizontal cabling located between the HDA and the EDA to allow frequent reconfiguration and added flexibility.

The consolidation point in the ZDA is called the local distribution point or LDP in CENELEC EN 50173-5 and in ISO/IEC 24764.

Horizontal cabling shall contain no more than one ZDA between the HC in the HDA and the mechanical termination in the EDA.

The zone distribution area may also serve as a zone outlet for nearby equipment in the computer room.

9.1.6. Equipment Distribution Area (EDA)

The EDA is the space allocated for end equipment, including all forms of telecommunications equipment (e.g., computer equipment, telephony equipment).

EDA areas shall not serve the purposes of an entrance room, MDA, IDA, or HDA.

9.2. Outside Plant Cabling Infrastructure

The data center site should have multiple duct banks with customer-owned maintenance holes from the property line to the data center.

The Duct banks should consist of a minimum of four 100 mm (trade size 4) or equivalent conduits or raceways. If initial plans include more than three access providers providing service to the facility, one additional 100 mm (trade size 4) or equivalent conduit or raceway should be provided for every additional access provider.

Each carrier’s cabling should be in separate, dedicated conduits or raceways. Carriers should not share pathways.

The upper surface of underground cable pathways shall be no less than 600 mm (24 in) below the surface.

Non-metallic conduits shall be encased in concrete with a minimum 17,000 kPa (2500 lb/sq in) compressible Strength where there is vehicular traffic above or a bend in the conduits.

Cabling entrance pathways shall terminate in a secure area within the data center, The telecommunications entrance pathways shall be coordinated with other electrical underground pathways (e.g., conduits) and mechanical underground piping systems (e.g., water, waste) while maintaining appropriate pathway separation from physical and operational perspectives.

In regions susceptible to iciness, the top of the conduit(s) should be below the frost line. Where this is not practical, adequate protection should be provided to ensure that conduits do not become damaged as a result of ground shifting, particularly at the point of entry into the building.

Maintenance holes and hand holes on the data center property should have locks or other means of deterring access such as nonstandard bolts.

The maintenance holes and hand holes should have intrusion detection devices connected to the building security system and monitoring of the maintenance holes and hand holes by CCTV or other means.

Redundant duct banks should have a 20 m (66 ft) separation minimum along the entire route from the property line to the facility.

Where possible; redundant maintenance holes should relate to at least 100 mm (trade size 4) or equivalent conduit or raceway.

Conduits for cable replacement should be designated and marked separately from those for additional cables.

When multiple access providers are providing service to the facility, coordination of security requirements of each individual access provider should be within the secure space.

The secure area that houses the telecommunications entrance facility (pathway termination) should preferably be in a telecommunications entrance room that is separate from the computer room.

Any pull boxes or splice boxes for data center cabling (entrance cabling or cabling between portions of the data center) that are in public spaces or shared tenant spaces should be lockable. They should also be monitored by the data center security system using either a camera or remote alarm.

Entrance to utility tunnels used for telecommunications entrance rooms and other data center cabling should be lockable. If the tunnels are used by multiple tenants or cannot be locked, they should be monitored by the data center security system using either a camera or remote alarm.

9.3. Aerial Service Pathways

Routes for aerial access pathways shall follow same provisioning guidelines from an availability and security perspective as underground data pathways.

All aerial pathways shall be properly bonded and grounded, the use of aerial cabling pathways should generally be avoided because of vulnerability to outages. Aerial cabling route selection should take into consideration several factors, including, but not limited to, terrain, soil conditions, and aesthetics, proximity to direct-buried and underground utilities, access, and weather conditions.

Customer-owned satellite dish or aerial towers should be located within the secure perimeter of the facility.

9.4. Service Providers

Data center designers shall coordinate with all Service providers to determine their requirements and to ensure that the data center's circuit, demarcation, and entrance facility requirements are provided to satisfy the access providers' specifications.

Access providers typically require the following information when planning entrance facilities:

- Address of the building
- General information concerning other uses of the building, including other tenants
- Plans with detailed drawings of telecommunications entrance conduits from the property line to the entrance rooms, including location of maintenance holes, hand holes, and pull boxes
- Assignment of conduits and inner ducts to the access provider
- Floor plans for the entrance rooms
- Assigned location of the access providers' protectors, racks, and cabinets
- Routing of cabling within entrance room (e.g., under access floor, over cabinets and racks, other)
- Expected quantity and type of circuits to be provisioned by the access provider, including any planned or foreseen additions or upgrades
- Media types and approximate distances of circuits to be provisioned by the carrier
- Service-level agreements
- Detailed schedules for the project, including date that the access provider will be able to install entrance cabling and equipment in the entrance room and required service activation date
- Requested location and interface for demarcation of each type of circuit to be provided by the access provider
- Carrier office diversity desired, preferably at least two separate access provider offices and service provider point-of-presences
- Carrier route diversity desired, preferably a minimum distance between any two routes of at least 20 m (66 ft.) along their entire routes
- Specification of pathways to be used for access provider cabling (e.g., aerial cabling allowed or all underground)
- Type and rating of fire stopping measures used at the site
- Requested service date
- Name, telephone number, and e-mail address of primary customer contact and local site contact
- Security requirements for lockable containment and cabinets
- Colocation providers may be required to provide customer name and contact details if requesting on behalf of their customers
- Space and mounting requirements for protectors and terminations of balanced twisted-pair cabling
- Quantity and dimensions of access provider's cabinets and racks or space requirements if they are to be provisioned in client cabinets and racks
- Power requirements for equipment, including receptacle types
- Access provider equipment service clearances
- Location of serving access provider central offices
- Route of access provider cabling and minimum separation between routes
- Specification on pathways used (e.g., all underground or portions of routes that are served by aerial cabling)
- Installation and service schedule

9.5. Application cabling lengths

The maximum supportable lengths in this annex are application and media dependent.

See below table in ANSI/TIA-568-C.0 for balanced twisted pair applications and table 7 in ANSI/TIA-568-C.0 for optical fiber applications.

9.5.1. T-1, E-1, T-3 and E-3 circuit lengths

Below table provides the maximum circuit lengths for T-1, T-3, E-1, and E-3 circuits with no adjustments for intermediate connections or outlets between the circuit demarcation point and the end equipment.

These calculations assume that there is no customer DSX panel between the access provider demarcation point (which may be a DSX) and the end equipment.

The access provider DSX panel is not counted in determining maximum circuit lengths.

Circuit type	Category 3	Category 5e,6 &6A	734 Type Coaxial	735 Type coaxial
T-1	159m (520 ft.)	193 m(632ft)		
CEPT-1 (E-1)	116m (380 ft.)	146m (477 ft.)	332m (1088 ft.)	148m (487 ft.)
T-3	-	-	146m (480 ft.)	75m (246 ft.)
CEPT-3 (E-3)	-	-	160m (524 ft.)	82m (268 ft.)

Repeaters can be used to extend circuits beyond the lengths specified above.

These circuit lengths should be adjusted for insertion- losses caused by a DSX panel between the access provider demarcation point (which may be a DSX panel) and the end equipment.

Maximum circuit lengths should be adjusted for insertion losses caused by intermediate connections and outlets.

Data center should have three connections in the backbone cabling, three connections in the horizontal cabling and no DSX panels between the access provider demarcation point and the end equipment.

Backbone cabling:

- one connection in the entrance room;
- Two connections in the main cross-connect;
- No intermediate cross-connect.
- Horizontal cabling:
- two connections in the horizontal cross-connect;
- An outlet connection at the equipment distribution area.

This “typical” configuration corresponds to the typical data center with an entrance room, main distribution area (MDA), one or more horizontal distribution areas (HDAs), and no zone distribution areas. Maximum circuit lengths for a typical data center configuration with six connections. These maximum

circuit lengths should include backbone cabling, horizontal cabling, and all patch cords or jumpers between the access provider demarcation point and the end equipment.

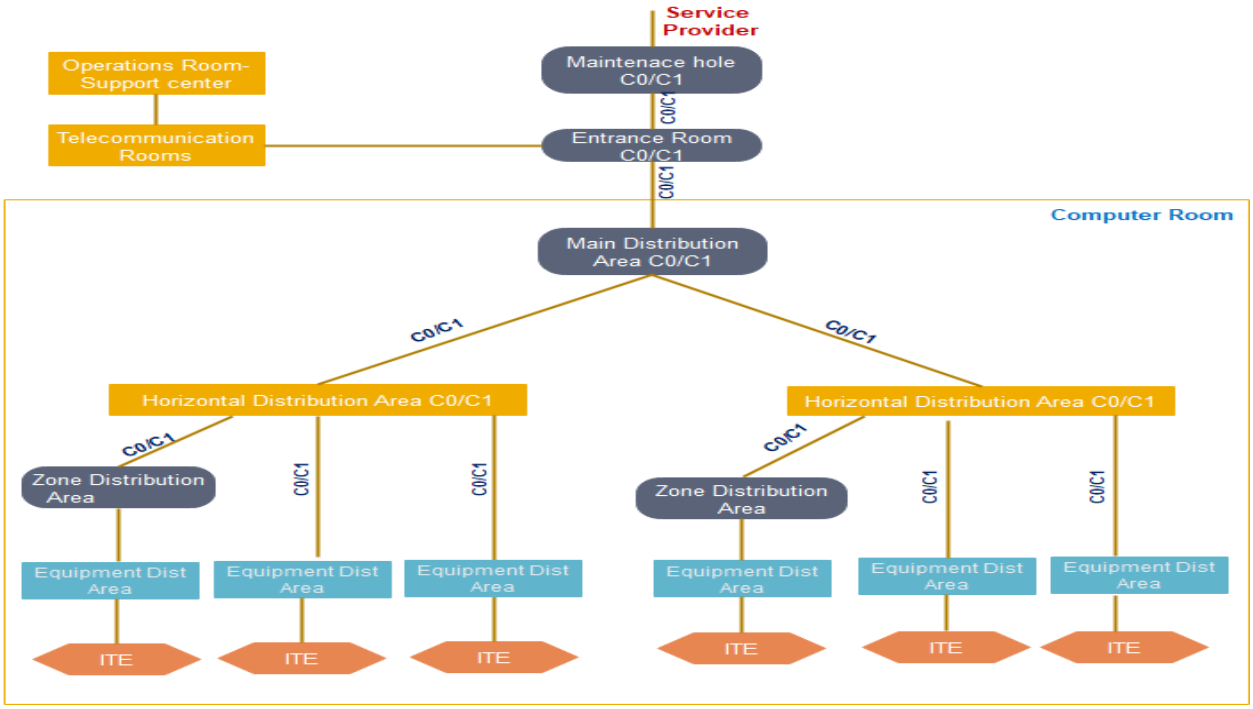
9.6. Telecommunications Cabling Infrastructure Classes

For the telecommunications cabling infrastructure reliability classes, the corresponding class designation is prefaced with a “C” to identify it represents the “cabling infrastructure” reliability criteria.

9.6.1. Class C0 and C1 Telecommunications Infrastructure

A Class C0 or C1 telecommunications cabling infrastructure is a single path cabling infrastructure. The cross-connect fields throughout the data center support a single path, non-redundant network architecture.

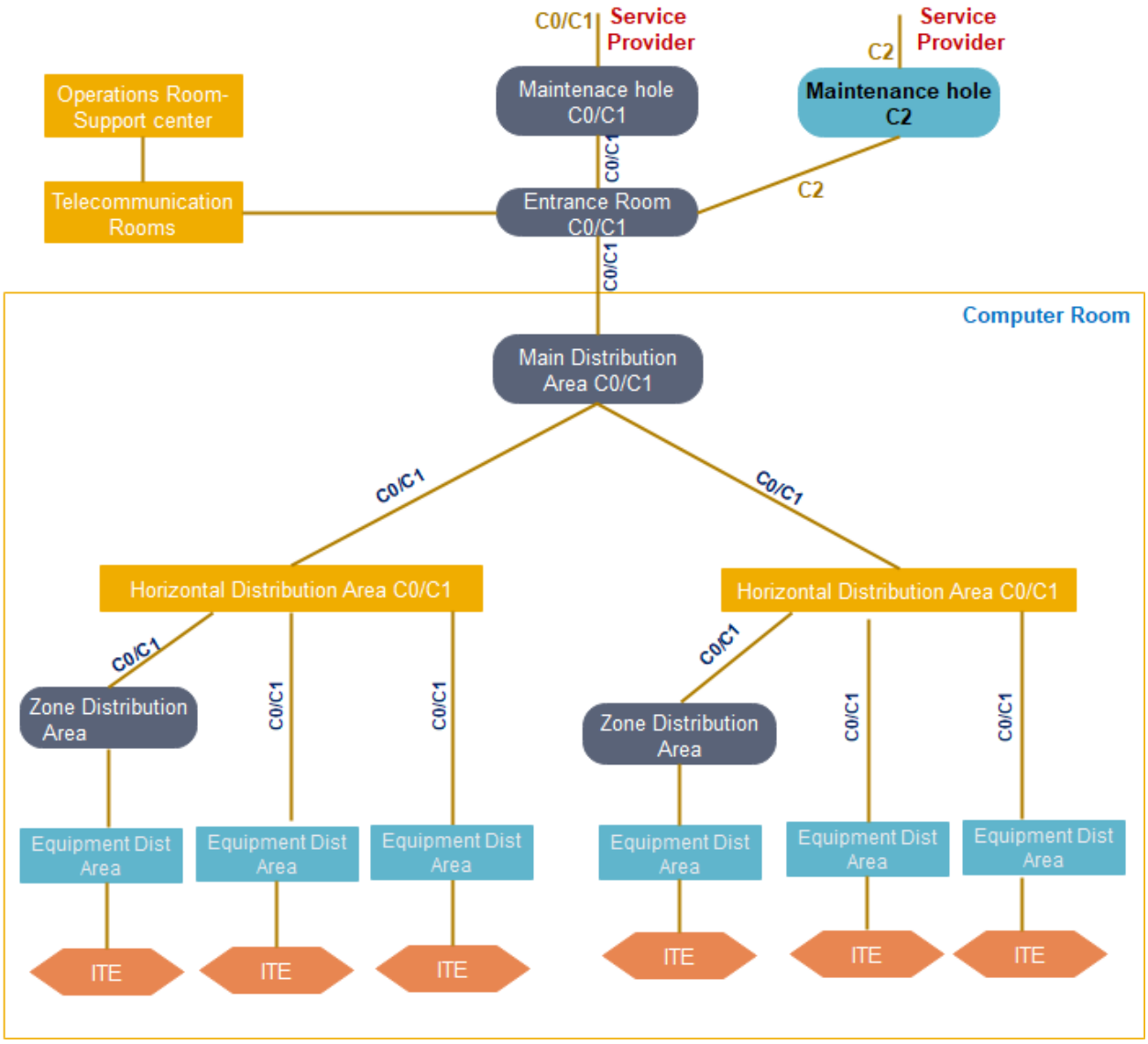
Entrance Pathways**:** Single path, multiple conduits from property line to
ER-Entrance Room: One ER accommodates a service provider
Main Distribution Area:
One MDA supports all core equipment
Intermediate Distribution Area
Each HDA supported by a single MDA or IDA
Horizontal Distribution Area:
Non-redundant HDA to support any intermediary switching equipment and horizontal cross-connect fields, multiple HDAs may be required to support port counts and distance limitations within large computer rooms.



9.6.2. Class C2 Telecommunications Infrastructure

A Class C2 telecommunications cabling infrastructure is a single path cabling infrastructure. The cross-connect fields throughout the data center support a single path, non-redundant network architecture. It contains redundant entrance pathways to support, at a minimum, a single link from two providers or ringed topology from one provider.

Entrance Pathways: Redundant and diverse multi-path, each path with multiple conduits from property line to ER.
Entrance Room: One ER accommodates a service provider(s)
Main Distribution Area: One MDA supports all core equipment
Intermediate Distribution Area Each HDA supported by a single MDA or IDA
Horizontal Distribution Area: Non-redundant HDA to support any intermediary switching equipment and horizontal cross-connect fields, multiple HDAs may be required to support port counts and distance limitations within large computer rooms.



9.6.3. Class C3 Telecommunications Infrastructure

A Class C3 telecommunications cabling infrastructure is a redundant path cabling infrastructure that has redundant cross-connect fields for all backbone network cabling.

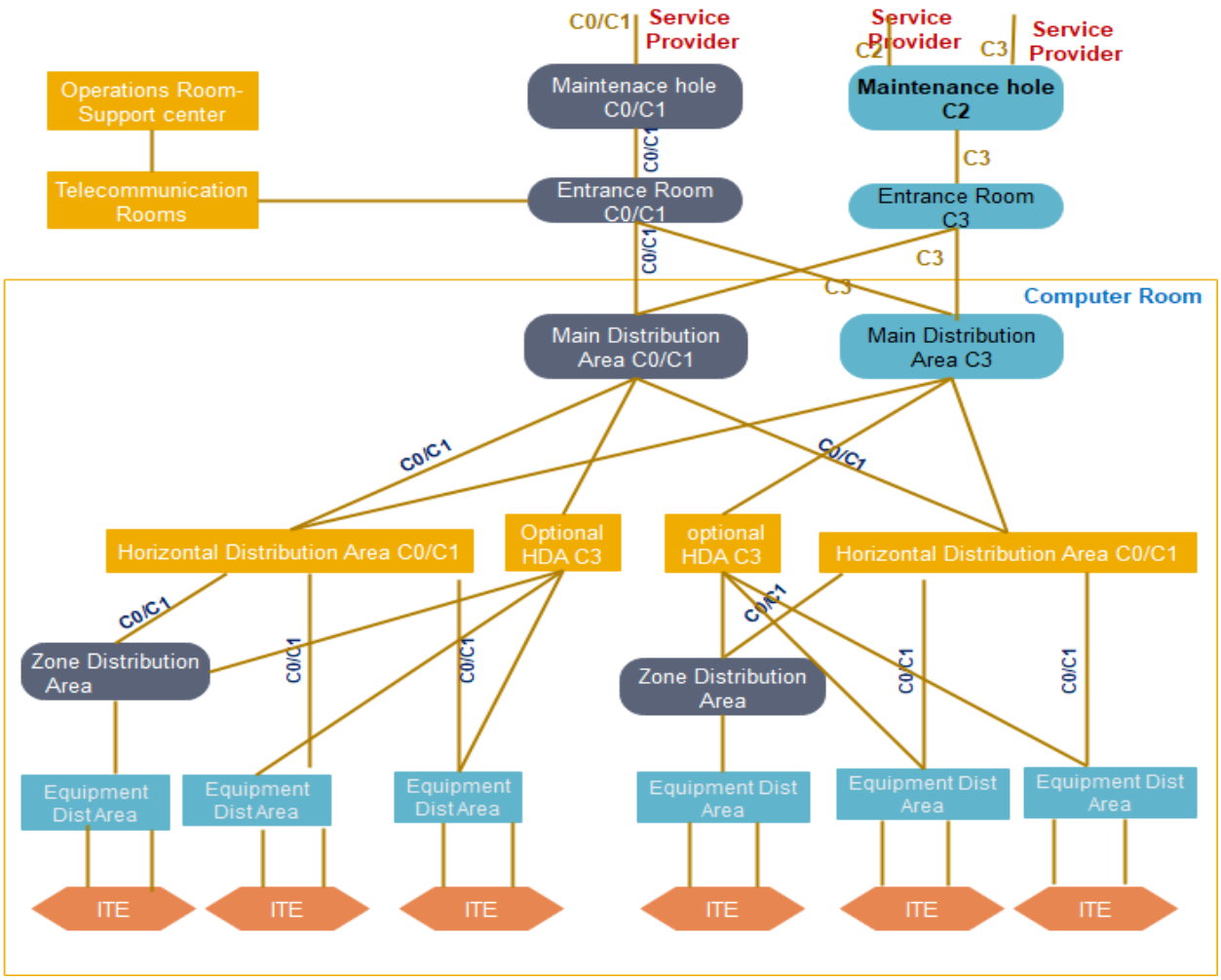
The redundant backbone cabling is intended to support a redundant network.

Physically separated redundant horizontal cross-connects and a redundant horizontal cabling to equipment cabinets (EDAs) is also recommended.

Physical separation between redundant MDAs, IDAs, or HDAs may minimize common modes of failure that may be present within the supporting critical infrastructure (e.g., failure of the sprinkler system, raised floor system, cabling pathway system, grounding system).

Physical separation may also minimize failure because of any event caused by human error or component failure, which is not contained within an MDA or HDA cabinet, thereby exposing adjacent cabinets to risk of failure.
Having redundant distributors and cabling may increase operational complexity.

Entrance Pathways: Redundant and diverse multi-path, each path with multiple conduits from property line to each ER.
Entrance Room: Two ERs to support multiple service providers, providing physical separation between Redundant provider and edge equipment.
Main Distribution Area: MDAs support the main cross-connect (MC) and backbone network equipment. Redundant MDAs should be physically separated.
Intermediate Distribution Area IDAs support the intermediate cross-connect (IC) and possibly backbone network equipment. Redundant IDAs should be physically separated.
Horizontal Distribution Area: HDAs support horizontal cross-connects and may support access layer switches.
Equipment cabinets (EDAs) should (but are not required to) have horizontal cabling to two different, physically separated HDAs.



9.6.4. Class C4 Telecommunications Infrastructure

A Class C4 telecommunications infrastructure is a redundant path cabling infrastructure that has redundant cross-connect fields throughout data center network to support redundant network architecture. It contains redundant entrance facilities to support multiple network service provider topologies.

Physical separation between redundant MDAs or HDAs is required to minimize common modes of failure that may be present within the supporting critical infrastructure (e.g., failure of; sprinkler system, raised floor system, cabling infrastructure pathway system, grounding system, electrical distribution system) or any event caused by human error or component failure, which is not contained within one MDA or HDA cabinet, thereby exposing adjacent cabinets to risk of failure as well.

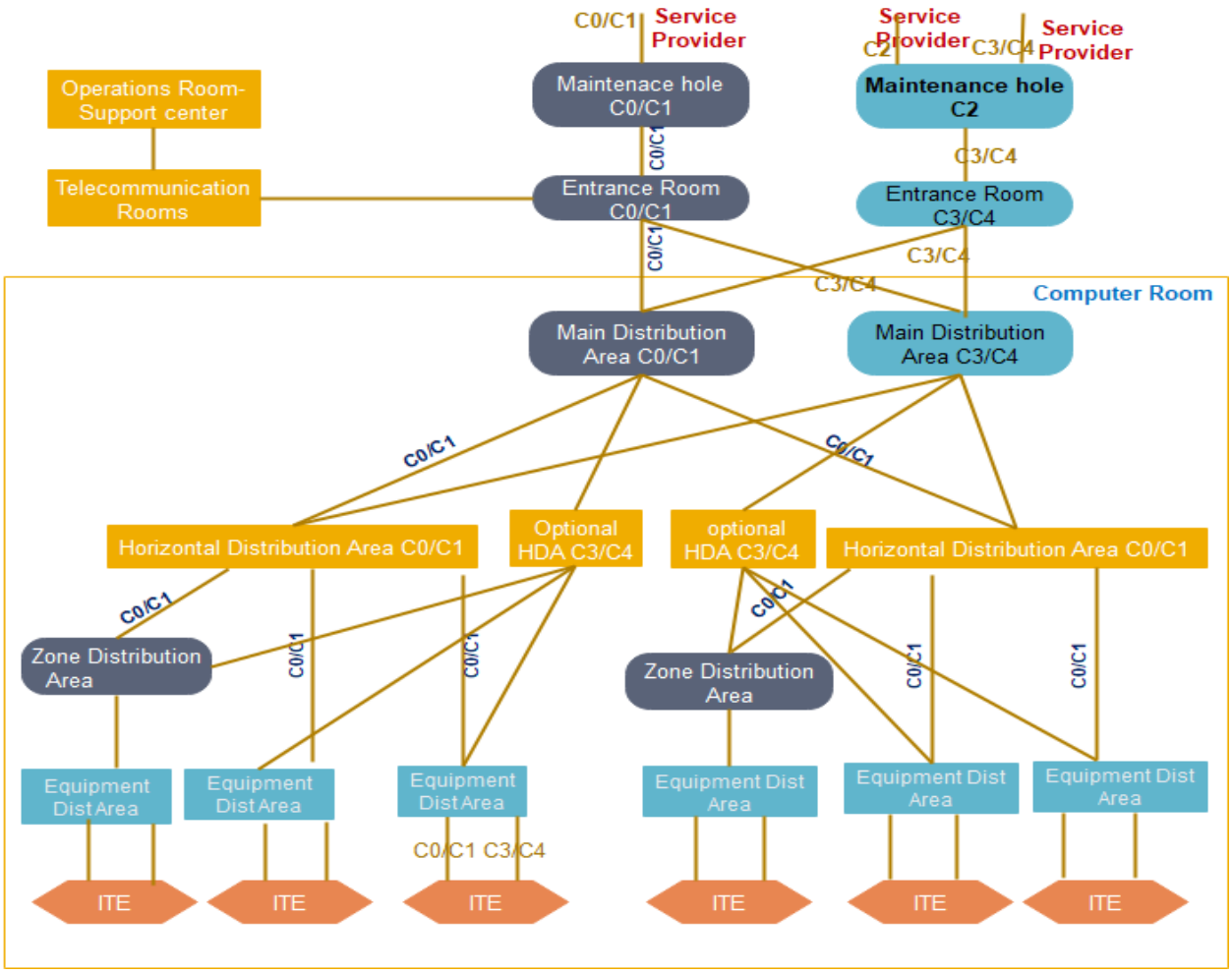
Entrance Pathways: Redundant and diverse multi-path, each path with multiple conduits from property line to each ER
Entrance Room: Two ERs to support multiple service providers, providing physical separation between redundant providers edge equipment.

Main Distribution Area: Two MDAs to support redundant core equipment. Physical separation between redundant MDAs is required to minimize common modes of failure that may be present within the supporting critical infrastructure.

Intermediate Distribution Area Redundant physically separated IDAs. If an HDA has backbone cabling to IDAs, it must be supported by diversely routed backbone cabling to two physically separated IDAs.

Horizontal Distribution Area: Redundant HDAs to support any intermediary redundant switching equipment and horizontal cross-connect fields, additional HDAs may be required on both the “A” and “B” network fabric to support increased port counts and distance limitations within large computer rooms.

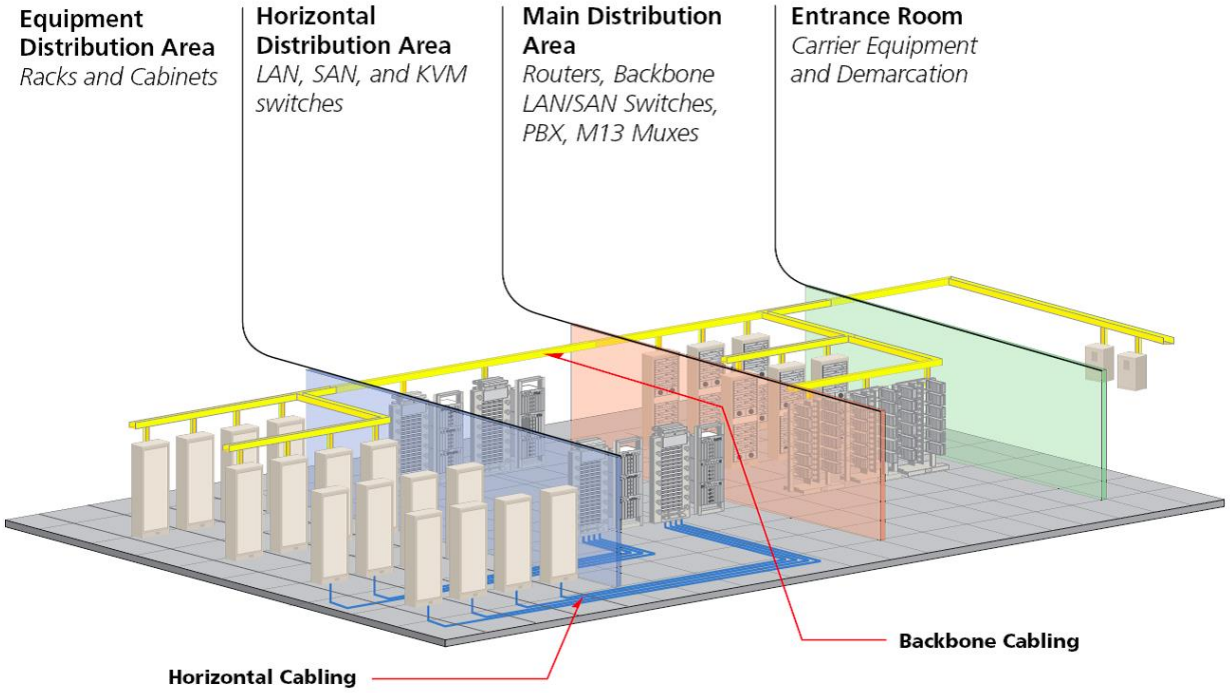
Physical separation between redundant HDAs is required to minimize computer common modes of failure that may be present within the supporting critical infrastructure



9.7. Cabling Topology

The basic cabling elements of the data center star topology should include:

- Horizontal cabling
- Backbone cabling
- Equipment cabling



9.7.1. Horizontal cabling

The system of cabling that connects telecommunications rooms to individual outlets or work areas on the floor.

In premise cabling, any cabling that is used to connect a floor's wiring closet to wall plates in the work areas to provide a local area network (LAN) drops for connecting users' computers to the network.

9.7.2. Backbone cabling

Backbone cabling systems provide necessary interconnects at the datacenter facility, providing the vital cabling foundation to datacenter stay connects with inside and outside of facility.

It Connects between MDA, IDA, HDA room and entrance section in the datacenter, Backbone cabling consists of the transmission media, main and intermediate cross-connects and terminations at these locations.

The presence of an HDA or IDA is not mandatory. Cabling extending from the TIA HC in the HDA, IDA, or MDA to the mechanical termination in the EDA is considered horizontal cabling. Sufficient horizontal cable slack should be considered allowing migration to a cross-connect in the HDA, IDA, or MDA. Backbone cabling cross-connects may be in TRs, computer rooms, MDAs, IDAs, HDAs, or at entrance rooms.

9.7.3. Equipment cabling

Equipment cabling connects the cable from one device to another device and this type of cabling occurs inside the cabinet and rack.

10. DATA CENTER CABLING PATHWAYS

Datacenter should ensure that capacity of pathway has been estimated as per quantities cable when the data center is fully populated, and all expansion areas are built.

Cabling pathway design should have an adequate capacity of pathways at entrance rooms, main distribution areas (MDAs), intermediate distribution areas (IDAs), horizontal distribution areas (HDAs), and intersections of cabling pathways.

Data centers cabling should not be routed through spaces accessible by the public or other neighbors and make sure that cables are enclosed conduit or other secure pathways.

All maintenance holes; pull boxes or splice boxes should be equipped with a lock and entrance cabling for data center should not be routed through a common equipment room and it should be a monitored datacenter security system using a camera or remote alarm.

Utility tunnels used for datacenter entrance rooms should be keep locked, if tunnels are shared with other data centers, it has to be in good metallic conduit or secure pathway separation.

Ensure that there is a proper distance between power cables and balanced twisted-pair cables as per ANSI/TIA 569 C Standards and there should be horizontal and vertical separation of power and network cables.

Make sure that different rows of tiles in the main aisles for power and network cabling. Provide vertical separation by placing network cabling in cable trays or baskets.

Twisted pair cable must be separated from fiber if used in same pathways. Cords and jumpers should be separated from other cabling.

Telecommunications pathways for datacenter should pass through underground and overhead pathways are not recommended. The entrance pathways should also have adequate capacity to handle growth and additional access providers.

10.1. Cable Tray Support Systems

Each access provider should have at least one metric designator 103 (trade size 4) conduit at each entrance point.

Additional conduits may be required for campus cabling. Conduits used for optical fiber entrance cables should have three inner ducts [two metric designator 40 (trade size 1.5) and one metric designator 27 (trade size 1) or three metric designator 32 (trade size 1.25)]. Consider the use of soft-sided duct material as a substitute for inner duct, which may optimize the use of finite conduit cross-sectional area.

All cables should be tied and labeled, and cables shall not be left abandoned under the access floor. Cables shall be terminated on at least one end in the MDA or an HDA or shall be removed.

10.2. Overhead Cable Trays

In data centers that use overhead pathways, 150 mm (6 in) minimum access headroom shall be provided from the top of the pathway to the obstruction located above such as another pathway or the ceiling. This clearance requirement does not apply where cable trays cross each other or cross beams, pipes or other building structures.

Typical cable tray types for overhead cable installation include wire basket cable tray, ladder type, or center spine cable tray. Adjacent sections of metallic cable tray shall be bonded together and grounded per manufacturers' guidelines, /NECA/BICSI 607, other applicable standards (e.g., TIA-607-B), and the local authority and shall be listed or classified by an NRTL for this purpose.

The metallic cable tray system shall be bonded to the data center common bonding network.

When they are supported from above; overhead cable ladders or trays (if used) shall be suspended from the structure above utilizing M12 (0.5 in) or greater threaded rods as required for structural support.

The cable trays or ladders may be supported by an overhead support structure using support pillars or a suspended frame designed to support the load of the cable tray and cables.

If used for seismic bracing, ladder racks and cable tray shall be continuous wall to wall to form a brace for the equipment.

Cable tray shall not be routed directly below fire suppression or sprinkler systems.

In data centers that use overhead pathways, 300 mm (12 in) minimum access headroom should be provided from the top of the pathway to the obstruction located above such as another pathway or the ceiling.

10.3. Underfloor Cable Trays

Ensure that necessary airflow is passing under the access floor it has to be properly ventilated. Refer ANSI/TIA-569-C for further cable tray design considerations.

Under floor cable trays may be installed in multiple layers to provide additional capacity. Metallic cable tray shall be bonded to the data center grounding infrastructure. The cable tray should have a maximum depth of 150 mm (6 in).

To provide room for cables to exit the pathways, there shall be a minimum of 20 mm (0.75 in) from the bottom of the access floor tiles to the top of the cable tray and cabling in a cable pathway that is loaded 100% of calculated capacity.

Under floor systems that require periodic access or maintenance of such as valves, electrical receptacles, and smoke detectors should not be located below under floor cable pathways unless there is an empty row of tiles adjacent to these pathways.
Under-floor cable tray routing should be coordinated with other under floor systems during the planning stages of the building.

Planning of overhead cable trays for telecommunications cabling should be coordinated with architects, mechanical engineers, electrical engineers, and plumbing and structural engineers that are designing luminaries, plumbing, and HVAC, power, and fire protection systems. Coordination should consider routing, clearances, and accessibility; consider use of three-dimensional drawings to simplify coordination.

Lighting fixtures (luminaries) and sprinkler heads should be placed between cable trays, not directly above cable trays.

Overhead cable trays should be routed to avoid impeding airflow, sprinkler patterns, and lighting. This typically implies routing cable trays over cabinets and racks rather than above aisles between them.

Overhead cable tray systems may alleviate the need for access floors in data centers that do not employ floor-standing systems that are cabled from below.

Typical installations include two or three layers of cable trays, one for power cables and one or two for cabling.

One of the cable tray layers may employ brackets on one side that hold the data center grounding infrastructure. These overhead cable trays may be supplemented by a duct or tray system for fiber patch cables. The fiber duct or tray may be secured to the same hanging rods used to support the cable trays.

Cable pathways should not be located where they interfere with proper operation of fire suppression systems such water distribution from sprinkler heads.

Overhead cable pathways should not block airflow into or out of cabinets (e.g., not block air exiting the hot aisle or cabinet vents if located at the top of cabinets).

Cables should not be left abandoned in overhead cable trays. Cables shall be terminated on at least one end in an MDA, IDA, or HDA, or shall be removed.

In aisles and other common spaces in internet data centers, co-location facilities, and other shared tenant data centers, overhead cable trays should have solid bottoms or be placed at least 2.7 m (9 ft) above the

finished floor to limit accessibility or be protected through alternate means from accidental and/or intentional damage.

The maximum recommended depth of cable in any cable tray is 150 mm (6 in). Typical cable tray types for overhead cable installation include policy-type cable ladders, center spine cable tray, or wire basket cable tray. The cable tray system shall be bonded and grounded per ANSI/TIA-607-B.

Overhead cable trays should be suspended from the ceiling. Where building structural characteristics make overhead suspension of a cable tray impossible, the tray can be suspended from a structural grid that is supported by other means. If all racks and cabinets are of uniform height, the cable trays may be attached to the top of racks and cabinets, but this is not a recommended practice because suspended cable trays provide more flexibility for supporting cabinets and racks of various heights and provide more flexibility for adding and removing cabinets and racks.

Lighting fixtures and sprinkler heads should be placed between cable trays, not directly above cable trays.

Cable trays should be located above cabinets and racks instead of above the aisles where lighting should be located.

Access flooring shall meet the performance requirements of ANSI/TIA-569-C. Access floors for data centers should use a bolted stringer understructure as they are more stable over time than stringer less systems. Additionally, access floor stringers should be 1.2 m (4 ft) long installed in a “basket weave” pattern to improve stability.

Pedestal adhesive should be applied under all base plates. Pedestal bases should also be bolted to the subfloor (except post-tension floors) for added stability in seismic areas.

Access floor tile cuts should have edging or grommets along all cut edges. If the edging or grommets are higher than the surface of the access floor, they shall be installed as not to interfere with placement of racks and cabinets.

The edging or grommets shall not be placed where the racks and cabinets normally contact the surface of the access floor.

In the case of down-flow AC systems where the access flooring is being used as an air distribution plenum, floor tile cuts should be limited in both size and quantity to ensure proper airflow.

Floor tiles with cement or wood cores should have their exposed cut edges sealed in order to prevent core material from being blown into the computer room.

After cuts are made to the access floor system and all equipment racks, cabinets, etc. are in place, it is recommended that the AC system be properly balanced.

10.4. Backbone Cabling

The function of the backbone cabling is to provide connections between the MDA, IDA, HDA, and entrance rooms in the data center cabling system.

Backbone cabling consists of the backbone cables, MC/MD, IC/ID, mechanical terminations, equipment cords, and patch cords or jumpers used for backbone-to-backbone cross-connection.

The backbone cabling shall allow network reconfiguration and future growth without disturbance of the backbone cabling.

10.5. Cabling Types

Each recognized cable has individual characteristics that make it suitable for a range of applications defined against each category or cabling type in the applicable cabling standards.

A single cable may not satisfy all end user requirements. It may be necessary to use more than one medium in the backbone cabling.

In those instances, the different media shall use the same facility architecture with the same location for cross-connects, mechanical terminations, and inter-building entrance facilities.

As a result of the wide range of services and site sizes where backbone cabling will be used, more than one transmission medium is recognized.

This standard specifies the transmission media that shall be used individually or in combination in the backbone cabling.

Recognized cables associated connecting hardware, jumpers, patch cords, equipment cords, and zone area cords shall meet all applicable requirements specified in applicable standards and related addenda (e.g., ISO/IEC 11801, TIA-568-series).

Backbone cabling shall consist of one or more of the following media types:
• 100-ohm balanced twisted-pair Category 3/Class C minimum, (Category 6/ Class E or higher recommended)
• OM3 multi-mode optical fiber cable minimum, (OM4 multi-mode optical fiber cable recommended)
• OS1 or OS2, single-mode optical fiber cable
• 75-ohm coaxial cabling (Telcordia GR-139-CORE 734-type and 735-type)

Redundant backbone cabling protects against an outage caused by damage to the primary backbone cabling.

Redundant backbone cabling may be provided in several ways, depending on the degree of protection desired.

Backbone cabling between two spaces (e.g., a horizontal distribution area and a main distribution area) can be provided by running two cabling channels between these spaces, preferably along different routes.

If the computer room has two main distribution areas, redundant backbone cabling to the horizontal distribution area may not be necessary although the routing of cabling to the two main distribution areas should follow different routes.

Some degree of redundancy can also be provided by installing backbone cabling between horizontal distribution areas. If the backbone cabling from the main distribution area to the horizontal distribution area is damaged, connections can be patched through another horizontal distribution area.

The Equipment cords and patch cords, the backbone cabling distances shall be designed to accommodate the maximum cordage length so that when configuring channels for use with applications the combination of equipment cord, a permanent link and patch cords never exceeds the channel loss limits.

10.5.1. Centralized Optical Fiber Cabling

Centralized optical fiber topologies permit the intermediate distribution areas and horizontal distribution areas to have no switches.

Centralized cabling design shall allow for the addition and removal of horizontal and backbone optical fiber cabling.

Enough space shall be left in the HDA and IDA to allow for the addition of patch panels needed for the migration of the pull-through, interconnect, or splice to a cross-connection.

Centralized cabling design shall allow for migration (in part or in total) of the pull-through (continuous sheath cables), interconnect, or splice implementation to a cross-connection implementation or configuration utilizing equipment (e.g., switches) in the distributors.

Centralized cabling shall support the administration and labeling requirements of the cabling standards being followed.

Administration of moves and changes shall be performed at the centralized cross-connect. In addition, computer room splice, and interconnect hardware shall be labeled with unique identifiers on each termination position.

Polarity shall adhere to the requirements of the cabling standards being followed. Service loop storage shall provide bend radius control so that optical fiber bend radius limitations are not violated.

Single-Mode and Multimode Connector Color Recommendations

The single-mode connector or a visible portion of it should be blue, referring to a flat-polished optical fiber end face; green should signify a connector featuring an angle polished optical fiber end face.

Where a mixture of OS1 and OS2 exist in a single data center space or room, additional identification should be applied to clearly identify the fiber type used.

10.5.2. Horizontal Cabling

The horizontal cabling is the portion of the telecommunications cabling system that extends from the equipment outlet (EO) in the EDA to the TIA HC or ISO/CENELEC ZD in an HDA, IDA, or MDA.

The horizontal cabling includes:

- Horizontal cables
- Mechanical terminations
- Equipment cords, patch cords, or jumpers;
- TIA zone outlet, TIA consolidation point (CP), or ISO/CENELEC local distribution point (LDP) in the optional ZDA

Horizontal cabling shall consist of one or more of the following media types:

- 4-pair 100-ohm balanced twisted-pair Category 6/Class E minimum (Category 6A/Class EA or higher recommended)

- OM3 multi-mode optical fiber cable minimum (OM4 multimode optical fiber cable recommended where horizontal fiber cabling lengths exceed 70 m [230 ft])

- OS1 or OS2, single-mode optical fiber cable

10.5.3. Balanced Twisted-Pair Cabling

Balanced twisted-pair cabling performance is described using a scale based on classes or categories, as defined by ISO/IEC and TIA, respectively. While Category 3/Class C is the minimum acceptable performance for backbone cabling, Category 6/Class E is the minimum requirement in TIA-942-A and CENELEC EN 50173-5 for horizontal cabling, and Category 6A/Class EA is the minimum requirement as listed in ISO/IEC 24764.

10.6. Cabling Installation

Cabling shall be installed and dressed neatly, taking care to adhere to minimum cable bend radii for cables. Take particular care not to leave excess optical fiber loops on the floor or in places where they can be damaged. While all transmission parameters are sensitive to transmission discontinuities caused by connector terminations, return loss, and all forms of crosstalk (e.g., near-end crosstalk [NEXT], attenuation-to-crosstalk ratio–far end[ACR–F], previously known as ELFEXT), performance of balanced twisted-pair systems are particularly sensitive to conductor untwisting and other installation practices that disturb pair balance and cause impedance variations.

To prevent these problems, the installer shall adhere to the following practices:

• Remove only as much cable jacket as is required for termination and trimming.

• Follow the manufacturer’s instructions for mounting, termination, and cable management.

• Minimize the amount of untwisting in a pair as a result of termination to connecting hardware. For untwisting cabling, maintain pair twists as close as possible to the termination point; the amount of untwisting must not exceed 13 mm (0.5 in) for Category 5e and higher cables.

10.7. Telecommunications and Computer Cabinets and Racks

As with all other systems of the data center—power, HVAC, and flooring—cabinets and racking systems provide the vital services of proper structural and secure housing for data center equipment. Active and passive equipment have different requirements for mounting, power, ventilation, and cable management.

The following criteria of racks shall conform to applicable codes, standards and regulations (e.g., EIA/ECA-310-E, IEC 60917):

- Channel dimensions and spacing
- Channel hole dimensions and thread systems
- Channel equipment mounting hole vertical spacing (U or RU)
- Panel opening and usable aperture opening

Maximum height should not exceed 2.4 m (8 ft.)
When in a row, multiple racks and their associated vertical cable managers should be bolted together

The following criteria shall conform to applicable codes, standards, and regulations (e.g., EIA/ECA-310-E, IEC 60917):

- Equipment mounting rail dimensions and spacing
- Equipment mounting rail hole vertical spacing (U or RU)
- Options for cable access into the cabinet shall be available from both the top and bottom.
- Access floor openings beneath cabinets for cable entry shall offer:
- Protection against damage to the cables
- Restrictions against intrusion of dirt and debris
- Restriction of air passage
- Cabinets shall be constructed of noncombustible materials.

Top access ports should provide a means to be closed when not in use.
In seismically active areas, multiple cabinets in a row should be bolted together at the top to provide additional Stability.

Within EDAs, select cabinets, racks, and vertical cable managers whose design minimizes obstruction of exhaust air and recirculation of hot air from behind the equipment to air intakes in the front of the equipment.

Within HDAs, IDAs, and MDAs, select cabinets, racks, and vertical managers whose design optimizes patch cord management, while minimizing air leakage between hot aisle and cold aisle.

In data centers that employ hot aisle/cold aisle orientation, ensure that the warm air is always exhausted toward the hot aisle.

Optical fiber and balanced twisted-pair ports are located at the rear of many servers.

To simplify patching and maintenance, structured cabling patch panels should be mounted so that the ports face the same direction as the network ports on the equipment to which they are patched. These ports are commonly on the rear of servers and the front of network switches.

For equipment that is cooled side-to-side (e.g., certain networking equipment), cabinets, racks, and vertical cable managers should be selected that introduce the least disruption to the proper functioning of the hot and cold aisles and that minimize recirculation of hot air toward the air intakes.

Finishes should conform to applicable codes, standards, and regulations (e.g., ANSI/TIA-942-A, ATIS 0600336);

Conductive finishes are recommended to ensure a good bond between equipment and cabinet or rack ground and to prevent oxidation of the base metal.

For painted racks, a supplementary bonding/grounding bus bar system may be used to ensure a good bond between equipment and cabinet or rack ground.

Cabinet and rack bonding and grounding should comply with applicable codes, standards, and regulations (e.g., NECA/BICSI-607, TIA-607-B, and ISO/IEC DIS 30129 currently in development).

Racks in entrance rooms, main distribution areas and horizontal distribution areas should have dimensions and cable management capacities in accordance with applicable codes, standards, and regulations (e.g., TIA-942-A).

Twisted pair or coaxial patch panel should be used unless a specific high-density solution of managing the patch cords on the sides for every unit is chosen.

Exceptions exist when a non-angled patch panel features an integrated horizontal management product design.

Vertical cable management should always be provided unless patching is provided directly above or directly below mated passive patch panels (e.g., balanced twisted-pair, coaxial cabling, or optical fiber cabling) or between passive patch panels and active equipment that are installed directly above or below one another.

In such cases, relatively short (typically less than 1 m [3 ft.] patch cord assemblies (or equipment cord assemblies) may be used. When angled patch panels are used, horizontal cable managers are typically not installed.

Vertical cable managers should always be sized to accommodate the anticipated maximum cordage that may be deployed given the equipment requirements at the time of deployment.

Shorter power cords, equipment cords, patch cords, and keyboard-video-mouse (KVM) cabling should be specified to reduce the cable management density in the back of the cabinet or rack.

Rack depth should meet the mounting and protection needs of the equipment they are to host and, as a minimum, conform to the criteria established in applicable standards (e.g., EIA/ECA-310-E, IEC 60917).

Each rack should have vertical cable managers sized for maximum rack capacity attached on both sides. Vertical cable managers between two racks should be sized to serve both racks simultaneously.

Equipment mounting rails should be adjustable front-to-rear and should have rack unit number indications (with numbers starting at the bottom).

Equipment mounting rail dimensions should conform to applicable codes, standards, and regulations (e.g., EIA/ECA-310-E, IEC 60917).

Doors should be removable without tools. Door hinge orientation should be reversible or dual hinged.

Side panels should be removable and lockable without requiring intrusion into the equipment mounting area within the cabinet.

In applications where active equipment, patch panels, and horizontal cable distribution are mixed, floor-tile-width (e.g., 600 mm [24 in] width) cabinets may lack adequate vertical cable management space.

Blank panels should be installed in unused rack positions to maintain separation between hot aisles and cold aisles and prevent hot exhaust air from recirculating and mixing with chilled air at equipment in-takes. Blank panels also improve rigidity of cabinets.

10.8. Cabinet Airflow and Cabling Capacity

To ensure adequate airflow and to provide adequate space for power strips, telecommunications cabling, and safe access for work, the cabinet depth should be at least 150 mm (6 in) deeper than the deepest equipment to be housed if the cabinet is 700 mm (27.5 in) wide or larger.

If the cabinet is less than 700 mm (27.5 in) wide, 11.5 mm (0.45 in) depth should be added for every 10 mm (0.4 in) reduction from 700 mm (27.6 in) width.

Mesh doors are used for ventilation, the doors should be a minimum 63% open to airflow for allowing chilled air entrance or evacuating heated exhaust air from the cabinet.

It is recommended that the following formulae be used to calculate door airflow capacity:

Airflow capacity (AFC) calculations:
AFCD = SD × FEA
AC × HRMU × NRMU
(14-4)
Where:
AFCD is airflow capacity for cabinets with doors SD is total surface area of the door panel inside the outer extreme boundaries of airflow openings (mesh, perforations, slots, etc.), in mm2 (in2) FEA is effective (open) area factor of the door mesh material (e.g., 0.65 [65%], 1 if mesh or screen is not used)

AC is useable cabinet aperture opening at the door plane, in mm (in)
HRMU is height of one rack unit (44.5 mm [1.75 in])
NRMU is quantity of rack units in the cabinet.

Given:
• 19-in equipment cabinet

• Height: 42 RMU
• Mesh door with FEA = 0.65, 1,930 mm x 635 mm (76 in x 25 in)
• 1 RMU = 44.5 mm (1.75 in)
• Cabinet open aperture: 450.85 mm (17.75 in)
NOTE: Input data and criteria used in the examples above are provided as samples only. For actual parameters, please refer to the particular network cabinet or server cabinet design requirements.
Airflow capacity:
AFCD = (SD × FEA) = (1,930 mm × 635 mm × 0.65) AC × HRMU × NRMU 450.85 mm × 44.5 mm × 42
AFCD = 1,225,550 mm2 × 0.65 842,639 mm2 = 0.9454

Cabinet width	Deeper than the deepest equipment house in the cabinet	Additional depth for narrow cabinets
600 mm (24 in)	150 mm (6 in)	115mm (4.5 in)
700 mm(27.5 in)	150mm (6 in)	N/A
750 mm(29.5in)	150mm (6 in)	N/A
800 mm(31.5 in)	150 mm(6 in)	N/A

10.9. Cabinet and Rack Installation

Where the cabinets and racks are on an access floor, they shall be placed so that there are movable tiles in front and behind each cabinet and rack.

This typically means placing the rows of cabinets and racks parallel (rather than at an angle) to the rows of floor tiles and placing the front edge of the cabinets along the edge of the floor tiles to lock down the minimum number of tiles under the cabinets

All overhead cable management (e.g., ladder racks, cable tray, etc.) shall remain free of obstructions such as sprinklers, lighting, and electrical outlets.

The designer shall anticipate the weight of the equipment in the cabinets and racks; ensure that the cabinets, racks and floors (both access floors and slabs) are rated to handle the expected weight.

Adequate power shall be available to all cabinets and racks that will hold active equipment and must be installed in accordance with applicable codes.

Each cabinet and rack shall be labeled on the front and back with its identifier. All patch panels, cables, equipment cords, and patch cords shall be properly labeled per applicable standards (e.g., TIA-606-B, ISO 14,763-2-1).

Cabinet and rack layout designs should be harmonized with lighting (luminaire) delivery layout designs. Anticipate growth and leave room for expansion when/if possible.

Power strips should be labeled with power distribution unit or electrical panel board identifier and circuit breaker number.

Power cords should not be installed under equipment, mats, or covering other than access floor tiles.

The mounting surface for cabinet and racks should be prepared for the specific anchors required for the application.

Cabinets in a line-up where they are properly attached together may require fewer anchors per cabinet than those installed as standalone units.

When drilling into the mounting surface use proper technique to ensure that dust or particles do not get airborne. Using a drill with the attached vacuum is an effective way to prevent dust or particles while drilling in floors or walls.

Equipment in the computer room should be mounted to cabinet or rack rails rather than placed on shelves as equipment on shelves provides a return path for air between the rear and front of the cabinet or rack.

Floor tile openings under cabinets and racks should be no larger than required for entry of cabling to minimize loss of underfloor pressure through openings.

Consider using openings with gaskets or brush grommets to satisfy requirements to minimize air pressure loss and short-circuiting of cold aisle/hot aisle air circulation and subsequent reduction in cooling efficiency.

A dedicated pathway should be provided for equipment cords or patch cords within an MDA, IDA, or HDA that is separate from those used for horizontal and backbone cabling.

Ensure all active devices are properly supported and securely mounted to the rack to prevent equipment damage from improper installation.

In seismically active areas, it is recommended that the design of the attachment methods and the installation be reviewed by a licensed structural engineer. Many jurisdictions will require a seismic certification report signed by a professional engineer.

Sharp edges at the top of the threaded rods should be capped (using plastic covers, domed nuts, or other means).
The exposed threads under the access floor should be covered using split tubing or other method to avoid abrading cable.

Racks should be set in place and leveled throughout the line-up.

Shimming of any anchoring point should not exceed 13 mm (0.5 in) unless specified by the project engineer. If racks require more than 13 mm (0.5 in) of shimming, an engineered solution should be used to ensure rack line-ups are properly supported.

Adjacent racks in the line-up should be hanged together before anchors are installed. Install anchors per manufacturer specification, making sure all shims are properly located.

Some line-ups require additional bracing to meet customer specifications or local codes. Required bracing may be based on rack style, equipment, and location.

Bracing should be installed as a system to ensure proper fit and support. Install all parts hand tight and then tighten fasteners in a series to prevent stress on rack lineup. All bracing should be installed before racks are populated.

Avoid empty cabinet or rack positions in rows.

Replace removed cabinets or frames and fill any gaps in a row of cabinets with a substitute blanking panel of the same height as the cabinet or frames to either side to avoid recirculation of air between hot and cold aisles.

Cabinets and racks should be installed with no blank spaces between them. In the case of vacant cabinets and racks and where blank spaces exist in populated cabinets and racks, install blanking panels.

Vertical cable managers can provide cable management and block recirculation of air between racks.

Cabinets should be butted up against each other. Where possible, bayed cabinets should still share a side panel or include other means to seal the rear-to-front airflow path along the side of rack-mounted equipment.

Placing one edge of the cabinet creates unequal aisle sizes, the front aisle should be the larger one as it provides more working space for installation of equipment into cabinets and a greater area for providing cool air to cabinets.

In order to meet the requirement to restrict air passage through all openings outside the cold aisle on access floors, floor tile openings under cabinets and racks should be no larger than required for entry of cabling to minimize loss of underfloor pressure through openings considering anticipated growth.

Consider using openings with gaskets or brush grommets to minimize air pressure loss and short-circuiting of cold aisle/hot aisle air circulation and subsequent reduction in cooling efficiency.

Ensure that all active devices are properly supported and securely mounted to the cabinet to prevent equipment damage from improper installation.

Plan equipment; power strip, cable manager, and cabling layouts in cabinets before making a major purchase.

Either create detailed drawings or preferably create a mock up to ensure that:

- All equipment and cable managers fit properly
- There is adequate space and access to power strips
- There is adequate access to cabinet floor and top openings
- There is adequate space for cable management
- Equipment can properly slide in and out as required
- Equipment intakes and exhausts are not blocked by cabling, cable management, or cabinet structure so that air can flow freely within the rack and to exit out the hot side
- Cabinets, racks, and vertical management do not have large openings for recirculation of air from hot to cold aisles temporarily remove any doors and panels that may interfere with the cabinet installation.

On solid or slab floors, cabinets should be set in place and leveled throughout the line-up. Most cabinets are equipped with leveling feet. If leveling feet are not provided, consult manufacturer for proper shimming hardware.

On access floors, cabinets and racks should be secured to the concrete subfloor. If cabinets in the line-up are to be hanged, attachment hardware should be installed before anchors are installed. Install anchors per manufacturer's specification, making sure all shimming hardware is properly located.

In seismically active areas, it is recommended that the design of the cabinets and their installation be reviewed by a licensed structural engineer as many jurisdictions require a seismic certification report signed by a professional engineer.

Sharp edges at the top of the threaded rods should be capped (using plastic covers, domed nuts, or other means).

The exposed threads under the access floor should be covered using split tubing or other method to avoid abrading cable.

Floor tile panels should have correctly sized and placed cutouts for the cabinet or equipment placed over them.

The cutout should be under the cabinet/equipment cord opening and properly sized for the quantity and type of cables to be routed through the opening.

10.10. Thermal Management in Cabinets

There is no one thermal management configuration that works best in every instance. Each may be optimal, depending on different factors unique to the customer, application, and environment.

Consideration should be given to understanding the upfront installed costs as well as an ongoing operational cost from an energy efficiency and maintenance perspective.

Equipment should be installed in cabinets with the air intake oriented toward the front of the cabinet or rack and the air exhaust oriented toward the rear of the cabinet or rack, when possible, with the cabinet rows oriented in a “hot aisle/cold aisle” configuration—rears of cabinets facing each other and fronts of cabinets facing each other.

Use of any supplementary cooling mechanisms on a cabinet must take into consideration its effect on the overall fluid dynamics of the air space and how other equipment will be affected.

Considerations of supplemental cooling systems need to include criticality and required levels of redundant backup.

Cabinets with good passive air management systems in well-designed rooms remove concerns about single points of failure and can support heat loads of twenty kW and higher.

Cabinet fans for cabinets specially designed to handle high heat loads should be on UPS power and have redundant power cords or be on transfer switches to ensure continuous operation.

Cabinet fans should be on separate circuits from the equipment in the cabinet as fans are susceptible to ground faults.

The perimeter of the equipment mounting area is also a path for cold air bypass or hot air recirculation and should be blocked accordingly.

Careful planning is needed for capacities, heat loads, and redundancies required for the desired availability and reliability.

11. DATA CENTER HIGH AVAILABILITY

In general Tier 3 and Tier-4 datacenter will have redundancy to provide the business continuity with high availability to continue their function under unplanned or adverse conditions that would otherwise interrupt the data center’s telecommunications service.

The consistency of datacenter operation is dependent on the tier level of datacenter that was designed.

Tier 3 and Tier 4 datacenter will have redundant cross-connect area and pathway that are physically separated.

The datacenter needs to have multiple access providers to provide services, redundant network equipment for network level redundancy.

Minimal response time of technical support required in performing repairs to achieve the reliability of equipment to get high uptime.

The datacenter needs to have multiple entrance pathways from the property line to the entrance room to avoid a single point of failure; the maintenance hole and entrance pathways should be on opposite sides of the building and be a minimum 20m apart.

Both access providers are required to install two entrance cables in the datacenter with two entrance rooms.
One must go to primary entrance room and another one goes to a secondary entrance room and both the primary and secondary entrance room must have conduits from each other to provide flexibility.

Ensure that there are multiple access providers with multiple diverse pathways from the access provider to the datacenter for the business continuity.

The datacenter team must ensure that its services are provisioned for from different access provider central offices and the pathways to these central offices are diversely routed and this route pathways should be physically separated by at least 20m at all points along their route.

The datacenter admin team should make sure that access providers install circuit provisioning equipment in both entrance rooms so that circuits of all required types can be provisioned from either room.

The access provider provisioning equipment on both entrances must be the same and one room's equipment should be up if other room's equipment goes down.

The distance between two entrance rooms must be 20meter and it must be in different fire protection zone.

A secondary main distribution area (MDA) provides additional redundancy, but at the cost of complicating administration. Core routers and switches should be distributed between the two MDAs. Circuits should also be distributed between the two spaces.

Main and secondary distribution area must be placed in different fire protection zone and both of them have to get power from different power distribution units and from different cooling equipment.
Redundant backbone cabling protects against an outage caused by damage to backbone cabling.

Redundant backbone cabling may be provided in several ways depending on the degree of protection desired.

Backbone cabling between two spaces, for example, an HDA and an MDA, can be provided by running two cables between these spaces, preferably along different routes.

If the data center has redundant MDAs or redundant IDAs, redundant backbone cabling to the HDA from each higher-level distributor (IDA or MDA) is not necessary.

The routing of cables from the HDA to the redundant IDAs or MDAs should follow different routes.

Horizontal cabling to critical systems can be diversely routed to improved redundancy. There should be enough attention not to exceed maximum horizontal cable lengths when selecting paths.

Critical systems can be supported by two different HDAs if maximum cable length restrictions are not exceeded. The two HDAs should be in different fire protection zones for this degree of redundancy to provide maximum benefit.

11.1. Data center infrastructure Tiers

Single point of failure should be eliminated to improve redundancy and reliability, both within the data center and support infrastructure as well as in the external services and utility supplies.

This Standard includes four tiers relating to various level of resiliency of the data center facility infrastructure. The tier ratings correspond to the industry data center tier ratings as defined by the uptime institute.

This Standard includes four tiers relating to various levels of resiliency of the data center facility infrastructure.

A data center may have different tier ratings for different portions of its infrastructure. For example, a data center may be rated Tier 3 for electrical, but tier 2 for mechanical.

For the sake of simplicity, a data center that is rated the same for all subsystems (telecommunications, architectural and structural, electrical and mechanical) can be called out by its tier overall (e.g. a tier 2 data center would have a tier 2 rating in all subsystems).

All portions of the infrastructure are at the same level, the tiering should be called out specifically.
For example, a data center may be a tier rating of T2 E3 A1 M2 where:

- telecommunications are tier 2 (T2)
- electrical is Tier 3 (E3)
- architectural infrastructure is tier 1 (A1)
- Mechanical infrastructure is tier 2 (M2)

Although typically a data center's overall rating is based on its weakest component, there may be mitigating circumstances relative to that facility's specific risk profile, operational requirements or other factors that justify the lower rating in one or more subsystems.

Different areas within a data center may also be built and or used at different tier levels dependent on operational needs.

In such cases care should be given to describe these differences, for example, an area of a data center that has a tier 2 risk avoidance profile because it has T2, E2, A2 M2 services within a facility that may be Tier 3.

Care should be taken to maintain mechanical and electrical system capacity to the correct tier level as the data center load increases over time. For example, a data center may be degraded from Tier 3 or tier 4 to tier 1 or tier 2 as redundant capacity is utilized to support new computer and telecommunications equipment.

11.2. N - Base requirement

System meets base requirements and has no redundancy.

N+1 redundancy

N+1 redundancy provides one additional unit, module, path, or system in addition to the minimum required to satisfy the base requirement. The failure or maintenance of any single unit, module, or path will not disrupt operations.

N+2 redundancy

N+2 redundancy provides two additional units, modules, paths, or systems in addition to the minimum required to satisfy the base requirement. The failure or maintenance of any two single units, modules, or paths will not disrupt operations.
2N redundancy provides two complete units, modules, paths, or systems for every one required for a base system. Failure or maintenance of one entire unit, module, path, or system will not disrupt operations.

2(N+1) redundancy

2 (N+1) redundancy provides two complete (N+1) units, modules, paths, or systems. Even in the event of failure or maintenance of one unit, module, path, or system, some redundancy will be provided and operations will not be disrupted.

11.3. Concurrent maintainability and testing capability

The facilities should be capable of being maintained, upgraded, and tested without interruption of operations.

11.4. Capacity and scalability

Data centers and support infrastructure should be designed to accommodate future growth with little or no disruption to services.

11.5. Isolation

Data centers should be (where practical) used solely for the purposes for which they were intended and should be isolated from non-essential operations.

11.6. Data center tiering

11.6.1. Tier I Data Center: Basic

A Tier I data center is susceptible to disruptions from both planned and unplanned activity. If it has UPS or generators, they are single-module systems and have many single points of failure.

The infrastructure should be completely shut down on an annual basis to perform preventive maintenance and repair work. Urgent situations may require more frequent shutdowns. Operation errors or spontaneous failures of site infrastructure components will cause a data center disruption.

11.6.2. Tier II Data Center: Redundant Components

Tier II facilities with redundant components are slightly less susceptible to disruptions from both planned and unplanned activity than a basic data center. They have UPS, and engine generators, but their capacity design is “Need plus One” (N+1), which has a single-threaded distribution path throughout.

Maintenance of the critical power path and other parts of the site infrastructure will require a processing shutdown.

11.6.3. Tier III Data Center: Concurrently Maintainable

Tier III level capability allows for any planned site infrastructure activity without disrupting the computer hardware operation in any way.

Planned activities include preventive and programmable maintenance, repair and replacement of components, addition or removal of capacity components, testing of components and systems, and more.

Sufficient capacity and distribution must be available to simultaneously carry the load on one path while performing maintenance or testing on the other path.

Unplanned activities such as errors in operation or spontaneous failures of facility infrastructure components may still cause a data center disruption.

11.6.4. Tier IV Data Center: Fault Tolerant

Tier IV provides site infrastructure capacity and capability to permit any planned activity without disruption to the critical load. Fault-tolerant functionality also provides the ability of the site infrastructure to sustain at least one worst-case unplanned failure or event with no critical load impact.

This requires simultaneously active distribution paths, typically in a System + System configuration.

11.6.5. Tier 3

The data center should be served by at least two access providers. Service should be provided from at least two different access provider central offices or points-of-presences.

Access provider cabling from their central offices or points-of-presences should be separated by at least 20 m (66 ft.) along their entire route for the routes to be considered diversely routed.

The data center should have two entrance rooms preferably at opposite ends of the data center but a minimum of 20 m (66 ft.) physical separation between the two rooms.

Do not share access provider provisioning equipment, fire protection zones, power distribution units, and air conditioning equipment between the two entrance rooms. The access provider provisioning equipment in each entrance room should be able to continue operating if the equipment in the other entrance room fails.

The data center should have redundant backbone pathways between the entrance rooms, MDA, intermediate distribution areas (IDAs), and HDAs.

Intra-data center LAN and SAN backbone cabling from switches to backbone switches should have redundant fiber or wire pairs within the overall star configuration. The redundant connections should be in diversely routed cable sheathes.

There should be a "hot" standby backup for all critical telecommunications equipment, access provider provisioning equipment, core layer production routers and core layer production LAN/SAN switches.

All cabling, cross-connects and patch cords should be documented using software systems or automated infrastructure management systems as described in the ANSI/TIA-606-B.

Some potential single points of failure of a tier 3 facility are:

- Any catastrophic event within the MDA may disrupt all telecommunications services to the data center; and any catastrophic event within a HDA may disrupt all services to the area it servers.

A tier 3 data center should have protection against most physical events, intentional or accidental, natural or manmade, which could cause the data center to fail.

All systems of a tier 3 facility should be provided with at least N+1 redundancy at the module, pathway, and system level, including the generator and UPS systems, the distribution system, and all distribution feeders.

The configuration of mechanical systems should be considered when designing the electrical system to ensure that N+1 redundancy is provided in the combined electrical-mechanical system.

This level of redundancy can be obtained by either furnishing two sources of power to each air conditioning unit or dividing the air conditioning equipment among multiple sources of power.

Feeders and distribution boards are dual path, whereby a failure of or maintenance to a cable or panel will not cause interruption of operations.

Enough redundancy should be provided to enable isolation of any item of mechanical or electrical equipment as required for essential maintenance without affecting the services being provided with cooling.

By employing a distributed redundant configuration, single points of failure are virtually eliminated from the utility service entrance down to the mechanical equipment, and down to the PDU or computer equipment.

To increase the availability of power to the critical load, the distribution system is configured in a distributed isolated redundant (dual path) topology. This topology requires the use of automatic static transfer switches (ASTS) placed either on the primary or secondary side of the PDU transformer.

Automatic static transfer switches (ASTS) requirements are for single cord load only.

For dual cord (or more) load design, affording continuous operation with only one cord energized, no automatic static transfer switches (ASTS) is used, provided the cords are fed from different UPS sources. The automatic static transfer switches (ASTS) will have a bypass circuit and a single output circuit breaker.

A central power and environmental monitoring and control system (PEMCS) should be provided to monitor all major electrical equipment such as main switchgears, generator systems, UPS systems, automatic static transfer switches (ASTS), power distribution units, automatic transfer switches, motor control centers, transient voltage surge suppression systems, and mechanical systems.

A separate programmable logic control system should be provided, programmed to manage the mechanical system, optimize efficiency, cycle usage of equipment and indicate an alarming condition.

The HVAC system of a Tier 3 facility includes multiple air conditioning units with the combined cooling capacity to maintain a critical space temperature and relative humidity at design conditions, with enough redundant units to allow failure of or service to one electrical switchboard.

If these air conditioning units are served by a water-side heat rejection system, such as a chilled water or condenser water system, the components of these systems are likewise sized to maintain design conditions, with one electrical switchboard removed from service.

This level of redundancy can be obtained by either furnishing two sources of power to each air conditioning unit or dividing the air conditioning equipment among multiple sources of power.

The piping system or systems are dual path, whereby a failure of or maintenance to a section of pipe will not cause interruption of the air conditioning system.
Redundant computer room air conditioning (CRAC) units should be served from separate panels to provide electrical redundancy.

All computer room air conditioners (CRAC) units should be backed up by generator power. Refrigeration equipment with N+1, N+2, 2N, or 2(N+1) redundancy should be dedicated to the data center.

Enough redundancy should be provided to enable isolation of any item of equipment as required for essential maintenance without affecting the services being provided with cooling.

Subject to the number of Precision Air Conditioners (PAC’s) installed, and consideration of the maintainability and redundancy factors, cooling circuits to the Precision Air Conditioners (PAC's) should be sub-divided.

If chilled water or water-cooled systems are used, each data center dedicated sub-circuit should have independent pumps supplied from a central water ring circuit.

A water loop should be located at the perimeter of the data center and be in a sub floor trough to contain water leaks to the trough area.

Leak detection sensors should be installed in the trough. Consideration should be given to fully isolated and redundant chilled water loops.

11.6.6. Tier 4

Data center backbone cabling and distributor locations should be redundant.

Cabling between two spaces should follow physically separate routes, with common paths only inside the two end spaces.

Backbone cabling should be protected by routing through a conduit or by use of cables with interlocking armor.

There should be an automatic backup for all critical telecommunications equipment, access provider provisioning equipment, core layer production routers and core layer production LAN/SAN switches. Sessions/connections should switch automatically to the backup equipment.

The data center should have redundant MDAs preferably at opposite ends of the data center, but a minimum of 20 m (66 ft.) physical separation between the two spaces.

Do not share fire protection zones, power distribution units, and air conditioning equipment between the redundant MDAs. The redundant MDA is optional, if the computer room is a single continuous space, as there is probably little to be gained by implementing two MDAs in this case.

The two MDAs should have separate pathways to each entrance room. There should also be a pathway between the MDAs.

The redundant routers and switches should be distributed between redundant distribution spaces (e.g. redundant MDAs, redundant pair of IDAs, or redundant pair of HDAs, or redundant pair of entrance rooms).

Each HDA should be provided with connectivity to two different IDAs or MDAs. Similarly, each IDA should be provided with connectivity to both MDAs.
Critical systems should have horizontal cabling to two HDAs.
Some potential single points of failure of a tier 4 facility are at:

- The MDA (if the secondary distribution area is not implemented).
- The HDA and horizontal cabling (if redundant horizontal cabling is not installed).

A tier 4 data center must consider all potential physical events that could cause the data center to fail. A tier 4 data center must be provided with specific and in some cases redundant protections against such events.

Tier 4 data centers should consider the potential problems with natural disasters such as seismic events, floods, fire, hurricanes, and storms, as well as potential problems with terrorism and disgruntled employees.

Tier 4 data centers should have control over all aspects of their facility. Tier 4 facilities should be designed in a '2(N+1)' configuration in all modules, systems, and pathways.

All feeders and equipment should be capable of manual bypass for maintenance or in the event of failure. Any failure should automatically transfer power to critical load from a failed system to the alternate system without disruption of power to the critical electronic loads.

A battery monitoring system capable of individually monitoring the impedance or resistance of each cell and temperature of each battery jar and alarming on impending battery failure should be provided to ensure adequate battery operation.

The utility service entrances should be dedicated to the data center and isolated from all noncritical facilities. The building should have at least two utility feeders from different utility substations for redundancy.

The HVAC system of a tier 4 facility includes multiple air conditioning units with the combined cooling capacity to maintain a critical space temperature and relative humidity at design conditions, with sufficient redundant units to allow failure of or service to one electrical switchboard.

If these air conditioning units are served by a water-side heat rejection system, such as a chilled water or condenser water system, the components of these systems are likewise sized to maintain design conditions, with one electrical switchboard removed from service.

This level of redundancy can be obtained by either furnishing two sources of power to each air conditioning unit or dividing the air conditioning equipment among multiple sources of power.

The piping system or systems are dual path, whereby a failure of or maintenance to a section of pipe will not cause interruption of the air conditioning system.

Alternative source for water storage is to be considered when evaporative systems are in place for a tier 4 system.

11.7. Secure Operation:

Managing and operating a datacenter requires to follow tailored processes to reap expected results from the datacenter. While considering standard operating procedure (SOP); security in all the aspects is a most needed aspect. Datacenter SOP should be developed based on Standards like ISO 27001 and best practices like ITIL, which will provide the clear understanding on the control's requirements such as Administrative, Technical and Physical.

SOP should have minimum following aspects in it;

11.7.1. Security of Datacenter:

The datacenter should take all the required security measures to guarantee the confidentiality, integrity, availability of their client's information, networks and services. Appropriate technical and organizational measures should be identified and put in place to ensure minimum level of security.

A comprehensive Information Security framework that includes the essential components such as but not limited to;

- Risk Assessment and Management;
- Configuration Management;
- Change Management;
- Incident Management;
- Secured application acquisition, development and maintenance;
- Business continuity plan and Disaster recovery plan;
- Vulnerability assessment and Audit;
- Internal and external penetration testing and
- Legal and Regulatory compliance identifying, maintaining and monitoring.

Data Centre Team is solely responsible for security of the Data Centre Infrastructure, Network and Communication Infrastructure and Servers and Applications.
The required minimum Service Levels and the management of Data center should include but not be limited to:

- Measurement and Reporting of Service Level achieved
- Service Level target for external Service Providers
- Data Centre commitment on what must be provided to Customers

IT Infrastructure Resources Management:
HVAC – Heating, Ventilation, Air conditioning (Cooling, Humidification, De-humidification)

- Operations Parameter for Data Centre Room
- Minimum required standby Spare Parts available on-site
- Regular monitoring Duties and Responsibilities
- Monitoring external Water Supply for HVAC Status and condition of UPS – Uninterrupted Power Supply
- Minimum required standby Spare Parts available on-site Racks
- Regular Duties and Responsibilities
- Required Spare Parts available on-site

Internal Network and Communication Infrastructure Management
Core Switches
Cabling
Network and Communications management

- Broadband connections

Servers and Applications management

- Servers Management life cycle
- Rack-Mounting of Servers and Cabling
- Installation of Operating System
- Installation of Monitoring Agents and connect to Monitoring System

- Installation of Agents for Backup-System and configuring Backup
- Regular Monitoring by Manual Checks and / or automatic Warnings and Alarm from Monitoring System
- Infrastructure Applications
- Domain Name Servers (DNS)
- Central Authentication Server

Common ICT Processes

- Day to day operations procedures
- Emergency Reboot of Servers as and when required
- Regular Reboot of Serves Scheduled / unscheduled
- Onsite Spare Parts / Reserve Parts for Servers planning and making available
- Replacing faulty parts / parts with limited life time in Servers
- Regular Restoration Tests of Servers and Services
- Access control Process for allowing customer / visitor Data Centre
- Processing access Requests to locked cages / locked racks
- Capacity Management for Data Centre
- New acquisition / Project triggered processes
- Adding / Modify new Hardware to the Data Centre
- removing of Hardware and other Equipment
- Software Life-Cycle Management of Data Centre related software
- Third party / vendor of Support Contracts
- Regular recurring processes
- Data Centre Capacity Planning / Management

Disaster Recovery Planning

- DR – Tests
- Fail-over Test from public Power Supply to UPS

Asset management

Resources:

- Human Resources – Roles and Responsibilities
- Shift / Rota Planning
- Staff Technical Training and Certifications
- Capacity Building

12. CLOUD SERVICES DIRECTIVES

12.1. Introduction

Cloud computing is the provision of on-demand computing services such as software, operating system, processing power, storage and other hardware resource over the internet or Network.

Cloud computing is a model of enabling global, appropriate, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, four deployment models and three service models.

Instead of owning their own computing infrastructure or data centers, companies can rent access to anything from applications to storage from a cloud service provider to avoid the upfront cost and maintain their own IT Infrastructure.

Proper and well-designed datacenter is mandatory in order to provide cloud services to the customer. The above directives assist to implement the datacenter as per the standards and this directive is appropriate for computing security and implementation.

Cloud security provider should implement strong security controls to ensure the security of customer information which is stored and transmitted in the cloud infrastructure.

Cloud security provider should be certified by standards organization such as ISO27001 and cloud security alliance standards in order to get the confidence of customer and protect the information stored in the cloud infrastructure.

12.2. Cloud Deployment Model

There are four main cloud deployment models that differ pointedly and for which most of the companies select: a public, private, hybrid and a community.

12.2.1. Public cloud

A public cloud is a type of computing in which a service provider makes resources available to the public via the internet. Resources vary by provider but may include storage capabilities, applications or virtual machines. Services are always available to customer and resources are controlled by the cloud service provider. Public cloud can be accessed beyond boundaries.

12.2.2. Private cloud

A private cloud is a type of computing which is restricted to specific organization or institute and it is accessed via their private secured network. This type of cloud computing are managed Cloud deployment model where cloud services are used exclusively by a single Customer and resources are controlled by that Customer. A private cloud may be owned, managed and operated by the organization itself or a third party and may exist on premises or off premises. Private clouds pursue to set a closely controlled boundary around the private cloud based on limiting the customers to a single organization.

12.2.3. Community cloud

Cloud deployment model where cloud services exclusively support and are shared by a specific collection of customers who have shared requirements and a relationship with one another, and where resources are controlled by at least one member of this collection. A community cloud may be owned, managed and operated by one or more of the organizations in the community, a third party or some combination of them, and it may exist on or off premises. Community clouds limit participation to a group of Customers who have a shared set of objectives, in contrast to the openness of public clouds, while community clouds have broader participation than private clouds.

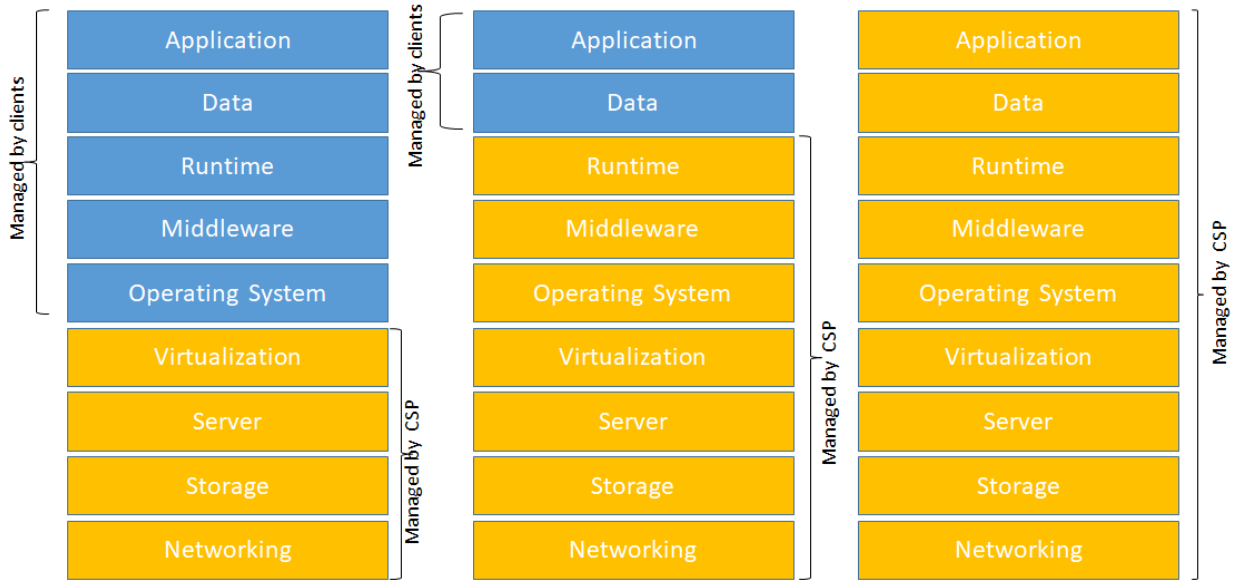
12.2.4. Hybrid cloud

This cloud infrastructure is combination of two or more clouds (private, community or public) that remain as an individual organization but connected together by technology to enable Mobility. Hybrid clouds are often used for redundancy or load-balancing purposes for example, applications within a private cloud could be configured to utilize computing resources from a public cloud as needed during peak capacity times.

12.3. Cloud Service Model

There are many different types of cloud services, each involving different types of technology and assets. We give an overview below, we use this model later to indicate the different contribution of clients and cloud service provider.

Figure 1.1



12.3.1. Infrastructure as a Service

Infrastructure-as-a-Service (IaaS) denotes to the essential requirements and building blocks of computing that can be rented, physical or virtual servers, storage and networking.

In IaaS the provider offers storage (virtual file systems) or computing resources (virtual CPUs), accessible online. Examples include Amazon's Elastic Compute Cloud, Google's Compute Engine, Amazon Simple Storage Service, Google Cloud Storage, Microsoft Windows Azure Storage, Rackspace, Dropbox etc.

12.3.2. Platform as a Service (Paas)

Platform as a service denotes to cloud computing services that supply an on-demand environment for developing, testing, delivering, and managing software applications.
Platform as a service is designed to make it easier for developers to quickly create web or mobile apps, without worrying about setting up or managing the underlying infrastructure of servers, storage, network, and databases needed for development.
Platform-as-a-Service provides tools and software that developers need to build applications on top of that could include middleware, database management, operating systems, and development tools.
In Platform as a service, the provider distributes a platform for customers to run web and normal applications.

12.3.3. Software as a Service

Software-as-a-Service (SaaS) is the distribution of applications-as-a-service and it is a method for delivering software applications over the Internet, on demand and typically on a subscription basis. With SaaS, cloud providers host and manage the software application and underlying infrastructure, and handle any maintenance, like software upgrades and security patching.
In Software as a service, the provider deliver complete application via the internet such as email servers ,email clients, document editors and customer relationship management systems.
Users connect to the application over the Internet, usually with a web browser on their phone, tablet, or PC.

12.4. Facilities

Facilities are the basic IT resources which underlies all types of cloud services (IaaS, PaaS, and SaaS), network, housing, cooling, and power.

12.5. Organization-Human resources

Organization are the human resources, the processes and the policies and procedures that maintain the facilities and support the delivery of services.

Management of the Provider's human resources is largely out of the control of the Customer. The Customer's due -diligence processes should include an understanding of the Provider's human resources and ongoing information security awareness training practices.
Cloud service provider needs to conduct regular basis for assessing the employment screening process and security awareness training program as per the ISO 27001 controls and cloud security alliance standards.

12.6. Cloud Infrastructure

The Datacenter should be above Tier 3 to implement the cloud infrastructure and it is mandatory to follow the standards and procedures.

The main differences between cloud service categories relate to how control is shared between Customer and Provider, which is usually implicates the level of responsibility for both parties. It should be noted that in public cloud services , the customer hardly has control over hardware, and it is up to which virtual components, applications and software are managed by the different parties that differentiates the cloud service categories.
Software as a Service gives customers with the minimum amount of control, but Infrastructure as a Service provides the most control for the customer.

Figure 1.1 shows how control is usually shared between the Cloud Service Provider and the customer.
The customer needs to discuss with the Cloud service provider on suitable provision of information security roles and responsibilities.
The information security roles and responsibilities of both parties should be stated in an agreement. The cloud service customer should identify and manage its relationship with the customer support and care function of the cloud service provider.

The cloud service provider should agree and document an appropriate allocation of information security roles and responsibilities with its cloud service customers, its cloud service providers, and its suppliers.

12.7. Asset management and monitoring

Asset management and monitoring are processes and it needs to be regulated as per ISO 27001 and cloud security alliance standards.
In the case of cloud computing, many resources and assets are managed and monitored by the provider, but the customers might need to manage some assets and resources usually the more abstract and high-level assets and resources.

Customer runs applications on platform as a service, the provider manages the hardware, operating system and applications services but the customer needs to manage the apps running on the platform.

Similarly, the provider manages all assets from hardware to applications service in software as a service but the customer needs to manage the user account provisioning and customization.

Asset managements is crucial administrative tasks in cloud computing, and it is mandatory also from a security perspective. Standards are essential to allow customers integrate asset management interface.

12.8. Cloud Security

Below security measures needs to be considered in the cloud environment.

- Physical Security
- Network and Infrastructure Security (Systems, Hosts and Network)

- Application and DB Security
- Security and Compliance
- Information Security
- Software Security
- Security Operation and Management
- Business con

12.9. Physical Security

Cloud service provider must enforce the physical security as per the ISO27001 controls and it must be implemented and followed in a professional manner and the detailed control mapping is mentioned in the Annex A.

In a cloud environment, Individual entity environments should be physically and administratively separate from each other.

Customers utilizing a public or otherwise shared cloud must ensure that their environments are adequately isolated from the other cloud tenants.

In addition to enforcing separation between Customer environments, segmentation may also be recommended within a Customer's environment to isolate its sensitive servers as per ISO 27001 and cloud security alliance standards.

Segmentation on a cloud computing infrastructure must provide a level of isolation equivalent to that feasible through physical network separation.

Proper mechanism and process should be in place to ensure appropriate isolation may be required at the network, operating system and application layers; and most importantly, there should be guaranteed isolation of data that is stored.

Cloud tenant environments must be isolated from each other such that they can be considered separately managed entities with no connectivity between them.

Providers should test segmentation between all entities within their control at least biannually and demonstrate results.

Any systems or components shared by the Customers in multi-tenant environments, including the Hypervisor and underlying systems, must not provide an access path between environments.

The cloud service provider needs to take ownership of the segmentation between Customers and verify that it is effective and provides adequate isolation between individual Customer environments.

The cloud service provider must ensure the segmentation between customer environments and the Provider's own environment, and between client environments and other untrusted environments.

The Customer is responsible for the proper configuration of any segmentation controls implemented within its own environment and for ensuring that effective isolation is maintained components.

Cloud services involve physical resources located within the Provider environment (including DR Infrastructure) that are accessed remotely from the Customer's environment.

Physical security controls need to be implemented which will protect the provider's infrastructure as well as the customer infrastructure.

Cloud service provider ensure the segmentation where Cloud service Providers shared clouds provide services to multiple Customers whose data and virtual components co-exist in the same physical location and are managed by the same physical systems as those of other Customers.

12.10. Network and Infrastructure Security

Cloud service provider must enforce the network security as per the ISO27001 controls and it must be implemented and followed in a professional manner and the detailed control mapping is mentioned in the Annex A.

Cloud service provider must ensure the network security by implementing either virtual or physical firewall network segmentation at the infrastructure level and the firewalls at the hypervisor and VM level.

Cloud service provider must ensure the network segmentation by implementing either virtual or physical switch with the provision of VLAN tagging or zoning in addition to firewalls.

Cloud service provider must ensure the implementation of Intrusion prevention systems at the hypervisor level, VM level or both, to detect and block unwanted traffic.

A segmented cloud environment exists when the Provider enforces isolation between Customers in multitenant environments. Environments where Customers run their applications in separate logical partitions using separate database management system images and do not share disk storage or other resources.

As per ISO 27001 and cloud security alliance standards, the environments where organizations use the same application image on the same server and are only separated by the access control system of the operating system or the application.

Strong, two - factor authentication should be implemented as per ISO 27001 standards and cloud security alliance standards.

Virtualized servers that are individually dedicated to a particular Customer, including any virtualized storage such as Storage Area Networks (SANs), Network Attached Storage (NAS) or virtual database servers.

Environments where organizations use different images of an application on the same server and are only separated by the access control system of the operating system or the application.

12.11. Applications and Database Security

Environments where organizations' data is stored in the same instance of the database management systems data store.

12.12. Security and Compliance

Proactive testing, identification and mitigation of vulnerabilities are an important part of achieving and maintaining compliance ISO 27001 and cloud security alliance standards that utilize cloud services and systems.

Cloud service provider must ensure that the proper controls requirements is in place to protect the Data Breaches, unavailability, Account hijacking, malicious code.

There are six distinct areas of vulnerability management: web application vulnerability testing, internal network vulnerability scanning, external network vulnerability scanning, external penetration internal penetration testing and segmentation testing and Scoping is a critical element of vulnerability management.

Customers need to ensure that they have properly identified all in - scope systems and services, including those provided by the Provider, those for which the Customer and Provider have shared responsibility and those that fall uniquely to the Customer (e.g., on - premises, private cloud, hybrid systems, or applications or systems that the Customer maintains). Penetration testing is used to confirm segmentation controls intended to constrain scope, and to proactively identify vulnerabilities that could be exploited to allow an attacker to breach these boundaries.

Testing vulnerabilities in the cloud also requires an in - depth understanding of the cloud deployment model to determine responsibility when it comes to performing the appropriate testing exercise.

It is critical to understand the aspects of the environment that will be tested by the Provider and those that will be required to be tested by the Customer. It is not enough to identify responsibility by physical system, as each entity may have distinct or shared responsibility for aspects of a physical system (e.g., physical hardware, hypervisor, guest OS, application, configuration).

These responsibilities will vary depending on cloud service delivery model (i.e., IaaS, SaaS, and PaaS) or other division of control.

Where shared responsibility exists for vulnerability testing activities, the Customer and Provider should cooperate to ensure that these tests are performed, and vulnerabilities are resolved. It is ultimately the Customer's responsibility to provide evidence that all required tests have been performed.

All public - facing web applications must be protected, either by deploying an automated technical solution that detects and prevents web - based attacks or by employing application vulnerability security testing in accordance with ISO 27001 control requirements.

If a Provider is providing a web application, the application should be either protected by a web application Firewall (or similar solution) or tested by the Provider. Providers that expose APIs to their Customers should also perform testing and reporting on those APIs.

If it is the Customer's hosting web application, the customer should perform the web application vulnerability security testing as part of its ISO27001 and cloud security alliance standards.

Providers should recognize this requirement and support these required testing activities (e.g., by supporting the ability to disable controls that would impede controlled testing, by supporting applications that may perform these operations or offering a service to perform these services).

12.13. Information Security

IT governance by the cloud service provider is a significant concern for a cloud service customer, then customers are advised to establish whether a provider complies with one or more of these governance and management standards.

Cloud service customers must be aware that compliance with standards does not ensure effective security. In addition to confirming compliance, cloud customers must continually review service provider security controls to ensure they are properly defined and enforced.

There are also some standards that deal specifically with governance and management of information security, including the identification of risks and the implementation of security controls to address these risks.

The ISO/IEC 27000 series [1 9] of standards is probably the most widely recognized and used set of standards relating to the security of ICT (Information and Communication Technology) systems. The core standards are 27001 and 27002, with 27001 containing the requirements relating to an information security management system and 27002 describing a series of controls that address specific aspects of the information security management system.

ISO/IEC 27001 is an advisory standard that is meant to be interpreted and applied to all types and sizes of organization s according to the information security risks they face.
In practice, this flexibility gives users a lot of latitude to adopt the detailed information security controls that make sense to them but can make compliance testing more complex than some other formal certification schemes.

ISO/IEC 27002 is a collection of security controls (often referred to as best practices) that are often used as a security standard.

Cloud service customers often have a requirement to audit the IT systems and related processes that they use.

Audit requirements can stem from the regulatory environment that applies to the customer, or they may arise from business policies or IT security policies adopted by the customer organization.

The requirement to audit is likely to apply to the use of cloud services as well as to the in-house systems of the customer. As a result, there is a need to audit the systems and processes of the cloud service provider.

12.14. Security Operations and Management

12.14.1. Incident response

Customers need to be notified when an issue, incident, or breach has occurred and the impact to environment or to their data. Issues, incidents and data breaches should be communicated by the Provider to all affected Customers in a timely manner.
Customers should also consider whether their Provider requires all Customers to immediately notify the Provider of potential breaches in their environments, allowing the Provider to respond more quickly to contain the breach and minimize its impact to other Customers.
Based on the type of cloud service category used –relating to facilitating the storage, processing or transmitting of cardholder data each phase of the incident response life cycle is affected at a different level.
Notification processes and timelines should be included in SLAs, and incident response plans should include notification requirements.

Customers should contractually require data breach notification from their Providers in clear and clear-cut language, taking into consideration the need to comply with local and global Regulatory/breach laws, data privacy, security incident management and breach notification requirements.

12.14.2. Forensics Investigation

Incident investigation may involve consideration of legal and jurisdiction requirements, and these requirements should be included in SLAs or operational agreements.

The potential for Customer data to be captured by third parties during a breach investigation should also be clearly understood.

Forensic functionality should be specified in service level objectives (SLOs) incorporated into the SLA between the Customer and the Provider. SLOs may include requirements for notification, identification, preservation and access to potential evidence sources.
Customers and law enforcement agencies require, and rely on Providers for, forensics support, and these obligations varies depending upon cloud service category as noted below.

In software as a service, the capability for forensics is dependent upon the Provider's support, as Customers have no control over the Provider's environment. Forensics examiners may need to rely on high-level application logs available from the SaaS application. SLOs may include evidence sources such as logs from applications.

In platform as a service, the capability for forensics is shared between Customers and Providers. Customers control the Developed and hosted software application, and hence control forensics capability within the application, automatic logging to an external log server can be configured to capture the

applicable audit trail. However, since the actual operation of the application is within the Provider's controlled infrastructure, Customers must clearly identify Providers' responsibilities with respect to forensics investigation. SLOs may include evidence sources such as logs from the application, web, and database server, guest OS/host, portal, network capture, billing and management portal.

In an infrastructure as a service, the capability for forensics is shared between Customers and Providers. Customers have greater control over the range of potential evidence sources; however, some essential data only exists with Providers and under their control. Customers must clearly identify Providers' responsibilities with respect to forensics investigation. SLOs may include evidence sources such as logs from the cloud network perimeter, DNS servers, virtual machine monitor, APIs, host OS, and network capture, billing and management portal.

12.15. Business continuity and Disaster Recovery

Cloud service provider must develop an organizational requirement for business continuity plans (BCP), fault tolerance, high availability and disaster recovery (DR) controls apply to the Customer's outsourced environments as they do for Customer managed facilities.

Customers should consider whether the Provider's continuity and recovery procedures are enough to meet the Customer's or organizational requirements, and the scope of the cloud service should include any failover sites and systems that might be used to store the customer data in a BCP or DR situation.

The ability to perform tests of the BCP and DR capabilities and to observe results of the Provider's testing should also be considered.

12.16. Control Mapping

This below table represents the responsibilities of the Cloud Service Provider (CSP) and End User (EU) in the Cloud Security as per the ISO27001:2013 Standard, and Cloud Security Standard.
*CSP – Cloud Service Provider
*EU – End User

ISO 27001:2013	IAAS	PAAS	SAAS
A.5 **Information Security Policies** • To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.	CSP	CSP	CSP
A.6 **Organization of information security** • To establish a management framework to initiate and control the implementation and operation of information security within the organization.	CSP	CSP	CSP

ISO 27001:2013	IAAS	PAAS	SAAS
• To ensure the security of teleworking and use of mobile devices.			
A.7 **Human Resource Security** • To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered. • To ensure that employees and contractors are aware of and fulfil their information security responsibilities. • To protect the organization's interests as part of the process of changing or terminating employment.	CSP	CSP	CSP
A.8 **Asset Management** • To identify organizational assets and define appropriate protection responsibilities. • To ensure that information receives an appropriate level of protection in accordance with its importance to the organization. • To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.	CSP, EU	CSP, EU	CSP
A.9 **Access Control** • To limit access to information and information processing facilities. • To ensure authorized user access and to prevent unauthorized access to systems and services. • To make users accountable for safeguarding their authentication information. • To prevent unauthorized access to systems and applications.	CSP, EU	CSP, EU	CSP, EU
A.10 **Cryptography** • To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.	CSP, EU	CSP, EU	CSP
A.11 **Physical & Environmental Security** • To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities. • To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.	CSP	CSP	CSP
A.12 **Operation Security**	CSP, EU	CSP, EU	CSP

ISO 27001:2013	IAAS	PAAS	SAAS
• To ensure correct and secure operations of information processing facilities. • To ensure that information and information processing facilities are protected against malware. • To protect against loss of data. • To record events and generate evidence. • To ensure the integrity of operational systems. • To prevent exploitation of technical vulnerabilities. • To minimize the impact of audit activities on operational systems.			
A.13 **Communication Security** • To ensure the protection of information in networks and its supporting information processing facilities. • To maintain the security of information transferred within an organization and with any external entity.	CSP, EU	CSP, EU	CSP
A.14 **System acquisition, development and maintenance** • To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks. • To ensure that information security is designed and implemented within the development lifecycle of information systems. • To ensure the protection of data used for testing.	CSP, EU	CSP, EU	CSP
A.15 **Supplier Relationships** • To ensure protection of the organization's assets that is accessible by suppliers. • To maintain an agreed level of information security and service delivery in line with supplier Agreements	CSP, EU	CSP, EU	CSP
A.16 **Information security incident management** • To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.	CSP	CSP	CSP
A.17 **Information security aspects of business continuity management** • Information security continuity shall be embedded in the organization's business continuity management systems. • To ensure availability of information processing facilities.	CSP, EU	CSP, EU	CSP
A.18 **Compliance**	CSP, EU	CSP, EU	CSP, EU

ISO 27001:2013	IAAS	PAAS	SAAS
• To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements. • To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.			

Cloud Security Standard	IAAS	PAAS	SAAS
AIS-01 Application & Interface Security Application Security	CSP,EU	CSP,EU	CSP
AIS-02 Application & Interface Security Customer Access Requirements	CSP,EU	CSP,EU	CSP
AIS-03 Application & Interface Security Data Integrity	CSP,EU	CSP,EU	CSP,EU
AIS-04 Application & Interface Security Data Security / Integrity	CSP,EU	CSP,EU	CSP,EU
AAC-01 Audit Assurance & Compliance Audit Planning	CSP,EU	CSP,EU	CSP,EU
AAC-02 Audit Assurance & Compliance Independent Audits	CSP,EU	CSP,EU	CSP,EU
AAC-03 Audit Assurance & Compliance Information System Regulatory Mapping	CSP	CSP	CSP
BCR-01 Business Continuity Management & Operational Resilience Business Continuity Planning	CSP	CSP	CSP
BCR-02 Business Continuity Management & Operational Resilience Business Continuity Testing	CSP	CSP	CSP
BCR-03 Business Continuity Management & Operational Resilience Datacenter Utilities / Environmental Conditions	CSP	CSP	CSP
BCR-04 Business Continuity Management & Operational Resilience Documentation	CSP	CSP	CSP
BCR-05 Business Continuity Management & Operational Resilience Environmental Risks	CSP	CSP	CSP
BCR-06 Business Continuity Management & Operational Resilience Equipment Location	CSP	CSP	CSP
BCR-07 Business Continuity Management & Operational Resilience Equipment Maintenance	CSP	CSP	CSP
BCR-08 Business Continuity Management & Operational Resilience Equipment Power Failures	CSP	CSP	CSP
BCR-09 Business Continuity Management & Operational Resilience Impact Analysis	CSP	CSP	CSP
BCR-10 Business Continuity Management & Operational Resilience Policy	CSP	CSP	CSP
BCR-11 Business Continuity Management & Operational Resilience Retention Policy	CSP	CSP	CSP
CCC-01 Change Control & Configuration Management New Development / Acquisition	CSP,EU	CSP,EU	CSP
CCC-02 Change Control & Configuration Management Outsourced Development	CSP,EU	CSP,EU	CSP
CCC-03 Change Control & Configuration Management Quality Testing	CSP,EU	CSP,EU	CSP,EU

Cloud Security Standard	IAAS	PAAS	SAAS
CCC-04 Change Control & Configuration Management Unauthorized Software Installations	CSP,EU	CSP,EU	CSP,EU
CCC-05 Change Control & Configuration Management Production Changes	CSP,EU	CSP,EU	CSP,EU
DSI-01 Data Security & Information Lifecycle Management Classification	CSP,EU	CSP,EU	CSP
DSI-02 Data Security & Information Lifecycle Management Data Inventory / Flows	CSP,EU	CSP,EU	CSP,EU
DSI-03 Data Security & Information Lifecycle Management Ecommerce Transactions	CSP,EU	CSP,EU	CSP
DSI-04 Data Security & Information Lifecycle Management Handling / Labeling / Security Policy	CSP	CSP	CSP
DSI-05 Data Security & Information Lifecycle Management Non-Production Data	CSP,EU	CSP,EU	CSP
DSI-06 Data Security & Information Lifecycle Management Ownership / Stewardship	CSP,EU	CSP,EU	CSP
DSI-07 Data Security & Information Lifecycle Management Secure Disposal	CSP	CSP	CSP
DCS-01 Datacenter Security Asset Management	CSP	CSP	CSP
DCS-02 Datacenter Security Controlled Access Points	CSP	CSP	CSP
DCS-03 Datacenter Security Equipment Identification	CSP	CSP	CSP
DCS-04 Datacenter Security Off-Site Authorization	CSP,EU	CSP,EU	CSP,EU
DCS-05 Datacenter Security Off-Site Equipment	CSP,EU	CSP,EU	CSP
DCS-06 Datacenter Security Policy	CSP	CSP	CSP
DCS-07 Datacenter Security Secure Area Authorization	CSP	CSP	CSP
DCS-08 Datacenter Security Unauthorized Persons Entry	CSP	CSP	CSP
DCS-09 Datacenter Security User Access	CSP,EU	CSP,EU	CSP,EU
EKM-01 Encryption & Key Management Entitlement	CSP,EU	CSP,EU	CSP
EKM-02 Encryption & Key Management Key Generation	CSP,EU	CSP,EU	CSP,EU
EKM-03 Encryption & Key Management Sensitive Data Protection	CSP,EU	CSP,EU	CSP,EU
EKM-04 Encryption & Key Management Storage and Access	CSP,EU	CSP,EU	CSP,EU
GRM-01 Governance and Risk Management Baseline Requirements	CSP,EU	CSP,EU	CSP
GRM-02 Governance and Risk Management Data Focus Risk Assessments	CSP	CSP	CSP
GRM-03 Governance and Risk Management Oversight	CSP	CSP	CSP
GRM-04 Governance and Risk Management Program	CSP	CSP	CSP
GRM-05 Governance and Risk Management Support/Involvement	CSP	CSP	CSP
GRM-06 Governance and Risk Management Policy	CSP	CSP	CSP
GRM-07 Governance and Risk Management Policy Enforcement	CSP,EU	CSP,EU	CSP,EU
GRM-08 Governance and Risk Management Policy Impact on Risk Assessments	CSP,EU	CSP,EU	CSP
GRM-09 Governance and Risk Management Policy Reviews	CSP	CSP	CSP
GRM-10 Governance and Risk Management Risk Assessments	CSP	CSP	CSP
GRM-11 Governance and Risk Management Risk Management Framework	CSP	CSP	CSP
HRS-01 Human Resources Asset Returns	CSP	CSP	CSP
HRS-02 Human Resources Background Screening	CSP	CSP	CSP

Cloud Security Standard	IAAS	PAAS	SAAS
HRS-03 Human Resources Employment Agreements	CSP	CSP	CSP
HRS-04 Human Resources Employment Termination	CSP	CSP	CSP
HRS-05 Human Resources Mobile Device Management	CSP,EU	CSP,EU	CSP,EU
HRS-06 Human Resources Non-Disclosure Agreements	CSP,EU	CSP,EU	CSP,EU
HRS-07 Human Resources Roles / Responsibilities	CSP,EU	CSP,EU	CSP,EU
HRS-08 Human Resources Technology Acceptable Use	CSP,EU	CSP,EU	CSP,EU
HRS-09 Human Resources Training / Awareness	CSP	CSP	CSP
HRS-10 Human Resources User Responsibility	CSP,EU	CSP,EU	CSP,EU
HRS-11 Human Resources Workspace	CSP	CSP	CSP
IAM-01 Identity & Access Management Audit Tools Access	CSP	CSP	CSP
IAM-02 Identity & Access Management Credential Lifecycle / Provision Management	CSP,EU	CSP,EU	CSP,EU
IAM-03 Identity & Access Management Diagnostic / Configuration Ports Access	CSP	CSP	CSP
IAM-04 Identity & Access Management Policies and Procedures	CSP	CSP	CSP
IAM-05 Identity & Access Management Segregation of Duties	CSP	CSP	CSP
IAM-06 Identity & Access Management Source Code Access Restriction	CSP	CSP	CSP,EU
IAM-07 Identity & Access Management Third Party Access	CSP,EU	CSP,EU	CSP,EU
IAM-08 Identity & Access Management Trusted Sources	CSP,EU	CSP,EU	CSP,EU
IAM-09 Identity & Access Management User Access Authorization	CSP,EU	CSP,EU	CSP
IAM-10 Identity & Access Management User Access Reviews	CSP,EU	CSP,EU	CSP
IAM-11 Identity & Access Management User Access Revocation	CSP,EU	CSP,EU	CSP,EU
IAM-12 Identity & Access Management User ID Credentials	EU	CSP,EU	CSP,EU
IAM-13 Identity & Access Management Utility Programs Access	EU	CSP,EU	CSP
IVS-01 Infrastructure & Virtualization Security Audit Logging / Intrusion Detection	CSP	CSP	CSP
IVS-02 Infrastructure & Virtualization Security Change Detection	CSP,EU	CSP,EU	CSP,EU
IVS-03 Infrastructure & Virtualization Security Clock Synchronization	CSP,EU	CSP,EU	CSP,EU
IVS-04 Infrastructure & Virtualization Security Information System Documentation	CSP	CSP	CSP
IVS-05 Infrastructure & Virtualization Security Vulnerability Management	CSP	CSP	CSP
IVS-06 Infrastructure & Virtualization Security Network Security	CSP	CSP	CSP
IVS-07 Infrastructure & Virtualization Security OS Hardening and Base Controls	CSP	CSP	CSP
IVS-08 Infrastructure & Virtualization Security Production / Non-Production Environments	CSP	CSP	CSP
IVS-09 Infrastructure & Virtualization Security Segmentation	CSP	CSP	CSP
IVS-10 Infrastructure & Virtualization Security VM Security - Data Protection	CSP	CSP	CSP
IVS-11 Infrastructure & Virtualization Security Hypervisor Hardening	CSP	CSP	CSP
IVS-12 Infrastructure & Virtualization Security Wireless Security	CSP	CSP	CSP
IVS-13 Infrastructure & Virtualization Security Network Architecture	CSP	CSP	CSP
IPY-01 Interoperability & Portability APIs	CSP,EU	CSP,EU	CSP,EU
IPY-02 Interoperability & Portability Data Request	CSP	CSP	CSP
IPY-03 Interoperability & Portability Policy & Legal	CSP	CSP	CSP

Cloud Security Standard	IAAS	PAAS	SAAS
IPY-04 Interoperability & Portability Standardized Network Protocols	CSP	CSP	CSP
IPY-05 Interoperability & Portability Virtualization	CSP	CSP	CSP
MOS-01 Mobile Security Anti-Malware	EU	CSP,EU	CSP,EU
MOS-02 Mobile Security Application Stores	EU	CSP,EU	CSP,EU
MOS-03 Mobile Security Approved Applications	EU	CSP,EU	CSP,EU
MOS-04 Mobile Security Approved Software for BYOD	CSP	CSP	CSP
MOS-05 Mobile Security Awareness and Training	CSP	CSP	CSP
MOS-06 Mobile Security Cloud Based Services	CSP,EU	CSP,EU	CSP,EU
MOS-07 Mobile Security Compatibility	CSP	CSP	CSP
MOS-08 Mobile Security Device Eligibility	EU	EU	CSP
MOS-09 Mobile Security Device Inventory	CSP	CSP	CSP
MOS-10 Mobile Security Device Management	CSP	CSP	CSP
MOS-11 Mobile Security Encryption	CSP	CSP	CSP
MOS-12 Mobile Security Jailbreaking and Rooting	EU	EU	EU
MOS-13 Mobile Security Legal	CSP	CSP	CSP
MOS-14 Mobile Security Lockout Screen	CSP	CSP	CSP
MOS-15 Mobile Security Operating Systems	CSP,EU	CSP,EU	CSP,EU
MOS-16 Mobile Security Passwords	EU	EU	EU
MOS-17 Mobile Security Policy	CSP	CSP	CSP
MOS-18 Mobile Security Remote Wipe	CSP,EU	CSP,EU	CSP,EU
MOS-19 Mobile Security Patches	EU	EU	EU
MOS-20 Mobile Security Users	CSP,EU	CSP,EU	CSP,EU
SEF-01 Security Incident Management, E-Discovery, & Cloud Forensics Contact / Authority Maintenance	CSP	CSP	CSP
SEF-02 Security Incident Management, E-Discovery, & Cloud Forensics Incident Management	CSP	CSP	CSP
SEF-03 Security Incident Management, E-Discovery, & Cloud Forensics Incident Reporting	CSP	CSP	CSP
SEF-04 Security Incident Management, E-Discovery, & Cloud Forensics Incident Response Legal Preparation	CSP	CSP	CSP
SEF-05 Security Incident Management, E-Discovery, & Cloud Forensics Incident Response Metrics	CSP	CSP	CSP
STA-01 Supply Chain Management, Transparency, and Accountability Data Quality and Integrity	CSP	CSP	CSP
STA-02 Supply Chain Management, Transparency, and Accountability Incident Reporting	CSP	CSP	CSP
STA-03 Supply Chain Management, Transparency, and Accountability Network / Infrastructure Services	CSP,EU	CSP,EU	CSP,EU
STA-04 Supply Chain Management, Transparency, and Accountability Provider Internal Assessments	CSP	CSP	CSP
STA-05 Supply Chain Management, Transparency, and Accountability Supply Chain Agreements	CSP,EU	CSP,EU	CSP,EU
STA-06 Supply Chain Management, Transparency, and Accountability Supply Chain Governance Reviews	CSP,EU	CSP,EU	CSP,EU
STA-07 Supply Chain Management, Transparency, and Accountability	CSP,EU	CSP,EU	CSP,EU

Cloud Security Standard	IAAS	PAAS	SAAS
Supply Chain Metrics			
STA-08 Supply Chain Management, Transparency, and Accountability Third Party Assessment	CSP,EU	CSP,EU	CSP,EU
STA-09 Supply Chain Management, Transparency, and Accountability Third Party Audits	CSP,EU	CSP,EU	CSP,EU
TVM-01 Threat and Vulnerability Management Anti-Virus / Malicious Software	EU	EU	CSP
TVM-02 Threat and Vulnerability Management Vulnerability / Patch Management	EU	EU	CSP
TVM-03 Threat and Vulnerability Management Mobile Code	CSP,EU	CSP,EU	CSP,EU