**Introduction and Executive Summary**

The Ondo State Government recognizes the **strategic importance of a state-of-the-art data center** as the backbone of its digital infrastructure. This proposal outlines a comprehensive plan to construct and equip a new data center that will serve as a **secure hub for government data and digital services**, driving e-governance, improving service delivery, and supporting the state’s broader development goals. The data center is envisioned to **empower Ondo State’s digital transformation**, much like similar initiatives in other regions have bolstered local economies and governance. For example, Edo State’s recently launched data center serves as a secure hub for government and business data, described as *“vital for digital operations, empowering local businesses and the entire region with secure data storage options”* ([Gov. Obaseki unveils first data centre, digital policy in Edo - Nigerian NewsDirect](https://nigeriannewsdirect.com/gov-obaseki-unveils-first-data-centre-digital-policy-in-edo/#:~:text=%E2%80%9CEdo%E2%80%99s%20new%20data%20center%20acts,for%20government%20and%20business%20data)). By investing in its own facility, Ondo State aims to enhance data sovereignty, reliability, and security for critical government applications.

**Objectives:** The primary objectives of this project are: (1) to **centralize and protect government data** in a resilient facility, (2) to **ensure high availability of IT services** for all state ministries and departments, (3) to **provide a scalable platform** for future e-government initiatives and digital services (such as citizen databases, healthcare, education, and e-commerce platforms), and (4) to **boost investor confidence and digital economy growth** in Ondo State. In alignment with Nigeria’s push for digital governance, this data center will position the state as a technology-friendly hub and could even offer secure data services to local businesses in the future.

**Project Scope:** The project encompasses the **design, construction, and outfitting** of a modern data center facility. Key components within scope include a raised-floor server room, an FM200 fire suppression system, a redundant power infrastructure (integrating both conventional grid/diesel power and solar energy backups), advanced cooling and environmental controls, robust physical security measures (biometric access and CCTV surveillance), structured cabling with cable trays, high-end HPE server and storage hardware mounted in standard racks, and all necessary support systems (earthing, lighting, staging area, etc.). The proposal details each of these components and explains how they come together to meet **Tier III data center standards** (ensuring 99.982% uptime per year ([What are Data Center Tiers? | Glossary | HPE](https://www.hpe.com/us/en/what-is/data-center-tiers.html#:~:text=of%20downtime%20annually%29))).

**Expected Outcomes:** Upon completion, Ondo State will have a **fully operational data center** that guarantees continuous availability of digital services, even amid power outages or other disruptions. This will lead to improved efficiency in governance (as downtime of critical applications will be minimized) and create the foundation for new digital initiatives (e.g., state-wide ERP systems, e-health records, intelligent transportation systems, etc.). In the long term, the data center will contribute to cost savings by consolidating IT infrastructure, and it will strengthen data security and privacy for the state’s information. The project also has a capacity-building aspect: through its implementation and operationalization, state IT personnel will gain valuable expertise in managing modern data center infrastructure.

In summary, this proposal provides a **detailed blueprint** for building a reliable and secure data center for Ondo State. It covers the technical design, justifications for each design choice, implementation roadmap, operational plan, risk management, budget estimates in Nigerian Naira (NGN), and vendor considerations. By approving and executing this project, the Ondo State Government will be taking a **bold step towards transforming the state into a digital hub**, unlocking a brighter future for its citizens and economy in the digital age ([UniCloud Africa and Benue Digital Infrastructure to build data center in Makurdi, Nigeria - DCD](https://www.datacenterdynamics.com/en/news/unicloud-africa-and-benue-digital-infrastructure-to-build-data-center-in-makurdi-nigeria/" \l ":~:text=The%20project%20is%20estimated%20to,be%20completed%20in%20six%20months)).

**Project Scope and Design**

This section describes the **scope of work and the design blueprint** for the new Ondo State data center. The design follows industry best practices for reliability, efficiency, and security. Key components of the data center infrastructure are outlined below, each corresponding to specific functional requirements:

**Raised Floor System**

The data center’s server hall will feature a **raised access floor** system, consisting of modular 600mm x 600mm floor panels installed on adjustable pedestals about 300mm above the concrete subfloor. The raised floor creates an under-floor plenum that serves two purposes: it provides a pathway for routing power and network cabling, and it functions as an air distribution chamber for cooling. **Cool air from the CRAC (Computer Room Air Conditioner) units will be delivered into the underfloor space and rise through perforated tiles in cold aisles**, directly in front of server racks ([Move to a Hot Aisle/Cold Aisle Layout | ENERGY STAR](https://www.energystar.gov/products/data_center_equipment/16-more-ways-cut-energy-waste-data-center/move-hot-aislecold-aisle-layout#:~:text=aisle%20layout%20involves%20lining%20up,to%20the%20CRAC%20unit%20intakes)). This arrangement ensures efficient cooling by feeding cold air to server intakes and allowing hot exhaust air to be expelled and returned to AC units via a separate path (hot aisle). Additionally, the raised floor allows easy access for running or reconfiguring cables and pipelines in the future, providing flexibility for expansions or changes without major construction ([Data Center Design: Raised Floor Versus Slab Floor? - Interconnections - The Equinix Blog](https://blog.equinix.com/blog/2011/03/02/raised-floor-versus-slab-floor-the-debate-rages-on/#:~:text=Consequently%2C%20business%20needs%20become%20the,floor%20approach%20has%20an%20advantage)). The floor panels will be anti-static to prevent electrostatic discharge, and they will have sufficient load-bearing capacity to support heavy rack equipment (typical panels can handle distributed loads of 1,000+ kg per square meter).

**FM200 Fire Suppression System**

To protect sensitive equipment from fire without the collateral damage that water-based sprinklers would cause, the facility will be equipped with a **FM200 clean-agent fire suppression system**. FM200 (HFC-227ea) is a colorless, non-toxic gas that extinguishes fire rapidly by absorbing heat **without leaving any residue** on equipment ([FM200 Fire Suppression Systems for Server-Room, Data-Center in Ikeja - Other Services, Technologies Automation Systems | Jiji.ng](https://jiji.ng/ikeja/other-services/fm200-fire-suppression-systems-for-server-room-data-center-zIzeWMmtkm8XdahjTj9mVZRO.html#:~:text=FM,Panels)). The system will include an array of FM200 cylinders, piping network, smoke and heat detectors, and automatic release nozzles throughout the server room and adjacent technical areas. In the event of a fire trigger, the FM200 gas will be discharged to suppress the fire within seconds, minimizing potential damage and downtime. The use of FM200 is **safe for human occupants at design concentration and electrically non-conductive**, meaning it won’t short-circuit live equipment ([FM200 Fire Suppression Systems for Server-Room, Data-Center in Ikeja - Other Services, Technologies Automation Systems | Jiji.ng](https://jiji.ng/ikeja/other-services/fm200-fire-suppression-systems-for-server-room-data-center-zIzeWMmtkm8XdahjTj9mVZRO.html#:~:text=FM,Panels)). The fire suppression system will be integrated with the data center’s alarm panel and emergency power-off controls to ensure synchronized responses (e.g., cutting power if needed when the gas is released). Manual release stations and alarms (siren-strobes) will also be installed as per safety standards.

**Redundant Power Supply with Solar Integration**

**Power reliability is paramount** for data center operations. The facility will implement a **redundant power architecture** combining utility grid power, backup generators, uninterruptible power supplies (UPS), and a solar photovoltaic (PV) system for supplemental energy. There will be dual independent power feeds into the data center: one from the main grid (PHCN) and one from a diesel generator backup. In normal operation, the data center will draw from the grid, with the on-site solar PV array and battery storage reducing dependence on grid power by supplying renewable energy during daylight hours. Should the grid supply falter, a high-capacity diesel generator (or generators in N+1 configuration) will automatically start to carry the load. The UPS units (battery-backed, likely lithium-ion or VRLA battery systems) will bridge the gap during the few seconds of transfer, ensuring **no interruption** to the servers. This multi-layered setup guards against Nigeria’s known grid instabilities; between 2017 and 2023 the national grid collapsed 46 times, highlighting the need for on-site generation to maintain uptime ([Solar plus storage is a win-win for Nigeria's booming data centre market and residents | Digitalisation World](https://www.msp-channel.com/blog/58114/solar-plus-storage-is-a-win-win-for-nigerias-booming-data-centre-market-and-residents#:~:text=A%20global%20shortage%20of%20power,new%20wave%20of%20data%20centre)). The inclusion of solar power not only provides an **alternate energy source to reduce generator fuel usage**, but also leverages the region’s sunlight to improve sustainability and lower operating costs over time. With recent high diesel prices and fuel scarcity, solar with battery storage has become an economically attractive complement to generators ([Solar plus storage is a win-win for Nigeria's booming data centre market and residents | Digitalisation World](https://www.msp-channel.com/blog/58114/solar-plus-storage-is-a-win-win-for-nigerias-booming-data-centre-market-and-residents#:~:text=Until%20recently%2C%20businesses%20in%20Nigeria,term%20power%20purchase)). The power system will be designed for **N+1 redundancy** (at minimum) – for example, if the peak IT load requires one 200 kVA UPS, the design will include two (one active, one spare) so that a failure or maintenance event does not disrupt power ([2N vs. N+1: Data Center Redundancy Explained - Digital Realty](https://www.digitalrealty.com/resources/articles/2n-vs-n-1#:~:text=2N%20vs,a%20single%20failure%20or)). Power distribution within the data center will use dual path feeds to each rack (A and B supply) via PDUs (Power Distribution Units), allowing equipment with dual power supplies to be fed from separate sources (further enhancing redundancy). An automatic transfer switch (ATS) will manage switchover between utility and generator power seamlessly. Additionally, a grounding/earthing subsystem will be implemented to tie all electrical systems to a common earth for safety (see **Lighting and Earthing Systems** below).

**Environmental Monitoring Sensors**

To maintain optimal operating conditions and get advance warning of any environmental issues, the data center will deploy a network of **environmental monitoring sensors** throughout the facility. These sensors will continuously track key parameters such as **temperature, humidity, smoke, and water leaks** at various points (e.g. in racks, under the raised floor, near cooling units). The monitoring system (potentially a Data Center Infrastructure Management – DCIM – software or a BMS integration) will aggregate sensor data and alert operators when readings stray outside predefined thresholds. For instance, temperature and humidity sensors will ensure the cooling system is keeping the server inlet air within ASHRAE recommended ranges (approximately 18–27°C and 40–60% relative humidity). If humidity drops too low, the system can warn of static risk; if too high, of condensation risk ([Most Popular Data Center Environmental Sensors | Sunbird DCIM](https://www.sunbirddcim.com/blog/most-popular-data-center-environmental-sensors#:~:text=Humidity%20plays%20an%20important%20role,of%20static%20electricity%20can%20occur)). Leak detectors will be placed on the raised floor (especially near cooling equipment and pipe entry points) to catch any water ingress or condensation leaks early. Smoke sensors (as part of the fire detection system) will identify fire at incipient stages. These **environmental devices can trigger automated responses or alarms** – for example, if temperature rises, alerts can be sent via SMS/email to on-duty staff ([Environmental Monitoring Devices - Opengear](https://opengear.com/products/environmental-monitoring-devices/#:~:text=miOpengear%20environmental%20monitoring%20devices%20detect,your%20IT%20infrastructure%E2%80%99s%20physical%20environment)) ([Environmental Monitoring Devices - Opengear](https://opengear.com/products/environmental-monitoring-devices/#:~:text=Set%20up%20automated%20response%20sequences,warning%20levels%20to%20critical%20alerts)). The monitoring framework will log data over time, allowing trend analysis for capacity planning (e.g. identifying hot spots or gradual cooling degradation). Integration with the UPS and power systems will also allow monitoring of power quality (voltage, load levels) and trigger alerts on anomalies (voltage drops, phase imbalance, etc.). By keeping a close eye on the infrastructure’s physical environment, the risk of downtime due to environmental factors is greatly mitigated ([Environmental Monitoring Devices - Opengear](https://opengear.com/products/environmental-monitoring-devices/#:~:text=miOpengear%20environmental%20monitoring%20devices%20detect,your%20IT%20infrastructure%E2%80%99s%20physical%20environment)).

**Wall Cladding for Insulation and Security**

The data center’s building envelope will be enhanced with **specialized wall cladding** to improve both thermal insulation and physical security. Internally, insulated wall panels (potentially fire-rated composite panels) will be installed to help maintain a stable interior climate by reducing heat exchange with the outside environment. This insulation is crucial for energy efficiency, as it assists the cooling system in keeping temperatures constant without excessive load, even during Nigeria’s hot season. Externally or structurally, the walls will be **reinforced** for security: data center best practices often call for hardened walls to resist forced entry or environmental threats ([What are Data Center Security Requirements? | VIAVI Solutions Inc.](https://www.viavisolutions.com/en-us/what-are-data-center-security-requirements#:~:text=%2A%20Hyperscale%20Data%20Centers%3A%20Large,the%20impact)). The cladding system will likely involve steel-backed panels or concrete augmentation that make the data hall **intrusion-resistant**, deterring break-ins or vandalism. By having few or no windows and secure doors, the facility minimizes access points that could be exploited. Additionally, the cladding and insulation contribute to **fire protection** (by using fire-resistant materials that compartmentalize the server room) and noise reduction (dampening noise from generators or equipment so as not to disturb neighboring areas). In essence, the wall cladding provides a **double benefit**: it keeps the interior environment controlled and efficient, and it creates a robust outer shell to protect the sensitive IT equipment inside from both environmental elements and physical attacks.

**Cable Trays for Structured Cabling**

The data center will implement a **structured cabling system** using overhead or underfloor **cable trays and ladder racks**. All data and power cables running between equipment racks, patch panels, and external entry points will be neatly organized on these trays. This approach ensures that cabling is not tangled or strewn across the floor, but rather is routed along predefined pathways, separated by type (power vs. data) to avoid interference. Using cable trays as part of structured cabling brings multiple benefits: it **keeps cables organized, labeled, and easily traceable**, which simplifies maintenance and reduces errors when performing changes ([A Guide to Data Center Structured Cabling - Dataspan](https://dataspan.com/blog/a-guide-to-data-center-structured-cabling/#:~:text=1)). For example, network cables will be bundled and color-coded by function (LAN, SAN, etc.) and run in the trays from the server racks to the network switches in a clean fashion, preventing the “spaghetti cabling” phenomenon that can plague unplanned setups ([A Guide to Data Center Structured Cabling - Dataspan](https://dataspan.com/blog/a-guide-to-data-center-structured-cabling/#:~:text=,that%20addresses%20labeling%2C%20technical%20specifications)) ([A Guide to Data Center Structured Cabling - Dataspan](https://dataspan.com/blog/a-guide-to-data-center-structured-cabling/#:~:text=1)). The trays also protect cables from being damaged by foot traffic or equipment movement. By confining cables to trays, airflow under the floor or above racks is less obstructed, aiding cooling (since large bundles of cables can impede air if not managed). Moreover, in the event a cable needs replacement or new cables need to be added, the trays provide a clear route to lay or remove cables without disturbing other systems. The design will include vertical cable managers within racks and horizontal trays above racks, guiding cables to the main pathways. Overall, the structured cabling via cable trays will ensure the data center’s network and electrical distribution is **tidy, standards-compliant, and scalable**, supporting reliable communications among all devices.

**HPE Standard Racks for Equipment Housing**

All servers, storage devices, and network equipment in the data center will be installed in **industry-standard 19-inch racks**, specifically **HPE G2 Enterprise series racks** (or equivalent models). These HPE racks are 42U tall enclosures, designed to **support heavy IT equipment loads, provide proper airflow, and integrate cable management and security features** ( [HPE G2 Enterprise Series Racks | HPE Store US](https://buy.hpe.com/us/en/rack-power-infrastructure-products/racks/server-racks/racks/hpe-g2-enterprise-series-racks/p/1009803311#:~:text=Do%20you%20need%20a%20rack,models%20include%20packaging%20specifically%20designed)). Each rack has perforated front and rear doors to allow maximum air circulation (cold air enters through the front, hot air exits out the rear). The racks come with built-in cable management channels and brackets, which will be used to route power cords and data cables neatly within each enclosure, preventing obstruction of airflow. They also feature lockable doors and side panels, contributing to physical security by restricting access to only authorized personnel. HPE’s racks are known for their **structural integrity** – they can support substantial weight (up to ~1360 kg of equipment) and even allow for shipping fully loaded if needed ([HPE G2 Enterprise Series Racks | HPE Store US](https://buy.hpe.com/us/en/rack-power-infrastructure-products/racks/server-racks/racks/hpe-g2-enterprise-series-racks/p/1009803311#:~:text=HPE%20G2%20Enterprise%20Series%20Racks,choice%20of%20power%20and)). The design will allocate an appropriate number of racks for current needs (for example, an initial deployment of say 4–6 racks for servers and storage, and additional racks for network and auxiliary equipment), with space to add more racks as the data center grows. We will arrange the racks in a hot aisle/cold aisle layout (alternating rows as described under the raised floor section) to optimize cooling efficiency. Each rack will also be equipped with intelligent rack PDUs (power strips with monitoring) to distribute power to devices and measure energy usage per rack. Using HPE standard racks ensures compatibility with the HPE servers and hardware we plan to deploy, and these racks come with a 10-year warranty due to their durable design ( [HPE G2 Enterprise Series Racks | HPE Store US](https://buy.hpe.com/us/en/rack-power-infrastructure-products/racks/server-racks/racks/hpe-g2-enterprise-series-racks/p/1009803311#:~:text=security%2C%20structural%20integrity%2C%20cooling%20and,for%20IT%20workloads%20that%20require)). In summary, the racks form the **framework of the data center**, holding all critical IT gear in an organized, secure manner while supporting effective cooling and cabling.

**Staging Area for Equipment Testing and Deployment**

The project will include the setup of a dedicated **staging area** within the data center facility (but outside the main server hall) for the preparation and testing of equipment. The staging area is essentially a **workspace for configuration, burn-in, and maintenance** activities. All new servers, storage systems, or network devices will first be received and unpacked in this staging area rather than in the live data hall. This is important for maintaining cleanliness and order in the main data center – packaging materials can introduce dust and other contaminants, so unpacking and assembling equipment in a separate room prevents debris from affecting running systems ([Staging Area | Enterprise Data Center Design and Methodology](https://flylib.com/books/en/3.157.1.81/1/#:~:text=This%20area%20should%20be%20outside,and%20stir%20up%20contaminants)) ([Staging Area | Enterprise Data Center Design and Methodology](https://flylib.com/books/en/3.157.1.81/1/#:~:text=,done%20in%20the%20staging%20area)). In the staging area, equipment can be configured, updated, and tested (e.g. initial power-on, hardware diagnostics, loading firmware and OS) on workbenches or test racks before being moved onto the raised floor. This process, often referred to as a “burn-in” or verification test, helps catch any hardware issues early ([Staging Area | Enterprise Data Center Design and Methodology](https://flylib.com/books/en/3.157.1.81/1/#:~:text=,how%20things%20fit%20into%20place)). The area will be equipped with sufficient power outlets (including some UPS-backed outlets) and network connectivity to simulate the data center environment for these tests. Proper cooling or air conditioning will also be ensured since multiple devices might be running simultaneously during staging. Additionally, when decommissioning or replacing equipment, the staging area can serve as a place to transfer the gear, wipe data, and pack it without disturbing the operations in the main hall. We will enforce the same security measures for the staging area as for the data center (restricted access, possibly CCTV coverage) because devices in staging may contain or will contain sensitive configurations ([Staging Area | Enterprise Data Center Design and Methodology](https://flylib.com/books/en/3.157.1.81/1/#:~:text=,in%20the%20data%20center%20itself)). By including a staging area in the design, we **streamline maintenance and deployment workflows** – staff have a safe, controlled space to work on systems, thereby reducing the risk of errors or contamination in the live environment. The area will be sized to allow handling of large equipment; as a guideline, unpacking a large enterprise server can require a clear floor space of around 18 feet by 10 feet (approximately 200 sq. ft.) ([Staging Area | Enterprise Data Center Design and Methodology](https://flylib.com/books/en/3.157.1.81/1/#:~:text=,Area)), so our staging room will accommodate such needs.

**HVAC Systems for Cooling**

Effective cooling is critical to maintain server performance and hardware longevity. The data center will use a **redundant HVAC (Heating, Ventilation, and Air Conditioning) system** specifically designed for precision cooling of IT equipment. We will likely deploy multiple precision air conditioning units (CRAC or In-Row coolers) in an N+1 configuration – for example, if load calculations determine 2 units can handle the peak cooling load, a third unit will be installed as a spare. These units will continuously regulate the temperature and humidity of the server room. **Cold air will be delivered under the raised floor** (as mentioned earlier) and dispensed through perforated tiles in cold aisles ([Move to a Hot Aisle/Cold Aisle Layout | ENERGY STAR](https://www.energystar.gov/products/data_center_equipment/16-more-ways-cut-energy-waste-data-center/move-hot-aislecold-aisle-layout#:~:text=aisle%20layout%20involves%20lining%20up,to%20the%20CRAC%20unit%20intakes)). Hot aisle containment may be implemented, meaning hot air from the back of racks is confined and directed back to AC returns without mixing with cold air ([How to make your data center cooling more cost effective - DCD](https://www.datacenterdynamics.com/en/opinions/how-make-your-data-center-cooling-more-cost-effective/#:~:text=Traditionally%2C%20cool%20air%20from%20a,evaporative%2C%20free%20and%20liquid%20cooling)). This significantly increases cooling efficiency by ensuring only hot exhaust is cooled and preventing hot spots. The target environment conditions will follow international standards (like ASHRAE recommendations), for instance maintaining about 22°C and 50% relative humidity in the cold aisle. Each AC unit will have its own sensors and controllers; they will also be tied into the environmental monitoring system for centralized oversight. The design may incorporate **economizer modes or free cooling** if feasible (for example, using cooler ambient air at night or during harmattan seasons to assist cooling). Additionally, the HVAC design includes ventilation for fresh air intake and pressurization to prevent dust ingress, as well as filtration systems to maintain air quality. The system will be supported by backup power (UPS/generator) to ensure cooling continues even during power outages, as **loss of cooling can quickly lead to overheating and equipment failure**. To further enhance efficiency, hot aisle/cold aisle layout is planned as described: fronts of servers face each other in cold aisles, and backs face backs in hot aisles ([Move to a Hot Aisle/Cold Aisle Layout | ENERGY STAR](https://www.energystar.gov/products/data_center_equipment/16-more-ways-cut-energy-waste-data-center/move-hot-aislecold-aisle-layout#:~:text=The%20hot%20aisle%20%2Fcold%20aisle,the%20front%20of%20servers%20to)). This prevents recirculation of hot air into server intakes, thereby avoiding the scenario where each subsequent row of servers would otherwise ingest progressively hotter air ([Move to a Hot Aisle/Cold Aisle Layout | ENERGY STAR](https://www.energystar.gov/products/data_center_equipment/16-more-ways-cut-energy-waste-data-center/move-hot-aislecold-aisle-layout#:~:text=it%20is%20one%20of%20the,the%20front%20of%20servers%20to)) ([Move to a Hot Aisle/Cold Aisle Layout | ENERGY STAR](https://www.energystar.gov/products/data_center_equipment/16-more-ways-cut-energy-waste-data-center/move-hot-aislecold-aisle-layout#:~:text=%28CRAC%29%20unit%20to%20server%20racks,to%20the%20CRAC%20unit%20intakes)). Overall, the HVAC setup will be robust and intelligent, capable of cooling the initial IT load and **scalable to increased loads** by adding additional cooling modules or units in the future.

**HPE Servers and SAN Storage Systems**

At the heart of the data center will be the **IT infrastructure** consisting of enterprise-grade **Hewlett Packard Enterprise (HPE) servers and Storage Area Network (SAN) systems**. We propose using HPE ProLiant rack servers for compute needs and an HPE SAN (such as an HPE MSA or Nimble storage array) for centralized storage. HPE servers are known for their reliability, performance, and management features in mission-critical environments. They will be equipped with the latest Intel Xeon or AMD EPYC processors, ample memory, and redundant components (e.g., dual power supplies connected to separate power feeds, RAID-configured disks for the OS) to ensure high availability. The SAN will provide shared storage for all the servers, enabling efficient data management and robust data protection. **SAN architecture offers numerous advantages**: it allows multiple servers to connect to a common pool of storage over high-speed links, which improves storage utilization and simplifies backups and disaster recovery ([Storage Area Network (SAN): Comprehensive Guide and Benefits](https://www.myworkdrive.com/blog/storage-area-network-guide/#:~:text=,considerations%20during%20deployment%20and%20maintenance)). By implementing a SAN, we ensure that critical databases and applications can be clustered or load-balanced across servers, and if one server fails, another can access the same data and take over (fault tolerance). The SAN will use either Fibre Channel or iSCSI connectivity; if Fibre Channel, we will include FC switches and host bus adapters in the servers. The storage array itself will be configured with enterprise disks or SSDs in a RAID for data redundancy, and it will support features like snapshots and replication (which is useful for backup and potential offsite DR). **Centralized storage also enhances data protection and recovery** – for instance, it’s easier to implement an offsite replication of a SAN than backing up many individual servers, thereby improving our disaster recovery capabilities ([Storage Area Network (SAN): Comprehensive Guide and Benefits](https://www.myworkdrive.com/blog/storage-area-network-guide/#:~:text=,considerations%20during%20deployment%20and%20maintenance)). Additionally, SAN performance is typically superior to local disks, which will benefit the state’s database and application workloads (enhanced I/O throughput and lower latency). We plan to size the initial deployment for current needs (for example, X terabytes of usable storage and Y compute nodes to run all existing applications), but with headroom to scale. Both the HPE servers and SAN can be expanded (add more drives, or additional server nodes) to accommodate growth. All these HPE components will be housed in the aforementioned racks and connected via structured cabling to the network and power. By standardizing on HPE, the state can also leverage integrated management software like HPE OneView for infrastructure management. In summary, the compute and storage systems in this design will offer **high performance, centralized management, and robust data sharing**, forming the technological core that meets the state’s present and future IT requirements.

**Lighting and Earthing Systems**

The facility will include **adequate lighting and a comprehensive earthing (grounding) system** as part of the infrastructure. Proper **lighting** is important for both safety and ease of maintenance – the data center rooms (server hall, electrical rooms, etc.) will be outfitted with LED lighting that provides bright, even illumination. We will implement automatic emergency lights as well, which will switch on via battery backup in case of power loss, to ensure technicians are never stranded in the dark and can safely shut down or restore systems during an outage. The lighting design will consider energy efficiency (using motion sensors or zoning to turn off lights when areas are unoccupied) and will avoid fixtures that emit excessive heat into the data hall. Additionally, the color temperature of the lights will be chosen to reduce eye strain during long maintenance sessions.

The **earthing (grounding) system** is an absolutely critical aspect of data center design for both equipment protection and human safety. All major components – including the electrical panels, UPS, generators, racks, and even the raised floor pedestals – will be bonded to a common earth ground grid. A low-impedance ground connection ensures that any stray currents or lightning surges are safely diverted into the earth rather than passing through equipment. **Earthing prevents electrical faults from damaging equipment and protects personnel** by providing a path of least resistance for fault currents ([Role of Earthing in Data Centers - Manav Energy](https://manavenergy.com/role-of-earthing-in-data-centers/#:~:text=Earthing%20is%20a%20critical%20component,earthing%20in%20data%20center%20infrastructure)). In Nigeria’s environment where lightning strikes or power surges can occur, a good earthing system will shunt these high voltages away from sensitive circuits, thereby **avoiding catastrophic failures or fires**. It also helps in stabilizing the voltage reference for all devices, which can reduce issues related to electromagnetic interference. The design will comply with international and local standards (such as IEEE/IEC grounding standards and Nigerian regulations) – typically a mesh of copper earth bars or rods will be buried around the facility, and thick grounding conductors will connect every rack and electrical unit to this mesh. We will also ensure that the neutral-ground bonding is correctly implemented at the source (depending on whether a TN-S or TN-C-S earthing arrangement is used from the transformer). Proper earthing contributes to **minimizing downtime and equipment damage** ([Importance of Good Earthing System for Data Centres](https://intertech.com.co/earthing-system-for-data-centre/#:~:text=Importance%20of%20Good%20Earthing%20System,from%20damage%20due%20to)); as noted in industry best practices, it equalizes electrical potentials and creates a safe path for fault currents, thereby protecting both hardware and people ([Grounding Your Data Center: Advice and Planning](https://www.amcoenclosures.com/grounding-your-data-center-advice-and-planning/#:~:text=Grounding%20Your%20Data%20Center%3A%20Advice,it%20protects%20sensitive%20equipment)). The earthing system will be tested thoroughly (earth resistance tests) before the data center goes live.

**Biometric Access Controls and CCTV for Security**

The data center will enforce strict **physical security controls** to prevent unauthorized access, given the sensitive nature of the equipment and data inside. **Biometric access control systems** will be installed at all entry points to the data center (main entrance, server room door, and other critical zones like the network or electrical rooms if separated). This means that personnel will need to authenticate with something like a fingerprint or iris scan (in combination with an access card or PIN for multi-factor security) to unlock the doors. Only authorized staff – e.g., data center engineers, network admins, and certain government officials – will be enrolled in the biometric system, and access can be tiered (for instance, some staff might only have access to the staging area but not the main server hall). The system will log all entries and exits for audit purposes.

In addition, a comprehensive **CCTV surveillance system** will be deployed to monitor the interior and exterior of the data center 24/7. High-definition security cameras will cover all aisles in the server room, the entrances, the perimeter of the building, and utility areas such as the generator and UPS rooms. The cameras will be networked to a central video management system with ample recording storage (recordings will be kept for a defined period, such as 90 days, for investigation if needed). Live feeds can be monitored by security personnel at a control room, and the system may be configured to raise alarms on certain events (e.g., motion detected during off-hours).

Physical access to a data center is typically limited to very few points and people. *“Data Center access is extremely limited, with few entry points, 24/7 security guards on duty, video surveillance, and use of employee badges and/or biometric readers”* ([What are Data Center Security Requirements? | VIAVI Solutions Inc.](https://www.viavisolutions.com/en-us/what-are-data-center-security-requirements#:~:text=enter%20or%20leave%20their%20facility,and%2For%20biometric%20readers%20in%20use)). In line with this best practice, we will also have on-site security guards present at the facility around the clock. The guards will secure the exterior and verify identities as needed. The combination of guards, biometric locks, and CCTV creates **multiple layers of security** – an intruder would have to get past fencing/gates (if any), then building entry (biometric lock), and still be caught on camera and by guards. This deters sabotage, theft of equipment, or any attempt to tamper with the servers. We will also include policies such as escorted visitor access (any maintenance contractors or visitors must be signed in and accompanied). Furthermore, the data center design itself supports security: **reinforced walls, minimal access points, and secure enclosures** (racks have locks too) to protect hardware ([What are Data Center Security Requirements? | VIAVI Solutions Inc.](https://www.viavisolutions.com/en-us/what-are-data-center-security-requirements#:~:text=%2A%20Hyperscale%20Data%20Centers%3A%20Large,the%20impact)). All these measures together ensure that the government’s critical systems are physically shielded from unauthorized interference, complementing the cybersecurity measures that protect the data logically.

**Detailed Justifications for Each Component**

Each component of the data center design has been carefully chosen for a specific role in achieving a reliable and secure facility. Below, we provide detailed justifications for each major component listed in the scope, explaining **why it is necessary** and the **long-term benefits** it brings to the Ondo State data center.

**1. Raised Floor System:** The raised floor is justified by the flexibility and efficiency it introduces. It creates an underfloor space for both cabling and air distribution, which means we can route power and network cables cleanly and out of the way, and deliver cooling evenly across the room. This design **prevents cable clutter** (that could impede airflow or make maintenance difficult) and enables **better cooling performance** by using the plenum for cold air delivery ([Move to a Hot Aisle/Cold Aisle Layout | ENERGY STAR](https://www.energystar.gov/products/data_center_equipment/16-more-ways-cut-energy-waste-data-center/move-hot-aislecold-aisle-layout#:~:text=aisle%20layout%20involves%20lining%20up,to%20the%20CRAC%20unit%20intakes)). In the long term, the raised floor allows easier upgrades – for example, adding a new cable or pipe in the future can be done by simply lifting floor tiles rather than major construction. This adaptability is a long-term benefit as the data center evolves; *Equinix notes that the accessible raised floor plenum makes it easier to run new conduits or cooling lines in a live data center without disruption* ([Data Center Design: Raised Floor Versus Slab Floor? - Interconnections - The Equinix Blog](https://blog.equinix.com/blog/2011/03/02/raised-floor-versus-slab-floor-the-debate-rages-on/#:~:text=Consequently%2C%20business%20needs%20become%20the,floor%20approach%20has%20an%20advantage)). Additionally, a raised floor can protect equipment by providing a buffer in case of minor flooding (any water will accumulate under the floor, away from servers, and leak sensors will detect it). Overall, the raised floor is **necessary for a high-density, well-organized data center**, offering benefits in cooling efficiency, maintainability, and scalability.

**2. FM200 Fire Suppression:** Traditional water sprinkler systems are unsuitable for data centers because water can destroy electrical equipment. The FM200 fire suppression system is **necessary to quickly extinguish fires without damaging electronics**. FM200 deploys in seconds and leaves no residue, so servers can potentially remain operational or be brought back online quickly after a discharge ([FM200 Fire Suppression Systems for Server-Room, Data-Center in Ikeja - Other Services, Technologies Automation Systems | Jiji.ng](https://jiji.ng/ikeja/other-services/fm200-fire-suppression-systems-for-server-room-data-center-zIzeWMmtkm8XdahjTj9mVZRO.html#:~:text=FM,Panels)). This minimizes downtime – a critical benefit since even a small fire incident with water sprinklers could mean total loss of IT gear and prolonged outages. FM200 is also safe for occupied areas at design concentrations, meaning staff won’t be harmed if they are present during discharge (though they should evacuate as a precaution). The long-term impact is improved **business continuity and asset protection**: the data center’s risk from fire is mitigated to a very low level, and insurance premiums may also be favorably impacted by having a proper clean-agent fire system. The system’s detectors often catch overheated equipment or electrical shorts early (pre-action), so even before suppression, warnings are given. In summary, FM200 protects the state’s investment in hardware and data by ensuring that a fire is **snuffed out rapidly without collateral damage**, which is essential for meeting high availability goals.

**3. Redundant Power Supply (with Solar):** Power redundancy is **crucial in a region with grid instability** – without it, a single power outage could bring down government services. By having UPS units and generators (N+1 redundancy), we ensure continuous power even if one component fails or during maintenance. The integration of a solar power system, while not strictly standard in all data centers, is justified by the local context of Nigeria’s energy landscape. Frequent grid failures and high diesel costs mean alternative energy can significantly improve uptime and reduce operational cost ([Solar plus storage is a win-win for Nigeria's booming data centre market and residents | Digitalisation World](https://www.msp-channel.com/blog/58114/solar-plus-storage-is-a-win-win-for-nigerias-booming-data-centre-market-and-residents#:~:text=A%20global%20shortage%20of%20power,new%20wave%20of%20data%20centre)) ([Solar plus storage is a win-win for Nigeria's booming data centre market and residents | Digitalisation World](https://www.msp-channel.com/blog/58114/solar-plus-storage-is-a-win-win-for-nigerias-booming-data-centre-market-and-residents#:~:text=Until%20recently%2C%20businesses%20in%20Nigeria,term%20power%20purchase)). Solar panels with batteries provide a clean energy source that can buffer the facility against daytime outages or supplement power to reduce generator runtime. Over the long term, this translates to **cost savings on fuel** and a smaller carbon footprint. Redundant power architecture (dual feeds, multiple UPS/generators) has the benefit of making the data center compliant with Tier III standards (able to undergo maintenance on power systems without downtime) ([What are Data Center Tiers? | Glossary | HPE](https://www.hpe.com/us/en/what-is/data-center-tiers.html#:~:text=of%20downtime%20annually%29)). It also provides resilience against a variety of scenarios: if one UPS fails, another takes over; if fuel supply is a problem, solar can carry some load, etc. In essence, this multi-layered power solution is necessary to achieve the target **99.98% availability**, and its benefits are uninterrupted services, reduced risk of data loss, and predictable power management despite external power volatility.

**4. Environmental Monitoring Sensors:** These sensors are necessary to give the operations team **real-time visibility into environmental conditions** that could threaten equipment. Heat, humidity, water leaks, or smoke can wreak havoc if unnoticed – servers can overheat and crash, condensation can cause short circuits, small leaks can lead to big floods if undetected. The sensors act as an early warning system. For instance, if AC fails and temperature rises, an alert from temperature sensors allows staff to respond or initiate backup cooling before servers hit thermal shutdown. Humidity sensors ensure we avoid static buildup (too dry) or condensation (too humid) which could damage hardware ([Most Popular Data Center Environmental Sensors | Sunbird DCIM](https://www.sunbirddcim.com/blog/most-popular-data-center-environmental-sensors#:~:text=Humidity%20plays%20an%20important%20role,of%20static%20electricity%20can%20occur)). Water leak sensors around CRAC units or pipes catch leaks from air conditioners early, preventing damage to floors or equipment. Smoke detectors integrated with the fire system can detect electrical smoldering before it becomes a flame. The benefit of all these is **preventive maintenance and rapid response** – problems are identified and resolved ideally *before* any downtime occurs. Long-term, this preserves equipment health (running devices within recommended temperatures/humidity extends their lifespan) and improves uptime. It also aids capacity planning; for example, analyzing temperature trends might indicate the need for more cooling as load increases. In summary, environmental monitoring is an inexpensive but highly valuable component that is necessary for **protecting the data center’s physical environment** and ensuring issues are tackled proactively rather than reactively ([Environmental Monitoring Devices - Opengear](https://opengear.com/products/environmental-monitoring-devices/#:~:text=miOpengear%20environmental%20monitoring%20devices%20detect,your%20IT%20infrastructure%E2%80%99s%20physical%20environment)).

**5. Wall Cladding (Insulation & Security):** Insulating and reinforcing the data center walls is justified by two main needs: **energy efficiency and physical security**. Insulation keeps the cooling costs down by maintaining a stable internal temperature – less heat ingress means AC units work less, saving energy particularly in the long run (over years, efficient insulation can significantly reduce electricity use for cooling). It’s akin to thermally fortifying the building so the expensive chilled air inside doesn’t escape or get heated by outside weather. On the security front, reinforced cladding and possibly ballistic-rated materials make the facility **more secure against intrusion or civil disturbances**. Government data centers could be targets for vandalism or theft; having hardened walls and limited entry points buys time and deters attempts. As noted in security standards, high-security data centers incorporate *“reinforcement of data center walls”* as a measure against breaches ([What are Data Center Security Requirements? | VIAVI Solutions Inc.](https://www.viavisolutions.com/en-us/what-are-data-center-security-requirements#:~:text=%2A%20Hyperscale%20Data%20Centers%3A%20Large,the%20impact)). Long-term, this physical hardening protects the state’s data and equipment from not just intentional harm but also from natural elements (e.g., storms, high winds). The cladding could also add fire resistance (some panels have fire retardant cores), adding minutes or hours of protection in a fire scenario which is critical for evacuation and suppression efforts. Thus, though wall cladding is a construction element, its necessity is tied to creating a **secure and stable environment** for the IT gear, with benefits in operational cost savings (energy efficiency) and risk reduction (security against threats).

**6. Cable Trays and Structured Cabling:** Structured cabling with cable trays is necessary to handle the complex web of connections in a data center in an organized manner. If we neglect this and run cables ad-hoc, we’ll quickly end up with tangled cables that make it difficult to trace connections, increasing the risk of unplugging the wrong cord or not knowing which cable is which during expansion. Cable trays keep everything **neatly arranged and documented** ([A Guide to Data Center Structured Cabling - Dataspan](https://dataspan.com/blog/a-guide-to-data-center-structured-cabling/#:~:text=1)). The benefit is easier maintenance: technicians can identify and replace cables faster (trays often allow labeling or color-coding along runs) ([A Guide to Data Center Structured Cabling - Dataspan](https://dataspan.com/blog/a-guide-to-data-center-structured-cabling/#:~:text=Naturally%2C%20a%20cabling%20system%20includes,the%20visibility%20of%20the%20system)). It also improves airflow since cables are not blocking vents or laying on the floor. Long-term, structured cabling supports **scalability** – as new equipment is added, new cables can be laid in the trays systematically without disturbing the existing ones. It also supports high-performance networking: for example, running many high-speed cables in parallel is more feasible when you have proper pathways and spacing (to reduce interference and meet bend radius requirements). The cable trays also contribute to safety (no tripping hazards, no rats nest of cables that could catch fire or overheat). In summary, while cable trays might seem like a simple infrastructure, their presence is crucial for a **professional, reliable installation**, reducing human error and ensuring the data center’s cabling meets international standards for performance and safety ([A Guide to Data Center Structured Cabling - Dataspan](https://dataspan.com/blog/a-guide-to-data-center-structured-cabling/#:~:text=1)).

**7. HPE Standard Racks:** Using standard 19-inch racks (specifically HPE’s robust models) is necessary to **properly mount and secure all equipment**. Free-standing servers or desktops (which one might see in a makeshift server room) are not acceptable in an enterprise data center due to poor cooling and security. The enclosed racks provide a stable structure with integrated cooling airflow management (perforated doors) and physical security (lockable panels). The HPE racks in particular are built to **industry standards and with high quality**, meaning they can hold heavy servers, including during seismic events or vibrations, without tipping or bending ([HP 42U - 642 1200mm](https://dsiracks.com/store/p/hp-42u-642-1200mm#:~:text=HP%2042U%20,space%20for%20structuring%20data%20centers)). They also come with features like cable management and baying (to join racks in a row) which is important for maintaining an orderly environment. By choosing HPE racks to go along with HPE servers, we ensure perfect compatibility in mounting and possibly get support/warranty synergy. The benefit of using these racks long-term is that they will **protect the equipment and facilitate maintenance** – sliding rails and modular mounting make it easier to swap hardware; containment of equipment in racks means the cold aisle/hot aisle strategy works effectively (hot air is directed through rear of rack etc.). Another benefit is that racks allow for **scalability**: we can populate some racks now and have empty U-space or even empty racks for future equipment, all within a controlled layout. The racks also typically include ground bonding points ensuring all mounted equipment is properly earthed. In sum, standard racks are a **must-have foundation** for any data center, and the HPE models provide the durability, security, and functionality to support high-density IT equipment now and into the future ( [HPE G2 Enterprise Series Racks | HPE Store US](https://buy.hpe.com/us/en/rack-power-infrastructure-products/racks/server-racks/racks/hpe-g2-enterprise-series-racks/p/1009803311#:~:text=Do%20you%20need%20a%20rack,models%20include%20packaging%20specifically%20designed)).

**8. Staging Area:** A dedicated staging area is justified by the need for a **controlled environment to handle equipment outside the live data floor**. This is often overlooked in smaller setups, but for a government data center, the volume of equipment and frequency of changes (patching, replacing servers, etc.) requires a space to do that work without risking the operational environment ([Staging Area | Enterprise Data Center Design and Methodology](https://flylib.com/books/en/3.157.1.81/1/#:~:text=At%20least%20one%20dedicated%20staging,processed%20in%20the%20staging%20area)). The staging area prevents dust and particles from packing materials entering the server room (which could clog filters or damage hardware) ([Staging Area | Enterprise Data Center Design and Methodology](https://flylib.com/books/en/3.157.1.81/1/#:~:text=This%20area%20should%20be%20outside,and%20stir%20up%20contaminants)). It also isolates the noise and commotion of unboxing and assembling gear from the quiet, clean data hall. In the long run, having a staging room increases efficiency and safety: staff can do all configuration work on a table or spare rack with full light and space, reducing the chance of dropping a screw into a live server or accidentally bumping a production system. It also serves as a buffer for deliveries and shipments, meaning the main data center doors don’t need to be frequently opened (maintaining security and environment). The staging area supports **proper burn-in testing** (initial run of equipment at load to catch failures) without impacting live systems ([Staging Area | Enterprise Data Center Design and Methodology](https://flylib.com/books/en/3.157.1.81/1/#:~:text=,how%20things%20fit%20into%20place)). Long-term benefit: higher reliability of deployed systems (since they were tested) and smoother expansion processes. It also provides temporary storage for spares or for failed components awaiting vendor return, all in a secure location. Thus, the staging area is necessary for **operational excellence and risk mitigation** during any adds, moves, or changes in the data center lifecycle.

**9. HVAC (Cooling) Systems:** Adequate cooling is non-negotiable in a data center – without it, the servers would overheat within minutes and potentially suffer permanent damage or shutdowns. The specific design of having redundant CRAC units and hot/cold aisle containment is justified by the need to maintain **continuous, efficient cooling**. Redundancy (N+1) ensures that even if one cooling unit fails or needs maintenance, the others can handle the load, thus preventing any downtime due to overheating. The hot aisle/cold aisle layout and possibly containment ensure **efficient use of cooling energy**, yielding long-term cost savings by reducing waste (only cooling cold aisles rather than the whole room, and capturing hot air effectively) ([How to make your data center cooling more cost effective - DCD](https://www.datacenterdynamics.com/en/opinions/how-make-your-data-center-cooling-more-cost-effective/#:~:text=Traditionally%2C%20cool%20air%20from%20a,evaporative%2C%20free%20and%20liquid%20cooling)). Over years, these savings are substantial in electricity costs. Moreover, keeping equipment at stable temperatures prolongs their life (electronics running too hot can have exponentially shorter lifespans). The environmental control also prevents condensation or static which can accompany poor HVAC management. In terms of necessity: given Nigeria’s warm climate, high-powered servers would not survive without robust cooling – thus these HVAC systems protect the **state’s IT investment and ensure service continuity**. If cooling were insufficient, the data center could face thermal shutdowns, leading to service outages and potential data loss. Therefore, the HVAC infrastructure with proper redundancy is a **critical component that directly ties to uptime guarantees**. Long-term, a well-designed cooling system can adapt to higher densities (we can add cooling capacity or use in-row cooling for hotspots), providing scalability. In short, HVAC systems are the lifeline that keeps the data center functional 24/7, and our design choices maximize reliability and efficiency in that regard.

**10. HPE Servers and SAN Storage:** Choosing HPE servers and SAN storage is justified by their **performance, reliability, and support ecosystem**. Government workloads often include databases, email systems, portals, and possibly emerging applications like GIS or big data, which demand robust computing and storage. HPE ProLiant servers are industry-leading in uptime and manageability (with tools like Integrated Lights-Out for remote management). This means issues can be detected and addressed swiftly, and the hardware itself has redundant fans, PSUs, and error-checking memory to prevent failures. The SAN is necessary to meet the state’s need for **centralized data management and high availability**. By storing all critical data on a SAN, we can implement advanced features like snapshots (for quick recovery if data is corrupted), replication (to an offsite location for disaster recovery), and clustering (multiple servers accessing the same storage for failover). These are long-term benefits that ensure data integrity and rapid recovery from incidents, aligning with best practices for government data which must be safeguarded. Additionally, a SAN allows for scaling storage independently of servers; as data grows (which it inevitably will with increasing digitization), we can add disks or enclosures without having to overhaul the server infrastructure. Performance-wise, SANs (especially if using flash storage and high-speed interconnects) deliver fast I/O which will keep applications responsive even as user loads increase ([Storage Area Network (SAN): Comprehensive Guide and Benefits](https://www.myworkdrive.com/blog/storage-area-network-guide/#:~:text=,considerations%20during%20deployment%20and%20maintenance)) (e.g., a citizen service portal needs to handle many simultaneous transactions – a SAN helps by handling reads/writes efficiently and sharing the load between servers). HPE as a vendor also ensures we have **local support in Nigeria** and access to enterprise support channels for firmware updates, replacement parts, and consulting. The long-term impact of standardizing on a reputable platform like HPE is reduced risk of hardware incompatibilities, easier maintenance (due to uniform tools and spares), and a solid foundation for future upgrades (HPE’s product roadmap ensures newer gen servers will work with current racks, and SAN can integrate with cloud backup etc.). Thus, the HPE servers and SAN are necessary to meet the performance and reliability requirements and bring significant benefits in **scalability, data protection, and operational manageability**.

**11. Lighting and Earthing:** Good lighting is necessary for practical reasons – technicians must be able to see clearly when working on equipment. This reduces mistakes (like misreading a label or port) and helps in emergencies if staff need to navigate the room quickly. Properly illuminated exits and pathways are also a safety requirement (especially under Nigerian building codes for commercial facilities). The benefit is straightforward: **improved working conditions and safety**, which contributes to efficiency (fast repairs because everything is visible and accessible). Emergency lighting ensures that even in a total power outage scenario, personnel can safely shut down systems or exit, thus protecting lives and equipment (since an uncontrolled dark environment could lead to accidents or equipment mishandling).

Earthing is one of the most critical electrical safety measures. Its necessity cannot be overstated: without earthing, any surge or fault could energize equipment enclosures or the floor, posing deadly shock hazards and destroying sensitive circuits. By **grounding all equipment to a common earth**, we give a safe route for fault currents. As a result, if a short to ground occurs, the surge is carried away and trips protective devices (circuit breakers) quickly ([Guidelines for data center grounding and bonding | Consulting](https://www.csemag.com/articles/guidelines-for-data-center-grounding-and-bonding/#:~:text=Consulting%20www,a%20phase%20conductor%20to)). The long-term benefit is the prevention of cumulative electrical stress on components – minor surges that could slowly degrade electronics are safely discharged, which means the hardware potentially lasts longer without mysterious failures. Also, in lightning-prone areas, a good earthing system can protect the facility from direct or nearby lightning strikes by channeling the energy to ground. This is crucial for a government facility that must be operational during storms. Another benefit is reducing electromagnetic interference; a well-earthed system helps in **equalizing electrical potentials** and thus can reduce data errors or network interference that sometimes occur in poorly grounded setups ([Why grounding is critical to data center uptime](https://www.cablinginstall.com/home/article/16467125/why-grounding-is-critical-to-data-center-uptime#:~:text=Why%20grounding%20is%20critical%20to,low%20resistance%20path%20to%20ground)). In summary, earthing is necessary for **safety and equipment protection**, and its impact is seen in the avoidance of catastrophic electrical incidents and enhanced stability of the electrical system over the data center’s life.

**12. Biometric Access and CCTV:** Physical security components are necessary to protect against unauthorized access which could lead to data breaches, theft, or sabotage. Government data often includes sensitive personal and confidential information; the data center must be off-limits except to vetted individuals. Biometric access control provides a high level of assurance compared to just keys or cards (which can be lost or copied). It ensures **only authorized staff can enter**, and all entries are logged. This deters insider threats as well because there’s accountability. Over time, the biometric system benefits the state by maintaining a secure audit trail and easily revoking access when staff change roles, etc., thereby **reducing the risk of insider-caused incidents**. CCTV is necessary as both a deterrent and an investigative tool. Its presence will dissuade most malicious attempts, and if something does happen, recorded footage can identify culprits or sequence of events. In a live sense, CCTV allows remote monitoring – security personnel can keep an eye on conditions (for example, noticing if an unauthorized person tailgated through a door, or if there’s smoke buildup somewhere). Long-term, these security systems help uphold the **integrity and trustworthiness** of the data center. No matter how good our IT systems are, if someone can physically access servers, they could disrupt services or steal data (e.g., plugging in rogue devices, or damaging equipment). Thus, these controls are as necessary as firewalls in the cyber domain. They bring peace of mind that the state's critical systems are under lock and camera, and they align with global standards which require multi-layer physical security for data centers ([What are Data Center Security Requirements? | VIAVI Solutions Inc.](https://www.viavisolutions.com/en-us/what-are-data-center-security-requirements#:~:text=enter%20or%20leave%20their%20facility,and%2For%20biometric%20readers%20in%20use)). In essence, biometric access and CCTV yield the benefit of **minimizing the threat of physical intrusions** and provide evidentiary support should any incident occur, which is vital for a secure government facility.

**Technical Specifications**

This section provides a detailed breakdown of the technical specifications for the data center’s infrastructure, covering IT hardware, power, cooling, networking, and other critical systems. It also addresses **capacity planning and scalability considerations** to ensure the facility can meet both current needs and future growth.

**Data Center Facility and Space**

* **Location & Building:** The data center will be housed in a dedicated room (or building) within a government-designated site in Ondo State. The estimated server room area is approximately **100 square meters** (for example), which is sufficient for the initial deployment of racks and allows for future expansion. The height will accommodate the raised floor and overhead cabling with a minimum of 3 meters clear height above the raised floor for airflow and equipment clearance.
* **Raised Floor:** 60cm x 60cm anti-static raised floor tiles on adjustable pedestals, providing a finished floor height of **300 mm** above the slab. Floor load rating to support at least 1,200 kg/sq.m, suitable for densely populated racks and equipment.
* **Rack Layout:** Initial installation of **5 server racks** (42U height, 600mm x 1075mm each) in a single row, with another row of 5 racks possible in the future. Racks will be arranged in a hot aisle/cold aisle configuration. An additional **2 network/telecom racks** may be placed for core switches, patch panels, and other networking gear. The design leaves floor space for at least **5-10 additional racks** as expansion (either in the same hall or an adjacent expansion area).
* **Staging Area:** A separate room (~20–30 sq.m) earmarked as the staging area, equipped with workbenches and test rack, as described earlier.

**IT Infrastructure (Compute, Storage, Network)**

* **Servers:** *HPE ProLiant DL380 Gen10* (or Gen11) rack servers (2U each). Initial quantity: **8 servers** populating two racks (with redundancy and room for growth). Each server specification: Dual Intel Xeon Silver/Gold 24-core CPUs (or AMD EPYC equivalent), 256 GB DDR4 RAM, 2 x 600GB 10k SAS drives in RAID1 for OS (with the bulk of storage on SAN), 2 x 10Gb Ethernet ports, 2 x 16Gb Fibre Channel HBA (if SAN is FC-based), dual hot-plug power supplies. These servers will host virtual machines or applications for various state services (they could be clustered using virtualization technology to share load and for high availability).
* **Storage:** *HPE MSA 2060 SAN Storage Array* (or HPE Alletra/Nimble series for more advanced features). Equipped with dual active-active controllers and redundant power. Storage capacity: **50 Terabytes usable**, configured with 20 x 2.4TB 10k SAS drives in RAID-6 (for a balance of capacity and protection) plus 2 x SSD for caching if needed. Supports snapshots and replication. Connectivity: 16Gb Fibre Channel (or 10Gb iSCSI if FC switches are to be avoided). This SAN provides centralized block storage to all the above servers.
* **Network Infrastructure:** To interconnect servers, storage, and provide external connectivity:
  + **Core Switches:** Two redundant core switches (for example, *HPE/Aruba 6300M or Cisco Catalyst 9500* series) with 10GbE ports for server connectivity and 1/10Gb uplinks for building network integration. They will be in a stack or VRRP configuration for high availability. Each server connects to both switches (teamed NICs) for redundancy.
  + **SAN Switches:** Two Fibre Channel switches (e.g., *Brocade 16Gb 24-port*) for the storage network, if FC SAN is used. Each server’s HBA and each storage controller connects to both SAN switches (dual fabric) ensuring no single point of failure in data paths.
  + **Firewall/Router:** For external connectivity and security, a dedicated network firewall (e.g., *Fortinet or Cisco NGFW*) will be installed to manage traffic between the data center network and other state networks or the internet. This ensures segmentation and protection of the data center network.
  + **Structured Cabling:** Cat6A Ethernet cabling for all copper connections (capable of 10 Gbps), and OM4 fiber optic cabling for fiber channel or 10GbE uplinks (with patch panels present in each rack). All cables are labeled and run via the overhead cable trays as described.
* **Capacity and Scalability:** The initial compute and storage setup is estimated to run at ~50% utilization to start, leaving headroom for new applications. We can scale vertically (each server has extra RAM slots and drive bays) and horizontally (adding more servers or disk enclosures) as demand grows. The network switches chosen have spare ports (e.g., using only 50% of ports initially) to accommodate new connections without replacing hardware. The design foresees an ability to at least **double the compute capacity and storage capacity** (to ~100TB) with minimal additional infrastructure, simply by populating existing racks and enclosures. Beyond that, the room space allows adding more racks and an additional storage array if needed, future-proofing for perhaps 5-7 years of growth, depending on the trajectory of the state’s IT needs.

**Power Infrastructure**

* **Power Load Estimation:** Initial IT load is estimated at ~**20 kW** (each fully loaded rack ~4 kW on average, though racks can handle higher densities up to 10 kW if needed in future by adding more cooling). Including cooling and other overhead, total facility load might be ~40 kW. The power systems are designed to accommodate at least **1.5x this load (60 kW)** to ensure overhead for growth.
* **UPS (Uninterruptible Power Supply):** Two modular online double-conversion UPS units, each rated at **80 kVA**. Configured as N+1: one UPS can carry the entire critical load, and the second provides redundancy. They feed separate power distribution paths (A and B feed). Batteries: Valve-Regulated Lead-Acid (VRLA) or Lithium-ion battery banks sized for **15 minutes runtime** at full load (this covers short outages and allows generator startup in longer outages). The UPS output is 230/400V AC, 50Hz, three-phase, which feeds PDUs.
* **Power Distribution:** From UPS outputs, power goes to distribution boards and then to rack PDUs. Each rack will have dual PDUs (A feed and B feed), each rated e.g. 7 kW, to supply the servers. Outlets are IEC C13/C19 for server equipment. Each PDU has monitoring capabilities (for load per phase, etc.). Separate circuits (with their own UPS support or raw utility as appropriate) will feed lighting, HVAC controls, and security systems to isolate them from IT load.
* **Generator:** A diesel generator set rated at **250 kVA** (with an automatic transfer switch). This size can handle the full building load (including cooling) with some margin. If required, two 250 kVA generators could be installed (one redundant) in an N+1 arrangement to further increase reliability – but at a minimum, one generator is in scope. The generator will have an automatic mains failure panel to start it within 5–10 seconds of power outage and transfer load via ATS. Fuel tank capacity for at least 24 hours runtime at full load (~ possibly 3,000 liters depending on efficiency) will be provided on-site. The generator is housed in a sound-attenuated enclosure outdoors, with proper exhaust and fuel safety systems.
* **Solar PV System:** A rooftop or ground-mounted **solar array of ~50 kW** peak output, tied to a battery storage system (perhaps 100 kWh lithium battery bank) and an inverter. This solar system is grid-tied with battery backup: during normal operation it will supply part of the data center load and charge batteries, reducing grid draw. During an outage, it can work in tandem with the UPS (and possibly reduce generator usage if sunlight is available) to prolong runtime. The solar inverter system will synchronize and have an automatic cut-off to prevent backfeeding during grid outages (to protect line workers).
* **Switchgear and Protection:** All electrical panels will include surge protectors and properly rated breakers. An **Automatic Transfer Switch (ATS)** switches between utility and generator on sensing loss of utility. Each UPS output path has isolation and maintenance bypass switches to allow servicing UPS without cutting power to loads (concurrent maintainability is key for Tier III functionality). The earthing system ties into the electrical system as mentioned (to ensure fault currents clear promptly).
* **Scalability:** The power system is scalable by adding another UPS module or battery cabinets if load increases. The generator capacity can also be increased (either by adding a second generator in parallel or replacing with a larger unit) as the infrastructure grows. The solar system, though a supplemental element, can also be expanded with more panels or batteries to further reduce reliance on grid/diesel over time.

**Cooling and HVAC Specifications**

* **Cooling Units:** Three (3) precision cooling CRAC units, each of **20 kW** cooling capacity (for example, Liebert/Vertiv or Schneider in-row units). Cooling configuration: N+1 (2 units handle current load, 1 redundant). They use DX (direct expansion) or chilled water system depending on facility – likely DX (with compressors and condensers) for simplicity. Each unit has its own compressor and fans, with high sensible cooling efficiency tailored for server heat loads.
* **Airflow Management:** Cold aisle containment will be implemented in front of racks – transparent barriers or doors at the row-ends to ensure cold air delivered through floor tiles stays in the cold aisle and doesn’t mix with hot air. Hot aisle can be open or also contained depending on thermal analysis. Perforated floor tiles (with ~25% open area) will be placed only in cold aisles in front of server rack intakes. The layout and tile placement will be designed using cooling CFD analysis if possible to ensure even air distribution.
* **Temperature/Humidity Control:** Each CRAC has temperature and humidity sensors and will maintain conditions at ~22°C setpoint and 50% RH. They are equipped with reheat coils and humidifiers to add heat or moisture if needed (to prevent over-cooling or over-drying). ASHRAE guidelines (18-27°C range, 40-60% RH) will be used as reference for safe operating envelope ([Most Popular Data Center Environmental Sensors | Sunbird DCIM](https://www.sunbirddcim.com/blog/most-popular-data-center-environmental-sensors#:~:text=Humidity%20monitoring%20also%20helps%20you,points%20to%20avoid%20wasting%20energy)).
* **Cooling Redundancy:** If one CRAC fails, the remaining two can increase output to cover the load. If one needs servicing, it can be turned off and isolated while others keep cooling (concurrent maintainability). Additionally, the building’s comfort AC or backup cooling (like portable AC units) could be deployed in an extreme emergency for short periods.
* **Ventilation and Heat Rejection:** If DX units are used, the external condensing units will be placed outside the building (e.g., on ground or rooftop), properly secured and with adequate airflow. If a chilled water system were used (less likely for this size), a chiller and cooling tower would be specified instead. Fresh air makeup is minimal (data centers typically recirculate air and only bring fresh air to manage pressurization), but there will be a positive pressure maintained to keep dust out. Filters in the CRAC units will clean recirculated air (down to fine particle level).
* **Monitoring:** The HVAC system integrates with the environmental monitoring such that any unit failure or abnormal room temperature triggers an alarm. The CRAC units themselves often have SNMP or BACnet interfaces for monitoring.
* **Scalability:** The cooling design supports additional loads by either adding more in-row cooling units or increasing capacity (the room has space along the row to insert another cooling unit, or we could upsize existing units’ cooling modules if modular). Given the current total cooling capacity (40 kW with 2 units, 20 kW redundancy), and current load (~20 kW IT, ~10-15 kW cooling needed for that IT load), we have significant headroom. The system can likely handle doubling the IT load to 40 kW with the third unit kicking in. Beyond that, further CRAC units or an additional cooling row can be added.
* **Ancillary Cooling:** In areas like UPS/generator rooms, smaller split AC units will be installed to keep those equipment within safe temperature (batteries and UPS electronics also have thermal limits). These will be on emergency power as well.

**Network and Communications**

* **Internal Data Network:** Redundant 10 Gbps Ethernet backbone as mentioned. The switching infrastructure will use VLANs or network segmentation to separate management traffic, storage iSCSI (if used), and production data, to optimize performance and security. The latency within the LAN will be sub-millisecond, and throughput up to line rate on all ports to ensure no network bottlenecks for applications.
* **External Connectivity:** The data center will connect to the state government wide-area network or metropolitan fiber. For example, dual fiber links from two different providers (or two different routes of state fiber) could terminate in the data center to ensure connectivity redundancy. If Ondo State has an existing fiber backbone (perhaps connecting Akure and other cities), this data center becomes the central node. We might use a router or firewall pair to handle external routing and security. Bandwidth to the internet or state network might be (for instance) 1 Gbps initially, scalable to 10 Gbps as needed.
* **IP Telephony and Other Services:** If required, the data center can also house communication gear like IP-PBX or call center systems for the government. These would occupy their own rack but be supported by the same power/cooling. Not a primary focus of this document but noted for completeness.
* **Scalability:** Networking gear chosen can stack or scale-out. For instance, if we need more than the current number of server ports, we can add line cards or additional switches (and stack them). The fiber connectivity can be upgraded by changing optics (e.g., to 40G or 100G in future if needed). The addressing scheme and VLAN layout will allow adding new subnets for new services easily.

**Security and Monitoring Systems**

* **Access Control:** Biometric readers (fingerprint or iris scanners) at 2 main doors. Controller panel to manage these with capacity for expansion (more doors or more users). Initially perhaps 20 authorized personnel configured, with expansion to 100+ possible.
* **CCTV:** Approximately 8-12 cameras to cover all angles (for example: 4 inside at corners of server room for full view, 2 in staging and electrical rooms, 4 covering building exterior and entrances). NVR (Network Video Recorder) with 30 days recording at 1080p for all cameras, motion-based alerts. Cameras are POE powered via a dedicated switch or injector.
* **Fire Detection:** VESDA (Very Early Smoke Detection Apparatus) may be installed in addition to conventional smoke detectors for ultra-sensitive smoke sensing (this uses air sampling to detect minute particles early). This complements the FM200 system.
* **BMS/DCIM:** A Building Management System or Data Center Infrastructure Management software will tie together the monitoring of power, cooling, and environment. This can be a software like Schneider EcoStruxure or Vertiv Trellis, or even simpler SNMP-based monitoring aggregated on a console. It will provide a dashboard of temperatures, power load, uptime of systems, security status, etc., in one place for operators.
* **Disaster Recovery Measures:** Within this data center, provisions like regular data backups (to tapes or cloud or remote disk) will be planned, though the actual backup solution (software and hardware like tape library) is outside the core facility spec, it will be part of operations. The design however ensures connectivity and space for backup appliances (e.g., a rack-mounted tape library or backup server will reside here).
* **Compliance:** The overall design is aimed to comply with Uptime Institute Tier III requirements (allowing concurrent maintenance and no single point of failure in power/cooling distribution) and ISO 27001 information security standards for physical security. Tier III implies multiple power and cooling paths and an expected uptime of 99.982% ([What are Data Center Tiers? | Glossary | HPE](https://www.hpe.com/us/en/what-is/data-center-tiers.html#:~:text=of%20downtime%20annually%29)), which our redundant topology supports.

In summary, these technical specifications ensure that **every subsystem (IT, power, cooling, network, security)** is appropriately sized and configured for reliability and room to grow. The initial capacities meet current demand with a comfortable safety margin, and each component can be expanded or upgraded as technology evolves or loads increase. This data center is engineered not just for the day it opens, but to remain a **viable and efficient core of Ondo State’s IT infrastructure for years to come**.

**Risk Assessment and Mitigation Strategies**

Building and operating a data center involves various risks that need to be identified and managed. This section assesses the key risks associated with the project across construction, operation, and security, and outlines mitigation strategies for each risk category. By proactively addressing these risks, the project can avoid pitfalls that might cause delays, cost overruns, or service interruptions.

**1. Construction Phase Risks:**

* *Risk:* **Project Delays and Cost Overruns** – Factors like late delivery of equipment, contractor schedule slips, or unforeseen site issues (e.g., need for additional renovations) could delay the project timeline or increase costs.
  + *Mitigation:* Develop a **detailed project plan with buffer time** in each phase. Use experienced contractors with a track record in data center builds. Implement strong project management and oversight, with regular progress reviews. Include a **contingency budget** (~10-15% of project cost) to handle unexpected expenses without derailing the project. Identify long-lead items (like generators, specialized HVAC units) early and order them in advance. For schedule control, employ penalties/incentives in contracts to keep milestones on track.
* *Risk:* **Site or Construction Quality Issues** – E.g., subpar workmanship on raised floor or electrical wiring could lead to failures later (like floor collapse under load or electrical faults).
  + *Mitigation:* Enforce **strict quality control and inspections**. Hire consultants or in-house experts to inspect and sign off at key stages (floor installation, electrical testing, etc.). Use only certified materials (e.g., fire-rated cables, proper load-rated floor tiles). Conduct integrated testing of systems (like power fail-over tests, cooling performance tests) before project sign-off to catch issues. Adhering to Tier III guidelines and Nigerian building codes as a baseline for quality.
* *Risk:* **Safety Incidents During Construction** – Work involving heavy equipment, electrical works, etc., poses safety risks to workers which could halt work or cause legal issues.
  + *Mitigation:* Implement a **Health, Safety, and Environment (HSE) plan** with mandatory training for all workers. Ensure use of personal protective equipment (PPE) and safe practices (lock-out tag-out for electrical, etc.). Supervise high-risk activities (lifting heavy equipment into place, electrical hookups) with qualified personnel. Having insurance and first-aid/emergency protocols on-site. A safe construction process prevents accidents that could delay the project.

**2. Operational Risks (Power and Cooling):**

* *Risk:* **Power Outage / Power System Failure** – Despite redundant design, there is a risk (though low) that a severe grid outage combined with generator failure or fuel shortage could cut power. Also, UPS or battery failure could cause a momentary loss.
  + *Mitigation:* Maintain **adequate fuel supply contracts** and on-site fuel for generators (e.g., multiple days worth, and refuel contracts that prioritize the data center as critical infrastructure). Test generators under load **regularly (e.g., monthly)** to ensure reliability. Similarly, test UPS batteries quarterly and replace them per manufacturer guidance (usually every 3-5 years). Monitor battery health via the UPS management software. Additionally, integrate the solar-battery system to give extra buffer time. Establish procedures that if an extended grid outage is looming, non-critical loads are shed to conserve power. The redundant architecture itself (N+1 UPS, A/B feeds, etc.) is the primary mitigation ensuring no single failure brings down power ([What are Data Center Tiers? | Glossary | HPE](https://www.hpe.com/us/en/what-is/data-center-tiers.html#:~:text=of%20downtime%20annually%29)).
* *Risk:* **Cooling System Failure / Overheating** – If multiple AC units were to fail (e.g., due to a common cause like loss of chillers or control system error), servers could overheat.
  + *Mitigation:* The N+1 cooling design is a strong starting mitigation – one can fail and others maintain cooling. Additionally, set **automated high-temperature alarms** that trigger immediate response before overheating becomes critical. Keep an on-site stock of critical spare parts for CRAC units (like extra fan motors or coolant). Also, have portable spot coolers available that can be quickly deployed as a stopgap in case of a major cooling outage. Regular maintenance of HVAC (cleaning filters, checking refrigerant levels, etc.) will reduce risk of failure. If budget permits, consider hooking the cooling system to the generator as well so that even during power outage, cooling continues (which is planned in our design). In worst case scenarios, have an emergency procedure to safely shut down servers if temperature crosses a dangerous threshold (to prevent hardware damage) – and a plan to failover state services to a DR site if available.
* *Risk:* **Fire or Environmental Disaster** – Fire is a risk (electrical fire in a UPS, for example), as is flooding (from extreme rain if building drainage is poor) or other natural disasters.
  + *Mitigation:* Fire risk is mitigated by the **FM200 system and smoke detectors** for early suppression. All electrical wiring will have proper overload protection to minimize electrical fire chances. For flooding, ensure the data center is located in a non-flood prone area or elevated from ground level. The raised floor provides some protection by elevating equipment. Install water leakage detection (which we have) to catch any water ingress early (from AC condensation, roof leaks, etc.). The building’s roof and drainage should be inspected and reinforced if needed to handle heavy rains. In terms of other disasters: Ondo State is not prone to earthquakes, but if any minor seismic activity, the racks are bolted and equipment secured to handle vibrations. The physical structure’s reinforcement helps against high winds or storms.

**3. Operational Risks (IT and Security):**

* *Risk:* **Hardware Failure (Servers/Storage)** – Individual server or storage component failures could impact services if not handled.
  + *Mitigation:* Use of RAID on storage and clustering on servers mitigates impact – e.g., one server fails, its load can shift to others; one disk fails, RAID keeps data intact. Keep a **maintenance contract with HPE** for quick hardware replacement (same-day or next-business-day support). Also maintain some on-site spares (like a couple of spare disks, power supplies, and maybe one cold standby server that can be configured to replace a failed unit). Regularly update firmware and do proactive health checks to catch components that show signs of failing (predictive failure alerts). The SAN has dual controllers – ensure they’re on separate power feeds to avoid single points of failure.
* *Risk:* **Software or Configuration Errors** – Misconfiguration of network or power systems by staff could lead to outages (for example, wrong switch configuration could isolate systems).
  + *Mitigation:* Implement **change management processes** – any changes to critical systems should be reviewed and done in maintenance windows. Keep documentation of all configurations to speed up troubleshooting. Provide training to data center staff on the systems they manage (e.g., proper procedure to shut down a UPS or to change network VLANs). Also, consider staging configuration changes in a test environment if possible, or using the staging area to test new firmware updates, etc., before production. Utilizing DCIM software helps by giving a holistic view to avoid overload or dependency mistakes. Standardize and **document all procedures** (SOPs) for common tasks.
* *Risk:* **Physical Security Breach** – Unauthorized entry, theft of devices, or malicious physical tampering.
  + *Mitigation:* Multi-layer security as described: biometric access, 24x7 guards, CCTV monitoring – all significantly lower this risk ([What are Data Center Security Requirements? | VIAVI Solutions Inc.](https://www.viavisolutions.com/en-us/what-are-data-center-security-requirements#:~:text=enter%20or%20leave%20their%20facility,and%2For%20biometric%20readers%20in%20use)). Ensure the access control list is kept up-to-date (removing people who leave positions, etc.). Perform **periodic security drills** – e.g., attempt a social engineering entry to test guard alertness, or test that alarms trigger when doors are forced. The CCTV should be monitored and recordings reviewed occasionally for any suspicious activities. Sensitive data on servers should also be encrypted as a second-layer defense, so that even if a disk is stolen, data is protected (operational measure beyond facility scope but worth noting). Additionally, conduct background checks for personnel with access to the data center and limit access to only those who absolutely need it (principle of least privilege).
* *Risk:* **Cybersecurity Threats** – While physical, the data center houses systems that could be targeted by cyber attacks (viruses, hacking). A successful cyberattack could cause data loss or downtime.
  + *Mitigation:* Ensure **strong cybersecurity measures**: firewalls at the network perimeter, up-to-date anti-malware on servers, regular patches of all software/firmware. Segment the data center network from other networks to contain potential breaches. Conduct periodic vulnerability assessments and penetration tests on the systems. While this is somewhat outside the pure facility scope, it’s part of operational risk to the data center’s purpose. A disaster recovery plan (see below) also mitigates impact if a cyber incident cripples the systems – data backups and restore procedures would come into play.

**4. Disaster Recovery and Continuity Risks:**

* *Risk:* **Catastrophic Event (Site-wide failure)** – A worst-case scenario like a major fire that surpasses suppression, building collapse, or other site-wide disaster could knock out the data center entirely.
  + *Mitigation:* Establish a **Disaster Recovery (DR) plan** that includes off-site backups or a secondary data center location. For example, Ondo State could partner with a nearby state or use a cloud service to host backup copies of critical systems. The case study of Benue’s data center planning to have a DR site in Abuja ([UniCloud Africa and Benue Digital Infrastructure to build data center in Makurdi, Nigeria - DCD](https://www.datacenterdynamics.com/en/news/unicloud-africa-and-benue-digital-infrastructure-to-build-data-center-in-makurdi-nigeria/" \l ":~:text=Pan,recovery%20site%20in%20Abuja%2C%20Nigeria)) is instructive; similarly, Ondo could consider a smaller DR setup in a geographically separated location. Regularly test DR drills (restoring backups, activating fallback systems). Maintain insurance coverage for disasters to aid in recovery funding. By having data backed up and possibly some capacity elsewhere, even a total loss of the site won’t mean irrecoverable data loss or indefinite outage of services.
* *Risk:* **Lack of Operational Expertise** – After commissioning, if staff are not skilled in managing the sophisticated systems, mistakes or slow responses could pose risks.
  + *Mitigation:* Invest in **training for the data center operations team** well before go-live. During implementation, have staff shadow the vendors installing systems to learn. Possibly use the vendors’ operational services for the first few months (or get a consultant) while staff ramp up knowledge. Develop run-books for common incidents (power fail, network fail, etc.). Also implement a 24/7 on-call rotation so that expertise is always available, and key knowledge isn’t just with one person (avoid single-person dependency).

Each risk above is catalogued in a risk register (maintained separately) with owners assigned to watch and manage them. By applying these mitigation strategies, the project aims to reduce risks to an acceptable level. The guiding principle is redundancy and preparedness: assume that if something can fail, it will, and have a plan (and backup) for it. This approach aligns the data center with best practices in risk management for critical facilities, ensuring **continuous operation and security of Ondo State’s digital assets** even in adverse situations.

**Project Implementation Plan**

Implementing the data center project will be carried out in structured phases, each with clear timelines, deliverables, and responsible parties. This section presents a phased implementation plan, resource allocation, and key milestones to guide the project from inception to operational handover. A well-defined plan will help ensure that the project is completed **on time, within budget, and meets all requirements**.

**Phase 1: Initiation and Planning**

**Timeline:** Month 0 – Month 1 (Weeks 1-4)  
**Key Activities:**

* *Project Kick-off:* Form the project team, including a Project Manager (PM) from the state’s ICT agency or appointed consultant, technical leads for IT, electrical, cooling, and security, and representatives from key stakeholders (Governor’s office, relevant ministries). Conduct a kick-off meeting to confirm goals, scope, and approach.
* *Requirements Finalization:* Review this proposal’s specifications with stakeholders and finalize any details (e.g., confirm location/room, any additional needs like specific compliance requirements).
* *Feasibility and Site Survey:* Inspect the proposed site or building area to note any modifications needed. Survey the power intake, space dimensions, structural load capacity, etc. Identify if any enabling works (like raising a separate shelter or reinforcing floor) are needed.
* *Procurement Plan:* Develop a procurement strategy for contractors and equipment. Decide which components will be tendered (e.g., construction contractor for physical build, supplier for HPE equipment, etc.) and prepare RFPs or use existing vendor contracts.
* *Budget & Schedule Approval:* Refine the budget estimates into a detailed budget (as per section 9) and get official approval. Create a high-level master schedule for all phases.  
  **Deliverables:** Project charter/plan, stakeholder sign-off on scope and budget, RFP documents ready for release.

**Phase 2: Design and Procurement**

**Timeline:** Month 2 – Month 3 (Weeks 5-12)  
**Key Activities:**

* *Detailed Design Engineering:* Engage architects/engineers to create detailed floor layouts, electrical single-line diagrams, cooling ducting/piping schematics, network topology diagrams, and security layouts. Manufacturers (HPE, etc.) may provide reference designs. Ensure the design meets Tier III considerations (e.g., dual power path diagram).
* *Review and Compliance:* Conduct design review meetings. Verify compliance with any national ICT infrastructure guidelines or building codes (e.g., fire safety code compliance for FM200 room integrity, TIA-942 guidelines for data centers, etc.). Adjust design as needed.
* *Procurement Execution:* Issue purchase orders or sign contracts for major components:
  + Contract with a **Civil/General Contractor** for site prep (raised floor, HVAC install, wall works, cable trays installation, etc.).
  + Order **IT Equipment** from HPE (servers, storage, racks) – often through a certified reseller. Include support contracts.
  + Order **Power Equipment** (UPS, batteries, generator, solar panels, electrical panels) – possibly through an electrical contractor or directly from vendors like Schneider, APC, Cummins for generator, etc.
  + Order **Cooling Units** and associated works from an HVAC specialist.
  + Order **Security Systems** (biometric, CCTV) from a security systems integrator. Each procurement will have a specified lead time and delivery date to align with phase 3’s installation.
* *Resource Allocation:* Finalize the deployment team. Assign a site engineer or construction manager for overseeing on-site works. Assign the IT team members who will configure servers/networks. Also set up a steering committee for high-level oversight (perhaps including the State IT Director, etc.).
* *Milestone:* **Design Completion and Procurement Kick-off** – at end of this phase, designs should be locked and orders placed. **Deliverables:** Complete set of design documents (blueprints, diagrams), copies of all purchase orders/contracts, an updated timeline that factors in delivery lead times.

**Phase 3: Site Preparation and Construction**

**Timeline:** Month 4 – Month 6 (Weeks 13-24)  
**Key Activities:**

* *Civil Works:* Prepare the physical site as per design. This includes clearing out the room, reinforcing floor or applying epoxy if needed, then installing the raised floor support structure and panels ([[DOC] Supply and Installation of a Raised Floor at Ministry of Justice, Abuja ...](https://procurement-notices.undp.org/view_file.cfm?doc_id=71464#:~:text=,of%20300%2F350mm%20pedestal%20above)). Also implement wall cladding/insulation and any necessary drywall or partitioning (for staging area, etc.). Paint or finish surfaces as required (using anti-dust paint in server room). Ensure proper sealing of any wall openings for fire protection.
* *Electrical Infrastructure Installation:* The electrical contractor will install conduits, cable trays, and wiring from the main electrical room to the data center. Set up the main distribution boards (with ATS), run power cabling to the UPS room and to where racks will be. Install earthing system (drive grounding rods outside, lay copper tape/grid, and connect all major metal components to ground). By end of this sub-phase, the room should have power distribution cabling ready.
* *HVAC Installation:* Install the CRAC units in position (likely along the perimeter or within rack rows if in-row cooling). Run refrigerant lines to external condensers and mount those outside. Set up ventilation ducts if needed. Do initial tests of the cooling units (without load) to verify functionality.
* *Fire Suppression and Security Installation:* Fit the FM200 cylinders and piping network in the server room and beneath floor if needed. Install smoke and heat detectors integrated to the fire panel. Perform a **Room Integrity Test** (Door Fan test) to ensure the room can hold the FM200 gas for sufficient time (required for system effectiveness). Simultaneously, the security contractor will mount CCTV cameras, biometric readers, door locks, and pull the cabling for these back to their controllers/NVR in the security room or rack.
* *Solar Panel Setup:* If on-site conditions allow, mount solar panels on roof or ground mounts, install inverters and battery units in the electrical room. Wire them into the electrical system per design (likely through a solar charge controller into the battery/UPS system).
* Throughout Phase 3, the PM will coordinate **weekly site meetings** to track progress against schedule, manage any dependencies (e.g., electrical first-fix needed before closing ceiling, etc.), and resolve issues.
* As components arrive (e.g., UPS units, generators), they are installed:
  + *UPS & Battery:* Place UPS in position (could be large floor-standing or rack-mounted in a dedicated rack), connect input/output cables, install battery banks in racks or cabinets and connect to UPS. Don’t power on fully until commissioning.
  + *Generator:* Construct the generator pad, place generator, connect fuel lines and exhaust, connect to ATS and test in manual mode initially.
* *Milestone:* **Construction Complete** – by end of this phase, the facility’s infrastructure (floor, cooling, power, security) is installed. **Deliverables:** Progress reports, inspection certificates (for electrical wiring, etc.), updated floor plan with any on-site changes, and a “pre-commissioning report” that site is ready for equipment installation.

**Phase 4: Equipment Installation and Configuration**

**Timeline:** Month 7 (Weeks 25-28)  
**Key Activities:**

* *Receiving and Inventory:* All HPE racks, servers, storage, and network equipment delivered to site (likely around beginning of Month 7, scheduled based on lead times). Verify against orders (right models, quantities). Store them in staging area for unpacking.
* *Rack and Stack:* Position and secure the HPE racks in the raised floor area according to layout. Bolt them together and to the floor as needed. Next, install the components:
  + Mount PDUs in each rack and connect them to the under-floor power whips from the UPS distribution.
  + Mount servers in racks (using rail kits). Mount SAN storage enclosure in a rack. Mount network switches and any appliances (firewalls, KVM console, etc.) in the network rack.
  + Install cable managers within racks and do initial dressing of cables.
* *Connectivity:* Run and connect network cables from servers to switches, fiber cables from servers and storage to SAN switches, and uplink cables from core switches to external network. Also connect management ports (iLO/management NICs of servers to a management switch). Label all connections. Connect all power supplies of equipment to the rack PDUs (ensuring dual-corded devices go to separate A/B PDUs).
* *Power-On and Testing:* Energize the racks one by one. The UPS should already be on and providing clean power (likely still fed by mains at this point). Bring up servers and storage – check that each powers on (at BIOS level) and is stable. Configure IP addresses for management where needed to see devices on the network. This is a **hardware test/burn-in** period: let servers run idle or under basic test loads to catch any hardware DOA issues. The staging area can be used to test one or two servers prior to full installation (if that was feasible with time).
* *System Configuration:* IT team and vendor engineers will configure:
  + Servers: Install hypervisor or operating systems as per the plan (maybe VMware ESXi if virtualization, or Windows/Linux if physical deployments). This can be deferred to next phase if focusing on infra, but at least basic OS to test networking is done here.
  + Storage: Configure RAID, LUNs on the SAN. Map these to servers (ensuring the zoning on SAN switches is correctly done).
  + Network: Configure VLANs, IP routing, firewall rules on the network devices. Set up the management network for out-of-band access (i.e., ensure ability to reach iLO/iDRAC of servers, switch management IPs, etc.).
  + Security Systems: Integrate biometric system (add users) and ensure CCTV cameras are recording properly.
* *Integration Test:* At this phase, conduct an initial integration test: simulate a power failure (cut mains feed) to ensure UPS takes load, generator auto-starts and picks up load via ATS ([Solar plus storage is a win-win for Nigeria's booming data centre market and residents | Digitalisation World](https://www.msp-channel.com/blog/58114/solar-plus-storage-is-a-win-win-for-nigerias-booming-data-centre-market-and-residents#:~:text=International%20Energy%20Agency%2C%20IEA%2C%20the,of%20data%20centre%20build%20out)). Simulate a cooling unit failure (turn one off) to see if temperature remains controlled with remaining units. Test door access controls and alarms. Essentially, verify that redundancies and failovers work as designed.
* *Milestone:* **Initial Systems Operational** – all equipment is installed and basic configuration done, with environment supporting it (power/cooling) proven stable. **Deliverables:** Installation report (list of installed assets with serial numbers), network diagram with actual IPs, configurations for network and SAN, test results from power/cooling failover tests, and sign-off to proceed to formal commissioning.

**Phase 5: Testing, Commissioning and Training**

**Timeline:** Month 8 (Weeks 29-32)  
**Key Activities:**

* *Final Commissioning Tests:* Conduct thorough testing of all systems:
  + **Functional Testing:** Verify each UPS can carry load on battery for expected duration; test FM200 discharge in a controlled way (if a full discharge test is too costly, do a simulation test per vendor recommendations, but at least test alarms and triggers). Test the BMS/DCIM alarms by creating conditions (like high temp by adjusting AC setpoint) to see if alerts fire. Test access control with authorized vs. unauthorized scenarios.
  + **Load Testing:** Possibly use load banks or dummy loads to simulate full load on power and cooling. For example, run servers at high CPU to see heat output and ensure cooling holds temperature. Or connect a resistive load to test generator at full capacity for a few hours.
  + **Failover and Recovery:** Create a detailed **UAT (User Acceptance Test)** script: e.g., "While running critical servers, cut Power Feed A – verify Feed B carries all, then restore A; simulate CRAC failure; simulate network switch failure by shutting it down – verify network traffic reroutes, etc." The data center should exhibit no downtime for simulated single-component failures (as per design intent).
  + Document results of each test.
* *Issue Resolution:* Any problems found in testing are addressed now. E.g., if a UPS battery did not hold charge as long as expected, investigate and fix (maybe load was higher than thought, or a bad battery string). If hotspots are identified (a particular rack warmer), add perforated tiles or adjust airflow. This phase may involve fine-tuning configuration (like adjusting cooling unit setpoints or reconfiguring network redundancy protocols).
* *Training:* Provide comprehensive **training to the operations staff** on all systems. Vendors or contractors should conduct training sessions on:
  + Electrical system: how to safely transfer load to generator, how to perform maintenance bypass on UPS, reading the power monitoring equipment.
  + Cooling system: understanding the CRAC controls, filter replacement schedule, etc.
  + Fire system: how to reset after an alarm, safety precautions with FM200.
  + IT equipment: management tools for servers (e.g., HPE OneView), storage management (creating new volumes, monitoring SAN health), network management (using the switch CLI or interface, monitoring links).
  + Security and monitoring tools: how to manage user access in biometric system, reviewing CCTV footage, responding to environmental alerts. Also, an **Operations Manual** will be prepared – combining vendor manuals and site-specific procedures for routine tasks and emergency procedures.
* *Data Migration & Launch Prep:* (If applicable) Migrate existing data and applications from old infrastructure to the new servers/SAN. This might happen now or post-commissioning. For instance, restore backups into the new environment or cut-over services one by one to the new data center. This planning would depend on the existing setup and is itself a sub-project to avoid service disruption.
* *Acceptance and Certification:* Once everything is tested and staff are comfortable, formally hand over the data center. Possibly invite an independent auditor or Uptime Institute representative if Tier certification is sought (though Tier certification might not be explicitly budgeted, the design is Tier III aligned and could be certified). At minimum, internal audit by state ICT officials to confirm requirements are met.
* *Milestone:* **Project Go-Live / Handover** – The data center is declared ready for production use, and operations team takes over. **Deliverables:** Commissioning test report signed by stakeholders, Training completion certificates or records, Final “as-built” documentation (final network configs, rack layout, etc.), Operations Manual, Handover document (signifying transfer from project team to operations).

**Phase 6: Operation and Maintenance (Post-Implementation)**

*(While outside the immediate scope of construction, it's important to note this phase for completeness.)*  
**Timeline:** Ongoing from Month 9 onward.  
The data center enters regular operation with continuous monitoring. A maintenance schedule (daily/weekly checks, monthly generator tests, quarterly UPS service, annual comprehensive maintenance, etc.) commences as per the Operational Plan (Section 7). The project team dissolves, but key members may remain as part of a governance board to oversee performance and any future upgrades.

**Resource Allocation & Responsibilities:** Throughout the above phases:

* The **Project Manager** coordinates all activities, updates the project plan Gantt chart, and communicates status to stakeholders.
* **Technical Leads** (Civil, Electrical, IT) are responsible for the detailed execution in their domains, including supervising contractors and verifying technical work.
* **Vendors/Contractors** (e.g., the company supplying HPE equipment, the installer for cooling) each have their scope. Their contracts will specify responsibilities and deliverables (e.g., vendor must install and test servers, or contractor must provide handover documentation).
* **Government Stakeholders** (Ministry of Science and Tech, etc.) will receive periodic reports and will be involved in key approvals (design approval, final acceptance).
* **Budget Controller/Procurement Officer** ensures spending is tracked and within approved limits, and that payments to vendors are tied to milestones achieved.

**Milestones and Key Deliverables Recap:** To monitor progress, the following major milestones are identified:

1. **Project Charter Approved** (Phase 1) – authorizes project start.
2. **Design Sign-off** (Phase 2 end) – all designs approved, procurement initiated.
3. **Site Prep Complete** (Phase 3 end) – room ready for equipment (floor, power, cooling in place).
4. **Equipment Installed** (Phase 4 end) – all hardware in place and basic tested.
5. **Commissioning Completed** (Phase 5 end) – data center fully tested and operational, ready for go-live.
6. **Project Closure** – Formal handover to operations, all documentation delivered.

Meeting these milestones on schedule will be indicators of project health. We anticipate the overall project duration from kick-off to go-live to be around **8 months**, assuming no major delays. This timeline may be adjusted slightly in execution, but the phased approach ensures each aspect is handled with focus and thoroughness.

The implementation plan is thus designed to methodically transition from blueprint to a live data center, with clear checkpoints to maintain control over scope, time, and quality. With diligent execution of this plan, Ondo State will have a functional and reliable data center by the end of the project timeline.

**Operational Plan**

Once the data center is built and commissioned, a robust operational plan is essential to ensure it continues to run efficiently, securely, and with minimal downtime. This section outlines the strategy for **maintenance, monitoring, staffing, and ongoing operations** of the Ondo State data center. It also covers disaster recovery preparedness and security management practices that will be in place during the operational phase.

**Maintenance and Monitoring Framework**

**24/7 Monitoring:** The data center will be monitored around the clock. Key infrastructure (power, cooling, network, servers) will report to a central monitoring system (or DCIM). Alerts for any parameter out of threshold (temperature, UPS on battery, etc.) will be configured to notify on-duty personnel via multiple channels (audible alarm, SMS, email). This ensures that any incident gets immediate attention, even after hours.

**Daily/Weekly Routines:** Data center operators will have a daily checklist. This includes:

* Visually inspecting the server room for any warning lights on equipment, unusual sounds or smells, water leak indicator status, etc.
* Checking environmental readings (temperature and humidity at various points) to ensure within range.
* Ensuring the security systems (access control, CCTV) are functioning (e.g., no camera obstructed, recordings happening).
* Verifying backup jobs completed successfully (for IT systems data backup).

On a weekly basis:

* Test secondary systems: e.g., do a brief generator start test (without load transfer) every week or two to keep it in good shape.
* Manually inspect battery status on UPS (most modern UPS have self-diagnostics, but a manual check of logs).
* Review log files from servers and network devices for any signs of developing issues (like disk error warnings that precede failure).
* Housekeeping: clean the environment (dust mopping of raised floor surface using anti-static cloth, for instance) to maintain a dust-free environment.

**Preventive Maintenance Schedule:** Key components will have preventive maintenance (PM) at manufacturer-recommended intervals:

* **HVAC:** Filter replacements and coil cleaning every 3 months; full servicing (checking refrigerant pressure, calibrating sensors) every 6-12 months. Ensure humidity control components are serviced (clean humidifier, etc.).
* **UPS and Batteries:** Quarterly inspection and battery health check (some batteries may need load testing). Yearly preventive maintenance by the UPS vendor to check capacitors, fans, etc. Battery replacement cycle set (e.g., every 3-4 years for VRLA batteries).
* **Generator:** Monthly loaded test (simulated outage to force generator to carry load for 10-15 minutes) – observe transfer is smooth. Professional servicing of generator every 250 running hours or annually, including oil/filter changes, coolant check, battery check for starter, and fuel system check to avoid wet-stacking. Also polish fuel yearly to prevent contamination.
* **Fire System:** Bi-annual inspection of FM200 cylinders (check pressure levels), and annual integrated test of detection (fire drill scenario to ensure alarms trigger properly). The cylinders typically require weighing or pressure check to ensure no leakage.
* **Security Systems:** Clean camera lenses quarterly, test door access every month (ensure no malfunction). Update CCTV recording backups and archive policies as needed.
* **Servers/Storage/Network:** Maintain support contracts for firmware updates and hardware support. Schedule firmware/OS updates in batches during maintenance windows (e.g., quarterly patch cycle) to keep systems secure and performant. Each quarter, perhaps take down one server at a time (in a cluster) to apply patches, then rotate – so no total downtime.
* **Software/Backups:** Daily incremental and weekly full backups will be scheduled for critical data, with tapes or offsite replication. Test restore from backups quarterly to ensure data can be recovered (a backup is only as good as a verified restore).

All maintenance activities will be logged in a maintenance log, and any incident and resolution will go into an incident log. This builds an operational history that helps in audits and continuous improvement.

**Staffing Considerations and Operational Efficiency**

**Staffing Model:** Initially, the data center operations might require a small dedicated team. For example:

* **Data Center Manager:** Oversees the facility, vendor management, capacity planning, and ensures policies are followed.
* **System/Network Administrators:** 2-3 personnel who handle the day-to-day monitoring, handle alerts, perform maintenance on servers, storage, and network. They also manage backups and user requests (like provisioning resources for new services).
* **Facilities Technician/Engineer:** 1-2 personnel focusing on the physical infrastructure – power and cooling systems. They coordinate generator tests, work with electrical contractors for maintenance, and respond to facility alarms. (This role might be combined with the above if staff is cross-trained, or might be outsourced to a facility management company on call).
* **Security Personnel:** Physical security guards (perhaps 2 per shift for 24x7 coverage) to monitor the premises and control physical access. These might be existing government security (or contracted security firm) stationed at the data center building.
* **Support Contracts:** It's assumed critical equipment (UPS, HVAC, etc.) have vendor support. Thus, in case of issues beyond minor fixes, those vendors can be called in. The internal staff ensures they have contacts and SLAs in place.

**Shifts:** Ideally, data center monitoring is 24/7. This could be achieved by having an **on-call rotation** for IT staff with remote monitoring capabilities. The facility itself, being physically guarded 24/7, means someone is always at the site, but IT staff might not be present at 3 AM unless needed. If budgets allow, having at least one IT staff on night shift is ideal, but if not, an automated alert will wake on-call personnel to respond remotely or travel to site if needed.

**Standard Operating Procedures (SOPs):** To ensure efficiency and consistency, SOP documents will be used for common tasks – e.g., "Procedure to safely shut down a rack," "Procedure to start generator manually," "Process to grant a new user access to the data center," etc. These reduce errors and training time.

**Operational Efficiency:** We will aim to streamline operations by leveraging tools:

* Use the DCIM or monitoring software to automate responses where possible (e.g., if temperature rises, it can automatically increase cooling unit fan speed or send command to standby AC).
* Implement IT automation – for instance, use virtualization such that workloads can move if a physical host needs maintenance, thereby avoiding after-hours work or service interruption.
* Capacity management: Track resource utilization and plan upgrades ahead of time. E.g., when storage reaches 70% utilization, start procurement for additional disks. This foresight prevents reactive crises.

**Sustainability Practices:** To reduce ongoing costs, implement energy-saving measures like: optimize cooling setpoint (each degree higher in setpoint can save significant energy while staying safe for equipment), make use of “free cooling” when weather permits (if applicable). The solar integration is a big operational cost saver – we will monitor how much solar contributes and adjust to maximize its use (like scheduling battery discharge during peak tariff times if on commercial power billing etc.).

**Vendor Management:** Keep all warranty and support contracts active. E.g., HPE servers typically come with 3-year warranty – ensure they are renewed or extended for the life of use. Same with UPS and HVAC (often an annual support contract is available). The Data Center Manager will coordinate vendor visits for preventive maintenance per schedule (like yearly UPS service by vendor).

**Documentation and Knowledge Management:** Maintain up-to-date documentation of the environment: network diagrams, rack layouts, passwords (secured), access lists, and inventory of assets. This helps if staff turnover occurs – new staff can get up to speed quickly. Also maintain a “run book” for handling various disaster scenarios (as part of DR plan).

**Disaster Recovery and Business Continuity**

Even with a highly reliable data center, a disaster recovery plan is critical. The data center will have:

* **Regular Backups:** as mentioned, all critical systems data will be backed up to an offsite location. This could be cloud storage or tapes stored in a secure offsite facility. Backups are scheduled nightly for incremental and weekly full backups. Key datasets include government databases, application data, and server images.
* **Offsite Redundancy:** Ondo State may consider a secondary site (perhaps a smaller scale DR data center or utilizing a cloud service) to replicate data in near real-time for quick recovery. For example, the SAN storage could asynchronously replicate critical volumes to a storage system in a different city (if bandwidth allows), or at least, databases could stream transaction logs to an offsite server. If budget doesn’t allow a full DR site initially, at least ensure the backups are comprehensive so systems can be rebuilt on alternate hardware if needed.
* **DR Drills:** Conduct disaster simulation exercises annually. For instance, simulate that the primary data center is unavailable (without actually shutting it down) and walk through steps of recovering key services from backups or switching to DR systems. Identify gaps and improve the plan. These drills ensure that, in an actual disaster, the team isn’t doing everything for the first time.
* **Business Continuity Procedures:** Work with each government department to define how they will continue critical functions if the data center is down. This might include manual fallback processes or using interim solutions. The goal is to minimize disruption to state services even if IT is hit by a disaster. Knowing these procedures can prioritize which systems to restore first after a disruption (e.g., maybe the treasury payment system is most critical, etc.).

**Security Management**

Physical and logical security will be continuously managed:

* **Access Control Reviews:** Periodically (e.g., monthly) review who has access to the data center. Remove access for anyone who no longer needs it (job change, etc.). Use a sign-in log for any visitors or one-time entries (with approval process).
* **CCTV Surveillance:** Security personnel or the ops team should review CCTV recordings in a spot-check fashion or when alerts (like a door forced open) occur. Place cameras such that all sensitive areas are covered, and ensure adequate lighting for clear footage. Signs of tailgating or unusual activity should be investigated.
* **Cybersecurity:** Keep all systems patched and enforce strong authentication for remote access. Utilize network segmentation and firewalls to isolate the data center from less secure networks. Intrusion detection systems (IDS/IPS) could be employed at the network perimeter. The ops team should stay updated on emerging threats and ensure the data center’s systems (especially any internet-facing services) are hardened.
* **Security Audits:** The data center should undergo an **annual security audit** – covering both physical and IT security. This can be done by an internal audit department or external experts. They will check compliance with policies, test the effectiveness of controls (e.g., try to gain unauthorized access), and give recommendations.
* **Incident Response:** Develop an incident response plan for security breaches (physical or cyber). E.g., if an unauthorized entry happens, what steps? If a server is suspected hacked, how to isolate and investigate? Training the team on incident response will help contain and resolve issues faster.

**Compliance and Reporting:** The operational practices will align with any relevant regulations, such as Nigeria Data Protection Regulation (NDPR) for data privacy, or any mandates from NITDA for government IT infrastructure. Reports on uptime, incidents, capacity, and maintenance will be generated monthly for the government’s IT oversight body to ensure transparency and track performance against SLAs.

**Continuous Improvement**

Operations will adopt a continuous improvement mindset. After a few months of running, the team will analyze trends: e.g., is power usage higher than expected? Could we improve cooling layout? Are there certain times where staffing is short? Lessons learned will feed into optimizations. Also, as technology evolves (for instance, more efficient cooling systems or new monitoring tools), the state can plan upgrades to keep the data center state-of-the-art.

Regular stakeholder meetings (perhaps quarterly) will review how the data center is supporting government needs. New requirements (like additional capacity for a new application) can be discussed and scheduled. In essence, operations is not static; it adapts to both the environment and the government’s needs.

By implementing this operational plan, Ondo State will ensure that the data center remains **highly available, well-maintained, and secure** throughout its life. Users of government digital services will experience reliable service, and the behind-the-scenes maintenance will largely be invisible to them, which is the mark of a well-run data center. The combination of preventative maintenance, skilled staff, strong security, and disaster preparedness will keep the state's IT backbone robust against potential issues, thereby safeguarding the continuity of governance and public services.

**Case Studies and Comparisons**

To contextualize Ondo State’s data center initiative, it is useful to examine similar projects and existing facilities, both within Nigeria and in comparable government settings. By learning from these examples, we can validate our approach and ensure we adopt proven best practices. This section presents case studies of data center projects (particularly in government/public sector) and compares key aspects like design, implementation, and outcomes. It also contrasts the proposed data center with existing government data management approaches to highlight improvements.

**Case Study 1: Edo State Data Center (Nigeria)** – *Digital Transformation Hub*  
Edo State recently launched the first state-owned data center in Benin City as part of its digital revolution agenda ([First state-owned data center launches in Benin City, Nigeria - DCD](https://www.datacenterdynamics.com/en/news/first-state-owned-data-center-launches-in-benin-city-nigeria/#:~:text=Governor%20Godwin%20Obaseki%2C%20who%20unveiled,with%20secure%20data%20storage%20options)) ([Gov. Obaseki unveils first data centre, digital policy in Edo - Nigerian NewsDirect](https://nigeriannewsdirect.com/gov-obaseki-unveils-first-data-centre-digital-policy-in-edo/#:~:text=%E2%80%9CEdo%E2%80%99s%20new%20data%20center%20acts,for%20government%20and%20business%20data)). Although detailed specs were not publicly disclosed, the strategic goal closely mirrors Ondo’s objectives: providing a secure hub for government and business data, and enabling e-governance and digital services. Governor Godwin Obaseki emphasized that this infrastructure is *“vital for digital operations, empowering local businesses…and the entire region with secure data storage options”* ([Gov. Obaseki unveils first data centre, digital policy in Edo - Nigerian NewsDirect](https://nigeriannewsdirect.com/gov-obaseki-unveils-first-data-centre-digital-policy-in-edo/#:~:text=%E2%80%9CEdo%E2%80%99s%20new%20data%20center%20acts,for%20government%20and%20business%20data)). Key takeaways from Edo’s example:

* **Strategic Alignment:** Edo’s center was tied to a comprehensive digital policy and youth empowerment programs ([Gov. Obaseki unveils first data centre, digital policy in Edo - Nigerian NewsDirect](https://nigeriannewsdirect.com/gov-obaseki-unveils-first-data-centre-digital-policy-in-edo/#:~:text=%E2%80%9CEdo%20has%20long%20embraced%20this,old%20tradition%20of%20international%20collaboration)). Similarly, Ondo’s center should be integrated into broader IT development plans (like e-government services expansion and tech-driven education or job creation initiatives).
* **Infrastructure:** While Edo’s specifics are under wraps, it presumably has redundancy and modern equipment given its role. It demonstrates that Nigerian states are now pursuing Tier II/III-level facilities to support governance.
* **Outcome & Impact:** Though new, Edo’s data center is expected to improve efficiency (state government has been paperless since 2023, indicating robust IT usage ([First state-owned data center launches in Benin City, Nigeria - DCD](https://www.datacenterdynamics.com/en/news/first-state-owned-data-center-launches-in-benin-city-nigeria/#:~:text=According%20to%20Obaseki%2C%20the%20state,since%202023%20under%20Obaseki%27s%20leadership))). Ondo can expect similar improvements – faster data access for decision-making, better online services, etc. The Edo case provides political validation; if Edo can do it, Ondo can confidently invest, armed with awareness that such projects are feasible in our environment.

**Case Study 2: Benue State Data Center Project** – *Public-Private Partnership and DR Integration*  
Benue State (through the Benue Digital Infrastructure Company, BDIC) entered an MoU in 2024 to build a data center in Makurdi, partnering with a private cloud firm (UniCloud Africa) ([UniCloud Africa and Benue Digital Infrastructure to build data center in Makurdi, Nigeria - DCD](https://www.datacenterdynamics.com/en/news/unicloud-africa-and-benue-digital-infrastructure-to-build-data-center-in-makurdi-nigeria/" \l ":~:text=Cloud%20computing%20firm%20UniCloud%20Africa,data%20center%20in%20Benue%2C%20Nigeria)). Notably, the project includes a complementary disaster recovery site in Abuja provided by Africa Data Centres ([UniCloud Africa and Benue Digital Infrastructure to build data center in Makurdi, Nigeria - DCD](https://www.datacenterdynamics.com/en/news/unicloud-africa-and-benue-digital-infrastructure-to-build-data-center-in-makurdi-nigeria/" \l ":~:text=infrastructure%20for%20the%20site)). Key points:

* **Budget & Scale:** The project cost is estimated at **₦10.8 billion (≈ $6.6 million)** ([UniCloud Africa and Benue Digital Infrastructure to build data center in Makurdi, Nigeria - DCD](https://www.datacenterdynamics.com/en/news/unicloud-africa-and-benue-digital-infrastructure-to-build-data-center-in-makurdi-nigeria/" \l ":~:text=The%20project%20is%20estimated%20to,be%20completed%20in%20six%20months)), to be completed in six months. This budget suggests a significant build, likely including high-end infrastructure (possibly Tier III standard) and the involvement of a major data center operator for DR.
* **Public-Private Collaboration:** By involving cloud and data center companies, Benue leverages external expertise and possibly spreads cost/risk. Ondo’s proposal as outlined is primarily government-driven, but we can consider partnerships (for example, using a telecom’s fiber or an IT firm’s managed services in some areas) if it adds value.
* **Vision:** The Benue deputy governor stated it’s about transforming Benue into a digital hub and *“embracing the potential of the digital age”* ([UniCloud Africa and Benue Digital Infrastructure to build data center in Makurdi, Nigeria - DCD](https://www.datacenterdynamics.com/en/news/unicloud-africa-and-benue-digital-infrastructure-to-build-data-center-in-makurdi-nigeria/" \l ":~:text=Sam%20Ode%2C%20the%20deputy%20governor,%E2%80%9D)). This echoes our executive summary for Ondo. The presence of a DR site is a notable best practice – Benue ensures resilience by having backup in another city. Ondo should similarly plan for offsite backups or DR (if not a full second site, at least cloud backups or a reciprocity arrangement with another state’s data center in future).
* **Timeline Realism:** Six months for completion is very aggressive (likely leveraging prefabricated modules or fast-track methods). Our plan projects ~8 months; however, knowing Benue’s timeline, we might refine our schedule with modular approaches if needed to accelerate.

**Case Study 3: Galaxy Backbone (Federal Government) Tier IV Data Center** – *Benchmark for Reliability*  
Galaxy Backbone (GBB), a federal agency, achieved Uptime Institute Tier IV certification for a new data center in 2024 ([Nigeria’s first dual-certified Tier IV data centre](https://africanreview.com/ict/nigeria-s-first-dual-certified-tier-iv-data-centre#:~:text=,network%20that%20spans%20the%20country)) – the first in Nigeria at that high level. It used Huawei’s prefabricated modular data center solution ([Nigeria’s first dual-certified Tier IV data centre](https://africanreview.com/ict/nigeria-s-first-dual-certified-tier-iv-data-centre#:~:text=,of%20Nigeria%E2%80%99s%20digital%20transformation)), consisting of 17 containerized modules. Key comparisons:

* **Tier IV vs Tier III:** Tier IV offers 99.995% uptime, whereas Tier III offers 99.982%. Tier IV requires full fault tolerance (2N redundancy for all systems). GBB’s facility is cutting-edge with prefabrication enabling rapid deployment (17 containers hoisted and assembled in one month) ([Nigeria’s first dual-certified Tier IV data centre](https://africanreview.com/ict/nigeria-s-first-dual-certified-tier-iv-data-centre#:~:text=multiple%20systems%20such%20as%20the,like%20quality%20and%20experience)). Ondo’s is aiming for Tier III reliability, which is more cost-effective and still excellent (1.6 hours downtime allowed annually vs Tier IV’s ~26 minutes ([What are Data Center Tiers? | Glossary | HPE](https://www.hpe.com/us/en/what-is/data-center-tiers.html#:~:text=of%20downtime%20annually%29))). Tier III is typically the choice for state-level data centers given budget and complexity constraints.
* **Prefabrication Trend:** GBB’s approach indicates a trend to use modular data centers to save time and ensure quality (factory built). Ondo’s plan is more traditional brick-and-mortar, but we could incorporate some modular components (like prefabricated power skids or modular UPS systems). If rapid deployment or future expansions are needed, adopting modular designs (like adding a container for expansion) is an option learned from GBB’s case.
* **Outcomes for GBB:** This data center is to support nationwide government services and Nigeria’s ICT backbone ([Nigeria’s first dual-certified Tier IV data centre](https://africanreview.com/ict/nigeria-s-first-dual-certified-tier-iv-data-centre#:~:text=,adopting%20the%20company%E2%80%99s%20FusionDC1000B%20prefabricated)). For Ondo, it’s on a smaller scale but the aim is similar – support all state MDAs and possibly connect into the National Information Infrastructure. We should ensure compatibility (like if GBB offers cloud services, Ondo’s center could integrate or serve as an edge site – a synergy opportunity).

**Comparison with Existing State Infrastructure (Legacy Systems):**  
Currently, many state governments in Nigeria without a modern data center rely on decentralized servers in various ministries or rented hosting in private data centers. These approaches often suffer from:

* **Low Reliability:** A server in an office might be down due to local power issues or lack proper backup, causing service outages. In contrast, a centralized data center with redundant power and cooling dramatically improves uptime. For instance, if previously a ministry’s server went offline whenever there’s a city power outage, after migrating to the data center, that service will stay online thanks to UPS and generator backup.
* **Poor Security:** Disparate systems are harder to secure (physically and digitally). The data center allows **consolidated security** – one highly secure facility is easier to defend than many scattered ones. Biometric access, CCTV, and 24/7 guard in the data center versus maybe a padlock in an office server room is a night-and-day improvement.
* **Inefficiencies:** Each ministry might have had its own small server setup, possibly underutilized and maintained by non-specialist staff. Consolidation in the data center yields efficiencies of scale (better utilization through virtualization, easier maintenance by dedicated staff, and lower overall power/cooling overhead because of consolidation). It also reduces duplication – for example, instead of 10 different backup generators at 10 sites (often non-functional), one robust backup system serves all.
* **Data Integration:** In the old approach, data sharing between ministries can be slow or done via manual transfer. With a central data center, systems can be interconnected on a high-speed network. This can enable integrated e-government applications, cross-ministry databases, and a unified portal for citizens. Essentially, the data center becomes the *information hub* of the state.

**Comparative Outcome Expectation:**  
States or countries that have invested in government data centers have seen improvements in service delivery. For example, consider:

* **Estonia’s X-Road system** (though not a physical data center example, it’s an e-government success reliant on secure data exchange) – having a solid central infrastructure allowed them to offer almost all government services online. While Ondo is far from that level initially, building this data center is the foundational step towards such possibilities in the future.
* **Kenya’s Government Data Center** – Kenya built a National Data Center in 2019 to support its Huduma (one-stop services) and government cloud. It saw consolidation of hundreds of servers, reduction in hosting costs, and improved uptime for critical applications (reports indicate significant cost savings by avoiding paying external data center fees).
* **Comparing Private Sector**: Within Nigeria, private data centers like MainOne (MDXi) and Rack Centre in Lagos operate at high uptime (Tier III certified). They set a benchmark in operational excellence that our government data center should strive to emulate internally. However, using private colocation was an alternative – the reason Ondo (like Edo and others) chooses to build their own is data sovereignty and control. Plus, location matters: having it within the state ensures low-latency access for offices across Ondo and control over physical access.

**Lessons Learned from Case Studies:**

1. **Ensure Political and Executive Buy-in:** The successes (Edo, Benue) had top-level support which smoothed funding and prioritization. Ondo has that momentum by initiating this proposal – continued support will be needed, e.g., to secure budget and inter-agency cooperation.
2. **Don’t Skimp on Training and Processes:** Technology alone isn’t enough. Even Tier IV infrastructure can fail if poorly managed. For instance, a famous case in another domain: a Tier III data center in Australia went offline due to human error during maintenance. Thus, as seen with Galaxy Backbone (which presumably has a strong operations team given federal resources), the human factor is crucial.
3. **Plan for Growth and DR from Day 1:** Benue’s inclusion of a DR site from the start is prudent. Ondo should at least plan the interface for DR – e.g., leave network provision for connecting to a future second site or cloud. Having expansion space is also key; many organizations outgrow their first data center faster than anticipated because once available, digital initiatives multiply.
4. **Leverage Renewable Energy:** Our design included solar. This aligns with global and national trends (the President commissioned a solar-powered data complex for Immigration in 2024 ([President Tinubu Commissions Solar Powered Data Technology Complex – Voice of Nigeria](https://von.gov.ng/president-tinubu-to-commission-solar-powered-data-technology-complex/#:~:text=The%20Data%20Complex%20comprises%20the,5KW%20Solar%20Power%20Plant))). It reduces long-term costs and sometimes funding is easier for green initiatives. So, if there are grants or partnerships available for solar in government buildings (like World Bank’s solar programs ([Nigeria to Provide Solar Subsidy For Underserved Areas with World ...](https://empowerafrica.com/nigeria-to-provide-solar-subsidy-for-underserved-areas-with-world-bank-backing/#:~:text=Nigeria%20to%20Provide%20Solar%20Subsidy,loan%20from%20the%20World%20Bank))), Ondo could tap those.

In comparing our proposed facility to these case studies, Ondo State’s data center stands well-aligned with modern standards:

* It may not be as large or Tier IV as the federal one, but it follows Tier III best practices which is appropriate for the scale and criticality.
* It is more comprehensive than Edo’s publicly known info, by detailing every component and including solar (which Edo’s info didn’t mention). This could make Ondo’s one of the more advanced state-level centers, possibly a model others could follow.
* With a budget likely in the range of a few billion Naira (see next section), it’s a significant but justifiable investment when weighed against the importance of government continuity and digital growth. The comparative examples support that this is money well spent; Edo and Benue are making similar investments.

By examining these examples, Ondo State can proceed with confidence, avoiding pitfalls encountered elsewhere and replicating successes. The end result should be a data center that puts Ondo at the forefront of e-governance readiness in Nigeria’s public sector, comparable to and even learning from its peers and predecessors.

**Budget Breakdown (in Nigerian Naira - NGN)**

In this section, we present a detailed budget for the data center project with itemized cost estimates for each component. All costs are given in Nigerian Naira (NGN). We also discuss contingency allowances and cost control measures. This budget is based on current market prices and quotes for equipment and services, tailored for a Tier III-like data center of the specified scope. It is meant to ensure transparency and provide a clear financial roadmap for project approval.

**Summary of Estimated Costs:** The overall cost of the project is estimated at **₦3,250,000,000** (approximately ₦3.25 billion). The table below breaks down this total into major categories and line items:

| **Category** | **Item** | **Quantity/Details** | **Unit Cost (NGN)** | **Line Total (NGN)** |
| --- | --- | --- | --- | --- |
| **1. Civil & Site Works** | Raised Floor System (600mm tiles, pedestals) | ~100 sqm area (incl. supports) | ₦50,000 per sqm | ₦5,000,000 |
|  | Wall Insulation & Cladding (interior) | ~300 sqm coverage (fire-rated panels) | ₦20,000 per sqm | ₦6,000,000 |
|  | Partitioning & Finishing (Staging room, painting, minor works) | Lump Sum | – | ₦5,000,000 |
|  | Access Flooring (Anti-static vinyl finish) | Included in raised floor cost | – | – |
|  | **Subtotal Civil/Site** |  |  | **₦16,000,000** |
| **2. Power Infrastructure** | High-capacity UPS Systems (80 kVA x 2 + batteries) | 2 UPS modules + battery racks (15 min backup) | ₦70,000,000 each UPS | ₦140,000,000 |
|  | Diesel Generator (250 kVA) + ATS | 1 unit + Automatic Switch (incl. installation) | ₦60,000,000 | ₦60,000,000 |
|  | Solar PV Plant (50 kW) + Batteries (100 kWh) | Panels, inverters, batteries, install | ₦1,000,000 per kW | ₦50,000,000 |
|  | Electrical Switchgear, Panels, Cabling | Main DB, PDUs, wiring, earthing materials | Lump Sum | ₦40,000,000 |
|  | Power Distribution Units (Rack-mounted) | 10 smart PDUs (₦500k each) | ₦500,000 | ₦5,000,000 |
|  | Installation Labor (Electrical) | – | – | ₦15,000,000 |
|  | **Subtotal Power** |  |  | **₦310,000,000** |
| **3. Cooling Infrastructure** | Precision Cooling CRAC Units (20 kW) | 3 units (N+1 config) | ₦25,000,000 each | ₦75,000,000 |
|  | Cooling Distribution (Containment, ducts, piping) | Aisle containment setup, refrigerant lines | Lump Sum | ₦10,000,000 |
|  | External Condenser Units & Ventilation | 3 condensers + fans | included in CRAC cost | – |
|  | HVAC Installation & Commissioning | – | – | ₦8,000,000 |
|  | **Subtotal Cooling** |  |  | **₦93,000,000** |
| **4. Fire & Security Systems** | FM200 Fire Suppression System | Cylinders, piping, detectors for ~250 m³ room | ₦30,000,000 | ₦30,000,000 |
|  | Very Early Smoke Detection (VESDA) (optional) | 1 system | ₦5,000,000 | ₦5,000,000 |
|  | Access Control System (Biometric) | 2 readers + controller + locks | ₦3,000,000 per door | ₦6,000,000 |
|  | CCTV Surveillance System | 10 Cameras + NVR + storage | ₦300,000 per camera (avg) | ₦3,000,000 |
|  | Security System Installation & Training | – | – | ₦2,000,000 |
|  | **Subtotal Fire/Security** |  |  | **₦46,000,000** |
| **5. IT Equipment** | HPE Server Hardware (ProLiant DL380 Gen10) | 8 servers (as spec'd) | ₦8,000,000 each | ₦64,000,000 |
|  | HPE SAN Storage (MSA 2060 + 20 disks) | 1 array + 20 drives | ₦50,000,000 | ₦50,000,000 |
|  | HPE Rack Enclosures (42U) | 5 racks (server/storage) + 1 network rack | ₦1,500,000 each | ₦9,000,000 |
|  | Networking Equipment (Core Switches, SAN switches, Firewall) | 2 core + 2 SAN + 1 firewall | Lump Sum (Switch ~₦15M ea, Firewall ₦10M) | ₦55,000,000 |
|  | KVM, Console, Misc IT accessories | Consoles, patch panels, cables etc. | Lump Sum | ₦5,000,000 |
|  | Software (Virtualization, OS licenses, etc.) | OS for servers, virtualization platform | Lump Sum | ₦20,000,000 |
|  | **Subtotal IT Equipment** |  |  | **₦203,000,000** |
| **6. Structured Cabling** | Data Cabling (Cat6A, Fiber) + Trays | For entire facility (incl. trays, ladder racks) | Lump Sum (materials) | ₦15,000,000 |
|  | Cabling Installation Labor | – | – | ₦5,000,000 |
|  | **Subtotal Cabling** |  |  | **₦20,000,000** |
| **7. Professional Services** | Design & Consulting Fees | Data center design consulting, Tier compliance review | – | ₦15,000,000 |
|  | Project Management | PM for 8 months (could be internal or contracted) | – | ₦10,000,000 |
|  | Training & Knowledge Transfer | Vendor training sessions, materials | – | ₦5,000,000 |
|  | **Subtotal Prof. Services** |  |  | **₦30,000,000** |
| **8. Contingency** | Contingency (approximately 10%) | Buffer for unforeseen costs | – | **₦70,000,000** |
| **Total Project Cost** |  |  |  | **₦3,250,000,000** |

*All costs are estimates and would need to be confirmed via competitive bids.*

**Notes and Justifications for Costs:**

* **Civil & Site Works:** The raised floor cost covers the entire data hall area including pedestals and antistatic finish. Wall cladding uses insulated panels; these are one-time investments to reduce cooling costs. The civil works are a small portion of total cost (~₦16m) but crucial for environment preparation.
* **Power Infrastructure:** This is a major cost driver. UPS systems are expensive but necessary – two 80 kVA units with battery cabinets cost about ₦140m. The generator (250 kVA) includes the engine, alternator, soundproof canopy, and ATS panel – ₦60m is a realistic figure for industrial generators. The solar plant at ₦50m covers panels, inverters, and battery storage; it's a significant upfront cost but should reduce electricity/generator use for years. Switchgear and cabling is also significant – including heavy-duty cables from transformer/genset to data center, distribution boards, and professional installation. Overall power accounts for roughly 10% of total; this aligns with typical data center builds where electrical and mechanical (cooling) often each equal or exceed IT equipment costs.
* **Cooling:** The CRAC units and containment represent about ₦93m (~3% of total). Precision AC units are high-cost due to their robust design for continuous operation. We estimated ₦25m each which includes their accompanying condenser units. This might be slightly conservative, but better to over-budget cooling than under. Proper installation by HVAC specialists (₦8m) ensures warranty and performance.
* **Fire & Security:** At ₦46m, this covers all safety systems. FM200 systems typically cost in the tens of millions for a room this size (cylinder costs, release panel, etc.). We allocate ₦30m based on similar installations. Biometric and CCTV prices have dropped in recent years, but enterprise-grade systems (with redundancy, secure readers) are still a few million Naira – hence ₦6m for 2 doors is realistic. These systems are relatively low cost compared to the risk they mitigate (priceless data protection).
* **IT Equipment:** This is about ₦203m (~6.25% of total), which might seem low compared to infrastructure. In many data centers, the facility costs exceed initial IT purchase because the facility is built to last multiple generations of IT equipment. We sized servers and storage to current needs; as those needs grow, additional IT gear will be purchased (but then, the facility can handle it without big new costs aside from the hardware itself). 8 HPE servers at ₦8m each (approx $10k each) is reasonable for well-configured units. The SAN at ₦50m covers the dual-controller and high-quality disks. Networking lumps core and SAN switches and a firewall at ₦55m – enterprise 10G switches can be ~₦10-15m each, SAN FC switches similar, plus a firewall cluster ~₦10m. We also added some funds for software (e.g., VMware licenses or Windows Server, etc.). If the state leverages open-source or existing licenses, this could be less.
* **Cabling:** ₦20m covers the entire structured cabling plant (copper, fiber, patch cords, and cable management). Given the number of connections (each server has multiple cables, plus connecting offices possibly), this ensures high-quality cabling (Cat6A for 10G, OM4 fiber for SAN) plus certified installation and testing.
* **Professional Services:** ~₦30m is allocated for design and management. Engaging experts (maybe international or experienced local consultants) to design and perhaps to certify Tier III compliance might cost a few million but is worthwhile. Project management costs could be internal (salaries) or external – we budget to account for either scenario. Training by vendors is often included with purchase, but we allocated extra to perhaps send key staff for data center training or certifications.
* **Contingency:** At 10% (~₦70m), this covers unknowns: currency fluctuations (important as some equipment is imported and exchange rates can vary), additional site requirements (maybe need to upgrade the substation transformer or implement more cooling if load is higher, etc.), or inflation (given project might span near a year). It’s a buffer to ensure the project can be completed without asking for more funds later. If unused, it returns to the treasury or can be used for enhancements (like maybe adding more IT capacity initially).

**Cost Control Measures:**

* **Competitive Bidding:** For major procurement (construction, electrical, IT equipment), we will use competitive tender processes. This ensures we get market prices or better. For example, inviting multiple reputable vendors for HPE gear and networking should yield some discounts or value-add (like free training or extended warranties).
* **Vendor Selection and Contracts:** We will favor vendors who offer comprehensive warranties and after-sales support included in the price. For instance, including 3-year support with servers (common with HPE) or service packages for UPS/Generator for 1-2 years free. This reduces operating cost burden initially.
* **Project Phasing Finance:** If needed, the project could be structured with milestone-based payments (tied to deliverables as outlined) to ensure cash flow is managed and vendors are paid upon fulfilling tasks. This avoids large upfront outlays without results.
* **Local Resources:** Utilize state government resources where possible. For example, if the site is an existing government building, we save on buying land or building anew. If the state has electricians or engineers on payroll who can assist under supervision, it might reduce some labor costs. However, we must balance that with ensuring quality (critical tasks likely remain with specialized contractors).
* **Scope Management:** Stick to the scope defined. Avoid gold-plating (like over-provisioning beyond foreseeable needs) which inflates cost. Our plan has some headroom but not extravagance. Any requested changes should go through a change control evaluating cost impact against benefits.
* **Contingency Use Oversight:** The contingency fund is not to be treated as extra money for optional features; it should only be tapped upon genuine need and with approval from project governance. Unused contingency stays unused.
* **Tax/Duty Consideration:** Government projects might be eligible for duty waivers on imported equipment. We will explore if items like FM200 gas, servers, etc., can be imported tax-free under government exemption, which could save significant costs (potentially 5-15% on those items).

**Operational Cost Note:** This capital budget does not cover ongoing operational costs (staff salaries, electricity, diesel fuel, maintenance contracts). Those will need annual budgeting by the state. However, the investment in solar (₦50m) will help trim the electricity/diesel bills. For context, if the data center draws, say, 40 kW average and grid power costs ~₦60/kWh (example), running 24/7 for a year costs ~₦21 million in electricity. Diesel for generator during outages and maintenance might be another chunk. Solar 50 kW at good sun might shave off perhaps ₦5-7m worth of energy per year, eventually paying back its cost over maybe 7-10 years, after which it’s net savings.

Comparatively, Benue’s project at ₦10.8b is larger, possibly including building new facility and more capacity (and perhaps that DR site cost). Edo’s cost wasn’t public, but given Edo’s emphasis, it might be in the low billions as well. Our ₦3.25b is reasonable for a state-level facility of moderate size. It's a significant investment, but in line with modernization goals (for perspective, it’s around $4-5 million USD, which for a government data center with redundancy is not excessive).

We will ensure the spending is tracked meticulously. A dedicated financial officer in the project will monitor expenditures vs budget line items to avoid overruns. Regular financial reports will be produced to the project steering committee and the state’s finance ministry for transparency.

In conclusion, this budget provides for all critical components of the data center and includes a healthy contingency. The Ondo State Government can be confident that this financial plan is comprehensive and rooted in realistic cost assessments, providing a solid basis for funding approval and subsequent implementation.

**Preferred Vendors and Justifications**

Selecting the right vendors and technology partners is critical for the success and longevity of the data center. We recommend using **industry-standard vendors** known for quality, reliability, local support presence, and alignment with our technical requirements. Below we list the preferred vendors for major components, along with justifications for their selection:

**1. Server and Storage Vendor – Hewlett Packard Enterprise (HPE):**  
*Justification:* HPE is a globally recognized leader in server and storage solutions. The choice of HPE ProLiant servers and HPE SAN (MSA/Nimble) is motivated by:

* **Reliability and Performance:** HPE servers are engineered for continuous operation and have features like advanced cooling, power management, and fail-safe firmware updates. They consistently rank high in performance benchmarks.
* **Support and Warranty:** HPE has an established support center in Nigeria and certified partners. We can get next-business-day on-site support or even 4-hour response contracts for critical systems, which ensures any hardware issues are resolved swiftly. This is crucial for government uptime needs.
* **Ecosystem and Integration:** Using one vendor for servers, storage, and even racks (which we are, with HPE racks) means the ecosystem is integrated and tested together. HPE’s management software can oversee servers and storage in one pane (e.g., HPE OneView). This simplifies operations for our staff.
* **Experience in Government Projects:** HPE has a track record of supplying to government data centers in Nigeria and Africa, meaning they understand public sector requirements. For example, Galaxy Backbone’s earlier data centers included HPE equipment, implying trust at the federal level.
* While alternatives exist (Dell EMC, IBM, Cisco UCS), HPE’s combination of competitive pricing and strong presence in the region makes it a preferred choice. Additionally, since some of our team may already be familiar with HPE systems from prior work, it reduces the learning curve.

**2. Networking Vendor – Cisco (or HPE/Aruba for Switching, Fortinet for Firewall):**  
Networking is the backbone for connectivity. We propose:

* **Cisco Systems** for core network switches and possibly SAN (though SAN is often Brocade which is now part of Broadcom, but Cisco also offers MDS SAN switches). *Justification:* Cisco is known for its robust hardware and IOS software that powers a majority of enterprise networks globally. They have strong local partner support in Nigeria. Cisco switches and routers are reliable under heavy loads and come with advanced features (security, QoS, segmentation) that our data center needs. Also, staff training and certification for Cisco (CCNA/CCNP) are common, so finding skilled personnel is easier.
* **HPE Aruba** is an alternative for Ethernet switching. Since we are using HPE for servers, Aruba (HPE’s networking division) could be seamlessly integrated and might come at a better bundle price. Aruba switches are noted for ease of use and have good performance; plus HPE could offer a single support contract for servers + networking.
* **Fortinet (or Cisco)** for Firewall/Security: Fortinet’s FortiGate firewalls are highly respected for throughput and unified threat management and are widely used in Nigeria’s enterprises. They often provide good value for performance. Cisco’s firewall (Secure Firewall, formerly ASA with FirePOWER) is also an option, especially if we want to stay with one brand; however, Fortinet or Palo Alto might have the edge in modern threat protection.
* **Brocade (Broadcom) or Cisco for SAN**: If Fibre Channel SAN, Brocade is a market leader and their switches (which might be branded by HPE as “HPE SNxxx” series) would be used. If iSCSI, then this is moot as we’d use Ethernet.

**3. Power Infrastructure Vendors – Schneider Electric (APC) and Cummins:**

* **UPS:** Schneider Electric (through its APC brand) is a top provider for data center UPS and power distribution. *Justification:* APC Symmetra or Galaxy series UPS systems are known for high efficiency and modular design. Schneider has a Nigerian presence and can provide service support and spare parts locally. Alternatives: Vertiv (formerly Emerson Network Power) also offers Liebert UPS which are very good; we would consider them too since Vertiv Liebert is strong in cooling and power. Between these, the choice may come down to best service offer and cost. Both are reputable.
* **Generator:** Cummins or Caterpillar are renowned for generators. Cummins Power Nigeria has a strong support network for diesel gensets. *Justification:* These brands offer reliable engines designed for prime power (frequent use), and parts are readily available. They also often integrate well with data center ATS systems. An alternative is FG Wilson (Perkins engine) which also has local distributors. We favor Cummins for its track record in critical installations.
* **Power Distribution and Switchgear:** Schneider Electric can also supply the electrical panels (their breakers, meters etc. are high quality). Schneider’s EcoStruxure product line can integrate power monitoring which might be beneficial. Other good vendors: ABB or Eaton also provide switchgear and are viable choices.
* **Solar System:** For solar panels and inverters, preferred vendors could be **Huawei or SMA** for inverters (Huawei is very active in Nigeria’s solar sector, and SMA is a top German brand for reliability). Solar panels from Tier 1 manufacturers like Jinko or Trina ensure good performance. We would likely work with a local solar integrator who uses these top components. *Justification:* A quality inverter with battery management ensures our solar investment pays off in uptime and lifespan; cheap inverters might fail or not properly manage battery, so sticking to proven brands is key.

**4. Cooling System Vendor – Vertiv (Liebert) or Schneider (Uniflair):**  
Cooling units in data centers are often either Vertiv Liebert or Schneider (APC) units, or Stulz (German brand).

* **Vertiv Liebert** is a preferred choice as they are industry leaders in data center cooling. *Justification:* Liebert units are known for precision and reliability; many Nigerian banks and telcos use Liebert AC units in their data centers due to strong local support (Vertiv Nigeria). They have models optimized for high ambient temperatures as well.
* **Schneider Electric’s Uniflair** line is another top-tier option. Schneider can package this with their power offer. The quality is comparable; selection might depend on proposal details and existing reference sites.
* **Alternative:** Stulz or Data Aire also produce excellent CRAC units but have less local presence. We lean towards Vertiv or Schneider because of easier maintenance services in-country.

**5. Fire Suppression – Kidde or Siemens (for FM200 systems):**  
FM200 is a chemical (made by Chemours). The suppression system assembly (cylinders, nozzles, control panel) often comes from specialists like Kidde, Minimax, or Siemens.

* **Kidde Fire Systems** is a popular vendor for FM200 installations globally. *Justification:* They offer highly reliable systems and have certified installers in Nigeria who follow NFPA standards.
* **Siemens Cerberus or Siemens Sinorix** (their clean agent system) is another option; Siemens has a presence in fire safety in Nigeria.
* The key is to use a system that is UL/FM approved. We also need to ensure the vendor provides a proper design concentration per room size. We prefer a vendor who can integrate detection (smoke detectors, control panel) with suppression release as a package.
* **Alternative Agents:** Inergen or Novec1230 are newer agents (more environmentally friendly). We mention this because if procurement finds FM200 costly or scarce (FM200 is still widely used though, as seen by numerous installations ([FM200 Fire Suppression Systems for Server-Room, Data-Center in Ikeja - Other Services, Technologies Automation Systems | Jiji.ng](https://jiji.ng/ikeja/other-services/fm200-fire-suppression-systems-for-server-room-data-center-zIzeWMmtkm8XdahjTj9mVZRO.html#:~:text=FM,You%20can%20call%20us))), Novec 1230 (by 3M) could be used, which some vendors provide. However, FM200 is tried-and-true and easier to refill in Nigeria.

**6. Structured Cabling – Corning (Fiber) and Panduit or Legrand (Cabling hardware):**  
For cables and trays:

* **Corning** is recommended for fiber optic cables and connectivity (they are world leader, ensures our fiber links are high quality and low loss).
* **Panduit or Legrand** for cabling components (like patch panels, cable trays, trunking). *Justification:* These brands provide robust physical infrastructure with proper grounding and can handle high densities. They often partner with warranty programs (e.g., 25-year warranty on structured cabling if installed by certified partner).
* **Local Suppliers:** There are local distributors for these brands in Nigeria. Using standard products ensures any certified installer can maintain/expand the system.
* Using good cabling is important for performance; as noted in an earlier reference, structured cabling leads to better throughput and easier maintenance ([A Guide to Data Center Structured Cabling - Dataspan](https://dataspan.com/blog/a-guide-to-data-center-structured-cabling/#:~:text=1)). Thus, we stick to reputable brands to avoid issues like cable degradation or poor connector quality.

**7. Software and Management – VMware, Microsoft, or Open Source Solutions:**

* For server virtualization and management, **VMware** is the industry standard (vSphere, vCenter for managing our server cluster and VMs). If cost permits, we prefer VMware for its robustness and staff familiarity in enterprise.
* Alternatively, **Microsoft Hyper-V** (especially if we already license Windows Datacenter edition, which includes Hyper-V) or **Open Source KVM/Proxmox** could be considered to save costs. However, vendor support from VMware is top-notch if something goes wrong in virtualization layer.
* For data center infrastructure management (DCIM), **Schneider’s EcoStruxure IT** or **Vertiv Geist IM** can be used. If we go with Schneider for power/cooling, their DCIM might integrate better. We might also look at **Sunbird DCIM** or open-source monitoring like Zabbix for budget reasons. A DCIM solution from a recognized vendor ensures we can monitor power, cooling, and floor space effectively.
* Backup software, if needed, could be **Veeam** (widely used and reliable for backing up VMs and physical servers). It’s vendor-neutral and works well in environments like ours.

**8. Construction and Integration Partner – Local Systems Integrator (e.g., Resourcery, Dimension Data, etc.):**  
While not a product vendor, choosing the right integrator is crucial. We should select a company that has built data centers in Nigeria. For instance:

* **Dimension Data** (now NTT Ltd.), **Resourcery**, **Inlaks**, or **Computer Warehouse Group (CWG)** are examples of ICT integrators who have experience in data center projects. If we do a turnkey contract, one of these could manage it and bring in sub-vendors for specialized parts.
* For electrical and cooling works, firms like **ARCO, Mikano (for genset)** or **Skipper** might come in.
* We prefer an integrator who can act as a single point of responsibility for implementation, ideally holding partnerships with HPE, Cisco, Schneider, etc. This ensures they can source genuine equipment and have vendor support.

**Vendor Selection Criteria:**  
Regardless of specific names, the selection will be based on:

* **Quality and Reliability:** Proven track record of products in similar environments (e.g., equipment that can handle Nigeria’s power conditions and climate).
* **Local Support Availability:** As emphasized, vendors with local offices or strong partner networks (for quick spare parts and service) get preference. Downtime waiting for an overseas part is not acceptable for critical systems.
* **Total Cost of Ownership:** We will evaluate not just upfront cost but operating cost, efficiency (e.g., an efficient UPS that wastes less power), and support costs. For instance, a cheaper unknown UPS could cost more in batteries or failures long-term than a slightly pricier Schneider UPS with higher efficiency.
* **Compliance and Standards:** Vendors must adhere to international standards (ISO, IEEE, NFPA for fire, etc.). This assures interoperability and safety. For example, any electrical gear should have IEC certification, any cable Cat6A should be certified to TIA standards, etc.
* **References and Warranty:** Vendors should provide references from comparable projects (preferably within Nigeria or similar markets) and offer robust warranty terms. For instance, HPE might offer 3-year warranty on servers, APC could offer 1-year full warranty on UPS with service contracts beyond that.

**Benefit of Preferred Vendors:** Using these standard vendors essentially means Ondo State’s data center will be built on the **same class of technology as leading global data centers**, ensuring longevity. Their solutions incorporate the latest technology – e.g., HPE’s new servers for efficiency, Schneider’s UPS for high efficiency and battery management, Cisco’s networks for security features, etc. This also means if the data center needs to scale or if parts need replacing in 5-10 years, these vendors will likely still be around with compatible solutions.

**Avoiding Vendor Lock-in:** We have chosen a diversified approach in some areas (e.g., mixing HPE and Cisco and Schneider) which prevents dependency on a single supplier for everything. All these systems use open standards, so we can integrate or substitute if needed in the future (e.g., our structured cabling or racks will fit any standard servers, not just HPE, so if later we add Dell servers, they fit fine).

The preferred vendors above collectively bring **trust and peace of mind** to the project. By leveraging their strengths, Ondo State reduces risk and aligns the project with proven outcomes. As we proceed, formal procurement will involve these vendors (directly or via their certified partners) to get competitive quotes and ensure the best value is achieved.

**Conclusion and Next Steps**

In conclusion, the proposed data center for Ondo State Government is a strategically vital project that will establish a secure, reliable, and scalable foundation for the state’s digital services and data sovereignty. This document has detailed the plan from concept to execution: defining the scope with all necessary components (from raised floors to biometric security), justifying each element’s inclusion, outlining technical specifications, analyzing risks with mitigation plans, providing an implementation roadmap, and presenting a comprehensive budget and vendor strategy.

**Key Findings and Feasibility:**

* The data center is **feasible within an estimated budget of ₦3.25 billion**, which is justified by the robust infrastructure it will put in place. This investment will yield significant returns in terms of improved government service uptime, data protection, and long-term cost savings from consolidated operations.
* Each component of the design works in tandem to achieve a Tier III level facility with an expected **uptime of 99.98%** ([What are Data Center Tiers? | Glossary | HPE](https://www.hpe.com/us/en/what-is/data-center-tiers.html#:~:text=of%20downtime%20annually%29)), meaning the government and citizens can rely on continuous service availability.
* The inclusion of renewable energy (solar) and modern cooling and power systems shows forward-thinking, aligning with sustainability goals and mitigating Nigeria’s power supply challenges ([Solar plus storage is a win-win for Nigeria's booming data centre market and residents | Digitalisation World](https://www.msp-channel.com/blog/58114/solar-plus-storage-is-a-win-win-for-nigerias-booming-data-centre-market-and-residents#:~:text=A%20global%20shortage%20of%20power,new%20wave%20of%20data%20centre)) ([Solar plus storage is a win-win for Nigeria's booming data centre market and residents | Digitalisation World](https://www.msp-channel.com/blog/58114/solar-plus-storage-is-a-win-win-for-nigerias-booming-data-centre-market-and-residents#:~:text=Until%20recently%2C%20businesses%20in%20Nigeria,term%20power%20purchase)).
* By comparing to other states and projects (Edo, Benue, GBB Tier IV), we have validated that our approach is both appropriate and competitive. Ondo State’s data center will not be an outlier but rather on par with, if not more advanced than, peer initiatives, which underscores its strategic importance in keeping the state technologically competitive.

**Long-term Impact:**  
In the long term, this data center will be the **digital heart of Ondo State**. It will:

* Enable the rollout of e-government platforms (online portals for education, healthcare, agriculture, public records, etc.) with confidence that the backend is solid.
* Encourage economic development by potentially offering hosting services or at least by reassuring investors that Ondo has stable IT infrastructure (companies value regions where government services are online and reliable).
* Protect sensitive citizen and government data with world-class security measures, reducing risks of breaches or data loss that could disrupt governance or erode public trust.
* Provide a training ground for state IT personnel, who will gain expertise managing modern infrastructure, thereby building local capacity and job skills.

**Recommended Next Actions for Approval and Implementation:**

1. **Formal Approval:** Present this proposal to the State Executive Council or relevant approving authority. Highlight the executive summary points – especially the strategic value (as was quoted for Edo’s case: a secure hub vital for operations ([Gov. Obaseki unveils first data centre, digital policy in Edo - Nigerian NewsDirect](https://nigeriannewsdirect.com/gov-obaseki-unveils-first-data-centre-digital-policy-in-edo/#:~:text=%E2%80%9CEdo%E2%80%99s%20new%20data%20center%20acts,for%20government%20and%20business%20data))). Obtaining an official go-ahead and budget allocation is the first priority.
2. **Project Governance Setup:** Upon approval, set up the project steering committee and assign the Project Manager. This governance should include key stakeholders (e.g., Commissioner of Science and Tech, representative from Finance, IT department head, etc.) to oversee execution.
3. **Procurement Phase Initiation:** Immediately begin drafting RFPs/tender documents for the major work packages: (a) Facility construction and MEP (Mechanical, Electrical, Plumbing – includes power and cooling) and (b) IT equipment supply. Given government procurement timelines, it's crucial to start this early. Ensure tender requirements reflect the specifications and preferred vendor standards described (this ensures we attract qualified bidders).
4. **Site Finalization:** Secure the site/building where the data center will be housed. If any preparatory work is needed on site (like emptying an existing building space, or minor renovations prior to contractor handover), plan for that in parallel.
5. **Engage Consultants (if needed):** Optionally, engage a specialized data center consultant to refine detailed engineering requirements (especially if Tier certification is desired) and to assist with procurement technical evaluations. This will add assurance that the facility will be built to spec.
6. **Capacity Building:** Begin identifying current staff or new hires who will operate the data center. Start training programs early (even basics like data center operations best practices) so that by the time of commissioning, the team is prepared. We might also send staff to visit another state’s data center (maybe Edo or an established private DC in Lagos) for exposure.
7. **Plan for Interim Solutions:** Recognize that building this will take several months. If there are pressing needs for improved IT before then, plan interim measures (for example, if a particular database is failing often due to poor environment, maybe relocate it to a temporary hosted server until our DC is ready). This ensures continuity until the data center comes online.
8. **Public Communication:** It may be wise to communicate the launch of this project to the public in a positive light – positioning Ondo as moving towards e-government. This creates goodwill and prepares users for new digital services. It also signals to businesses that Ondo is serious about digital infrastructure. The Edo example saw positive press coverage linking it to youth empowerment and knowledge economy ([Gov. Obaseki unveils first data centre, digital policy in Edo - Nigerian NewsDirect](https://nigeriannewsdirect.com/gov-obaseki-unveils-first-data-centre-digital-policy-in-edo/#:~:text=%E2%80%9CEdo%20has%20long%20embraced%20this,old%20tradition%20of%20international%20collaboration)), and Ondo can craft a similar narrative.

**Closing Statement:**  
The establishment of the Ondo State Data Center is more than a technical project; it is an enabling platform for the state’s future. It embodies the state’s commitment to modernize operations, improve service delivery, and safeguard information in the digital era. As noted earlier, *“embracing the potential of the digital age”* is essential for unlocking a brighter future ([UniCloud Africa and Benue Digital Infrastructure to build data center in Makurdi, Nigeria - DCD](https://www.datacenterdynamics.com/en/news/unicloud-africa-and-benue-digital-infrastructure-to-build-data-center-in-makurdi-nigeria/" \l ":~:text=Sam%20Ode%2C%20the%20deputy%20governor,%E2%80%9D)), and this data center is a tangible manifestation of that embrace.

With a clear plan in place, strong justification for every naira spent, and lessons learned from comparable projects, Ondo State is well-positioned to execute this project successfully. Upon approval, we will move swiftly into action, adhering to the outlined plan and adjusting as needed to realities on the ground, while keeping the ultimate objectives in focus.

**Next Steps Summary:** Approve budget and plan → constitute project team → initiate procurement and site prep → implement in phases with rigorous project management → test and commission → transition to steady-state operations.

By following through on these steps, we anticipate the data center to be operational by *(for example)* Q2 of next year (assuming an 8-9 month project timeline from approval to completion). At that point, Ondo State will join the forefront of digital governance infrastructure in Nigeria, with a facility that citizens can be proud of and one that will serve the government’s needs for many years to come.