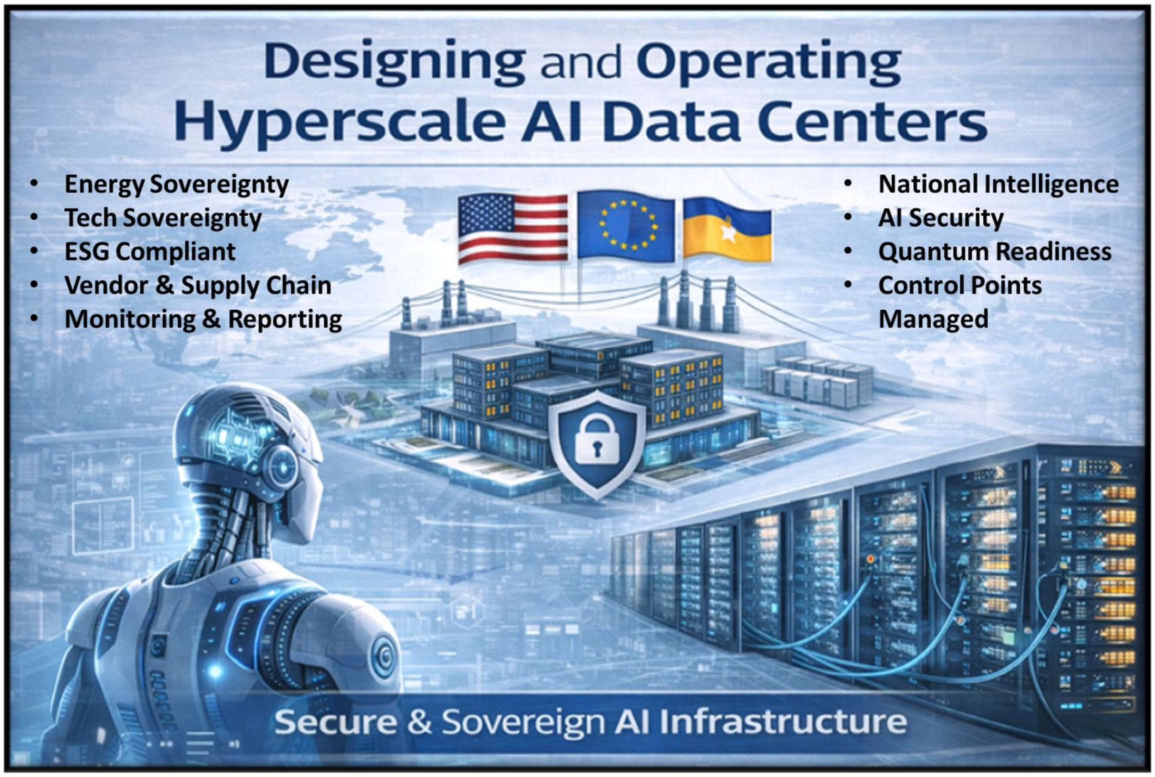
Designing and Operating Hyperscale AI Data Centers

Institutional-Grade Architecture, Energy, Sovereign Governance & Resilience Framework



Prepared By: Data Center Assistance Group, LLC

Executive Infrastructure, Energy & Resilience Advisory

Thomas Bronack, President

bronackt@dcag.com | bronack@gmail.om | www.dcag.com | (917) 673-6992

Contents

Executive Summary 5
1. Hyperscale AI Reference Architecture 5
2. Energy Systems & Interconnection Risk Modeling 6
3. Thermal Engineering & Water Governance 7
4. Cybersecurity & Regulatory Control Crosswalk 9
5. Sovereign AI Infrastructure Model 10
6. Institutional Risk Matrix 11
7. KPI & Governance Model 12
8. Implementation Roadmap (5-Phase Model) 13
9. Managing & Reporting on Data Center Operations 14
10. Strategic Conclusion 15
Microgrid Architecture for Sovereign Hyperscale AI Campuses 16
    Strategic Rationale 16
    1. Microgrid Architecture Overview 16
        Core Components 17
    2. Microgrid Operating Modes 17
    3. Black Start & First Recovery Techniques 17
        Sequence Model 18
ESG Sustainability Framework for Hyperscale AI 19
    ESG in hyperscale AI is not marketing. It is: 19
    4. Energy Sustainability Model 19
ESG-Aligned First Recovery Protocol 20
Microgrid Revenue Opportunity Layer 20
Integrated Risk Reduction Impact 20
Investor Narrative Framing 21
Financial Information Tables 22
    Assumptions 22
    CapEx (Capital Expenditures) Expenditures 22
    Operating Model 23

Revenue Model ... 23
IRR & NPV (Internal Rate of Return &Net Present Value) ... 23
Sensitivity Analysis ... 24
Sovereign AI Infrastructure Capital Raise Executive Summary ... 25
Investment Thesis ... 25
Capital Structure Overview ... 25
Revenue Model ... 25
Risk Mitigation ... 25
Strategic Positioning ... 25
Executive Mandates ... 26
Due Diligence and Fiduciary Responsibility ... 27
Application Factory with Adjustable Quality Control Gates ... 28
SBOM in Operation ... 29
Vendor Risk Management and Supply Chain Management ... 29
Quantum Readiness and Post-Quantum Cryptography ... 30
Pilot System – Phase I ... 30
Roll-Out in Waves – Phase II ... 31
Final System – Fully Implemented – Phase III ... 31
The final Deliverable – Your Ideal System ... 32
Completed project includes: ... 32

Table of figures

Figure 1: Hyperscale Data Center Architecture - Executive Overview....5
Figure 2: Energy Flow: Grid to GPU 6
Figure 3: : Liquid Cooling - Closed Loop Model....7
Figure 4: Liquid Cooling - Closed Loop Model (version 2) 8
Figure 5:Cybersecurity & Regulatory Controls Crosswalk diagram....9
Figure 6: Institutional Data Center Risk Matrix 11
Figure 7: KPI & Governance Model for Hyperscale AI Data Centers 12
Figure 8: Institutional Implementation Roadmap (5 Phase Model)....13
Figure 9: Microgrid overview. 16
Figure 10: Microgrid Operations....17

Executive Summary

Hyperscale AI Data Centers represent sovereign-scale digital infrastructure. These facilities function as compute power plants integrating high-density GPU clusters, industrial-grade energy systems, liquid cooling architecture, zero-trust cybersecurity, regulatory compliance frameworks, and resilience engineering.

This institutional white paper provides investors, regulators, and operators with an integrated framework for design, implementation, governance, and operational oversight.

1. Hyperscale AI Reference Architecture

The hyperscale model integrates energy, compute, cooling, network fabric, cybersecurity overlay, and governance monitoring into a unified operating system.

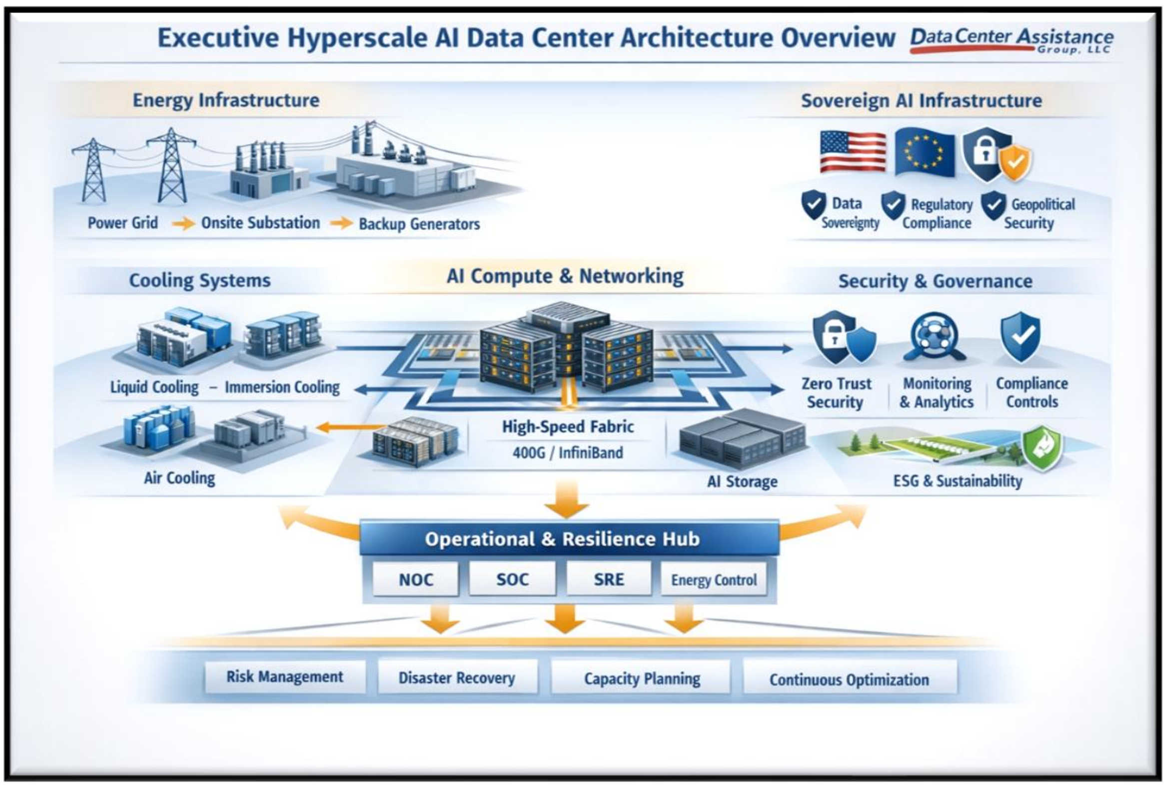


Figure 1: Hyperscale Data Center Architecture - Executive Overview of Operational areas.

2. Energy Systems & Interconnection Risk Modeling

Energy planning is the primary gating factor for hyperscale AI campuses. Design requires multi-year utility coordination, transformer procurement, renewable integration, and redundancy topology.

Key Components:

- Dual high-voltage utility feeds
- Onsite substation integration
- 2N or N+1 redundancy
- Battery Energy Storage Systems (BESS)
- Renewable Power Purchase Agreements (PPA)

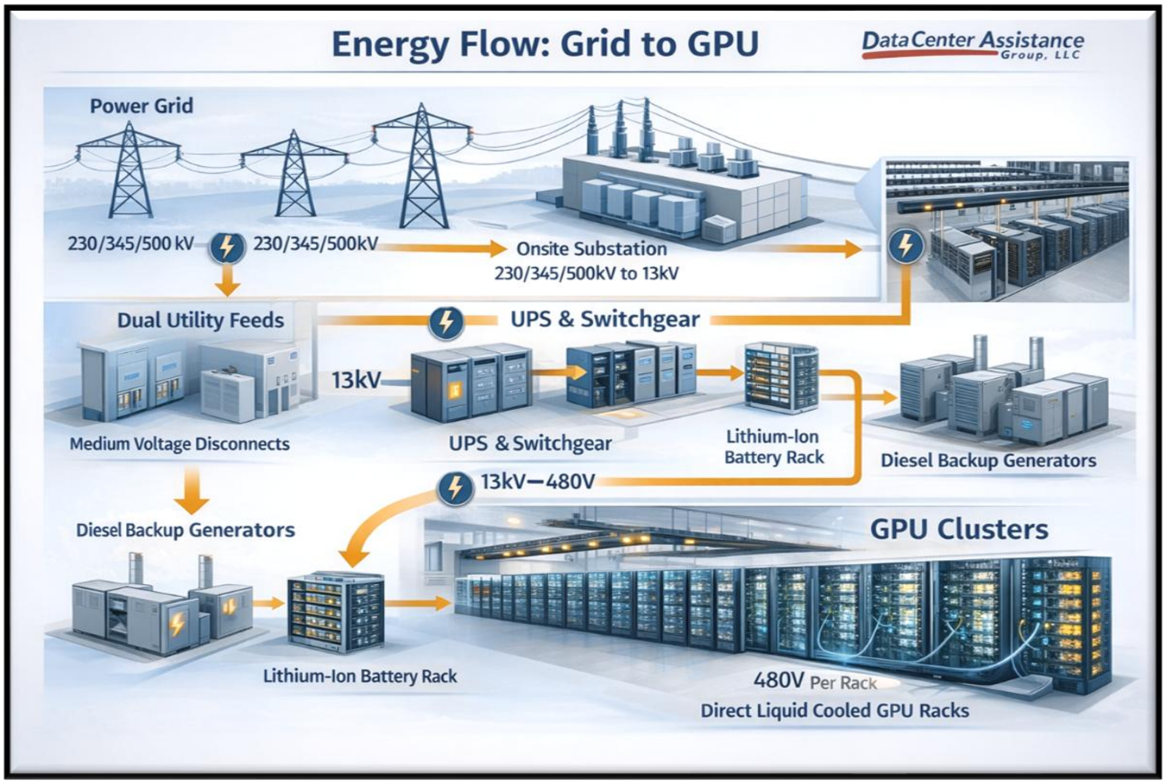


Figure 2: Energy Flow: Grid to GPU

3. Thermal Engineering & Water Governance

AI rack densities exceeding 100kW require liquid-based thermal management. Cooling resilience directly correlates with AI workload availability.

Cooling Models:

- Direct-to-chip liquid cooling
- Immersion cooling
- Hybrid chiller integration
- Heat reused infrastructure.

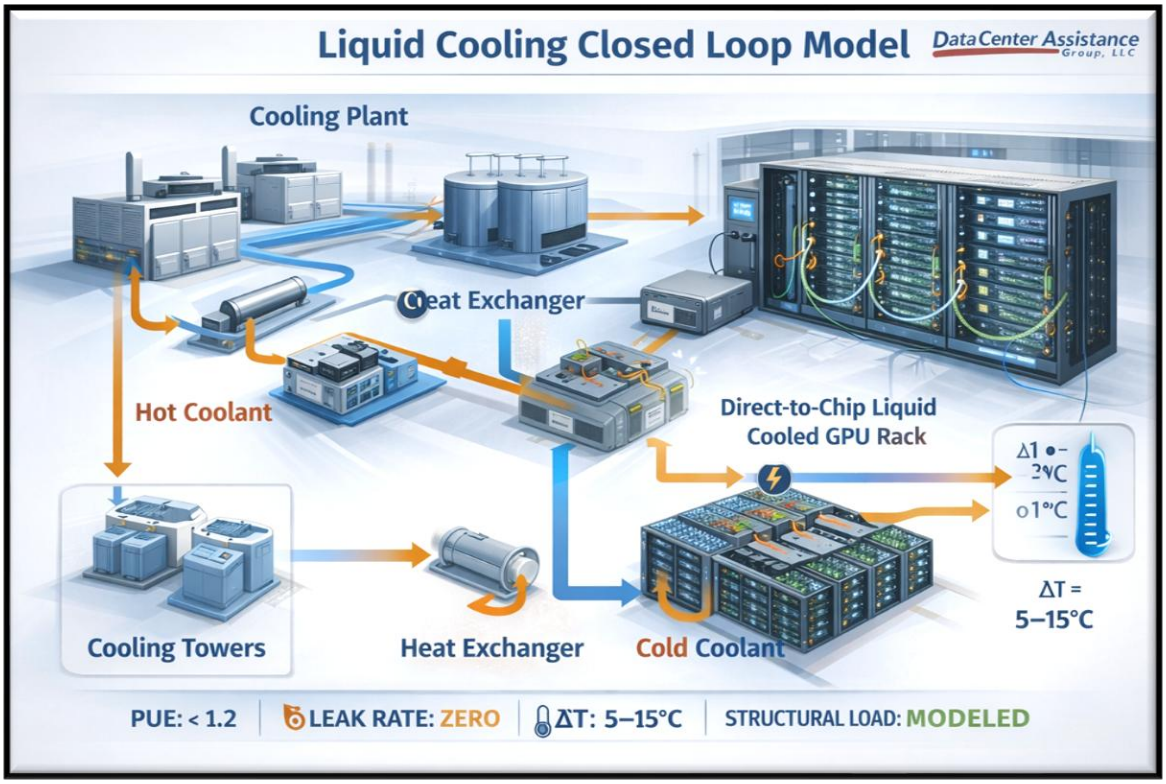


Figure 3: : Liquid Cooling - Closed Loop Model (Version 1).

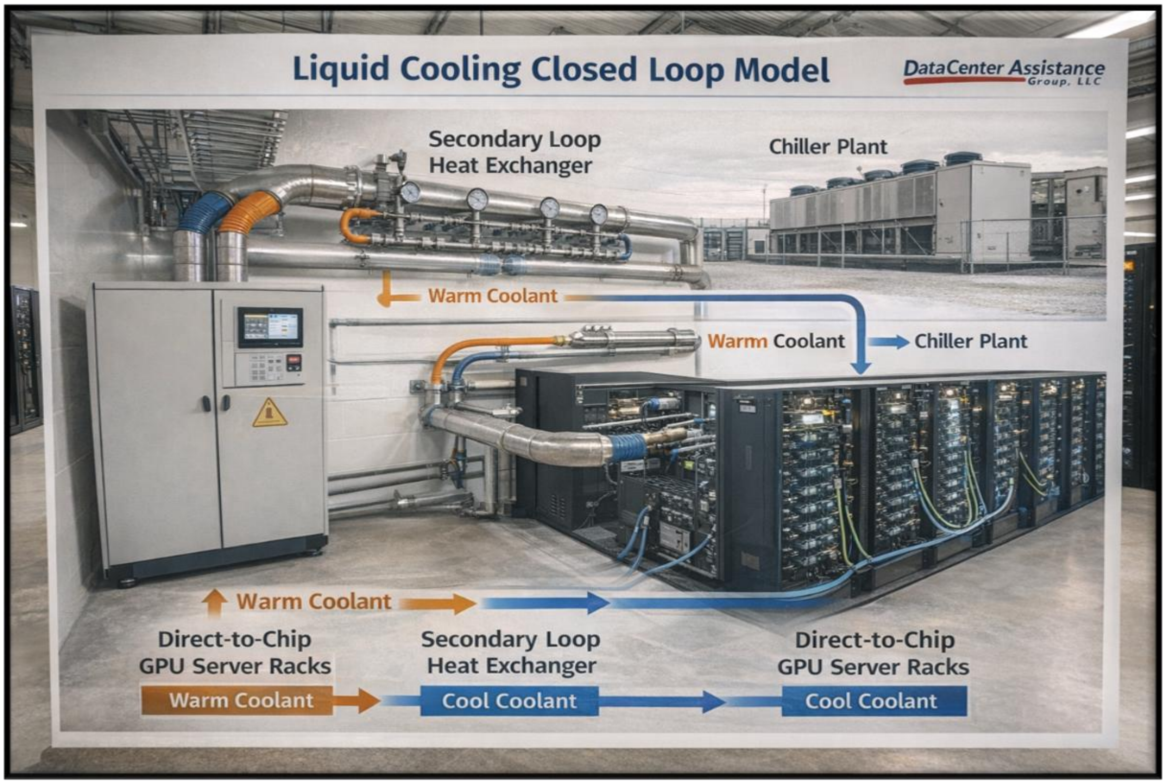


Figure 4: Liquid Cooling - Closed Loop Model (version 2).

4. Cybersecurity & Regulatory Control Crosswalk

Hyperscale AI facilities must map engineering components to regulatory control families including NIST SP 800-53, ISO 27001, SOC 2, CMMC, GDPR, and energy regulations.

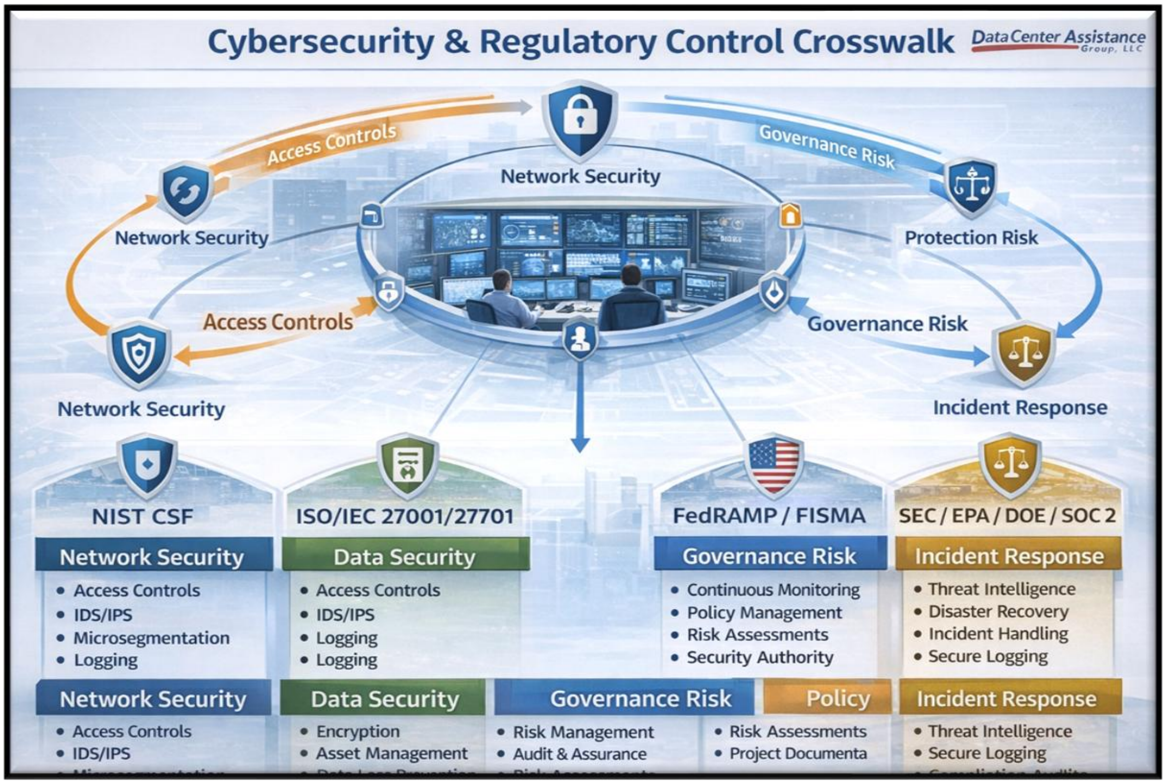


Figure 5:Cybersecurity & Regulatory Controls Crosswalk diagram.

Control Domains:

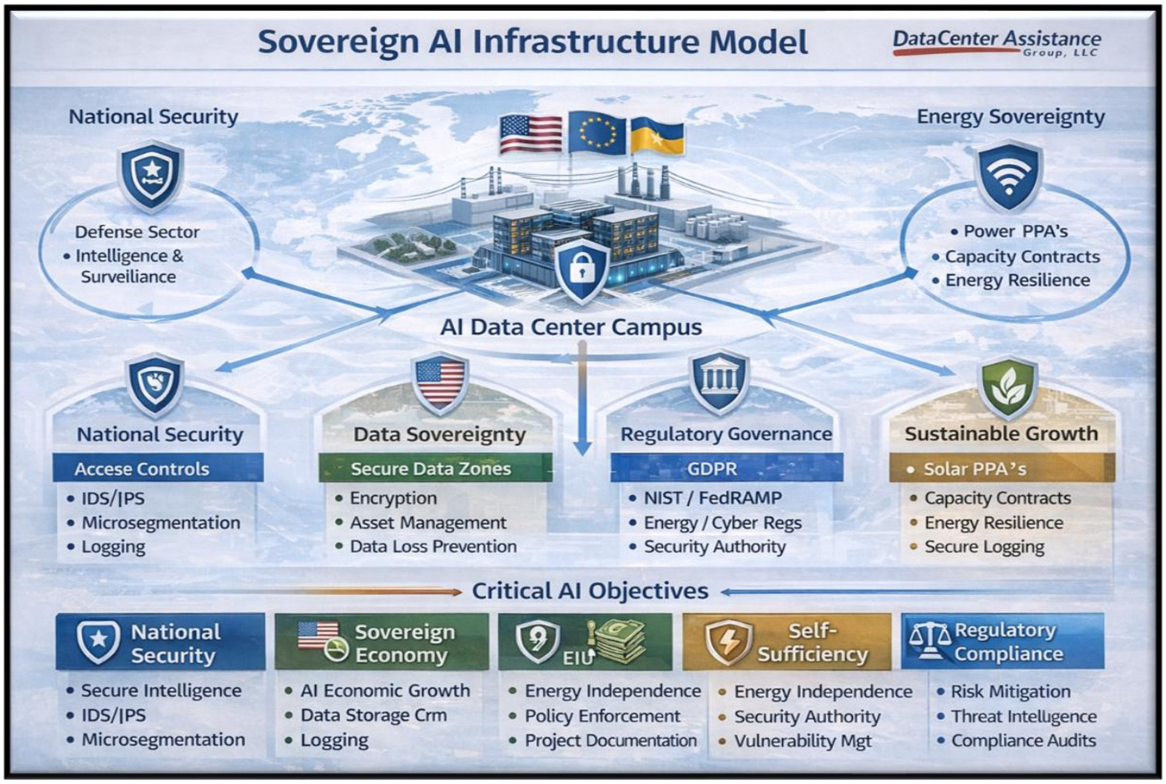
- Physical Security (PE)
- Network Security (SC)
- Identity & Access Management (IA)
- Audit & Logging (AU)
- Supply Chain Risk (SR)
- Environmental Compliance

Audit Process:

- Define all laws & regulations requirements within your “Audit Universe.”
- Create Crosswalk documents with laws covered and artefacts required.
- Develop Auditor documents and process (also frequency of audits).
- Perform audits and produce audit reports.
- Place gaps and exceptions into Risk Register with corresponding POA&M.
- Resolve issues within agreed upon time limit.

5. Sovereign AI Infrastructure Model

Sovereign AI campuses must enforce data residency, geopolitical supply chain control, national security zoning, lawful intercept capability, and independent energy assurance.



Sovereign Controls Include:

- Domestic manufacturing preference
- Controlled firmware provenance
- AI workload segmentation by authority
- National cyber oversight alignment

6. Institutional Risk Matrix

Figure 6: Institutional Data Center Risk Matrix

Primary Risk Domains:

- Grid instability
- Transformer procurement delays
- Cooling cascade failure
- GPU supply chain constraint
- Water restrictions
- Regulatory enforcement action
- Cyber compromise of AI models

7. KPI & Governance Model

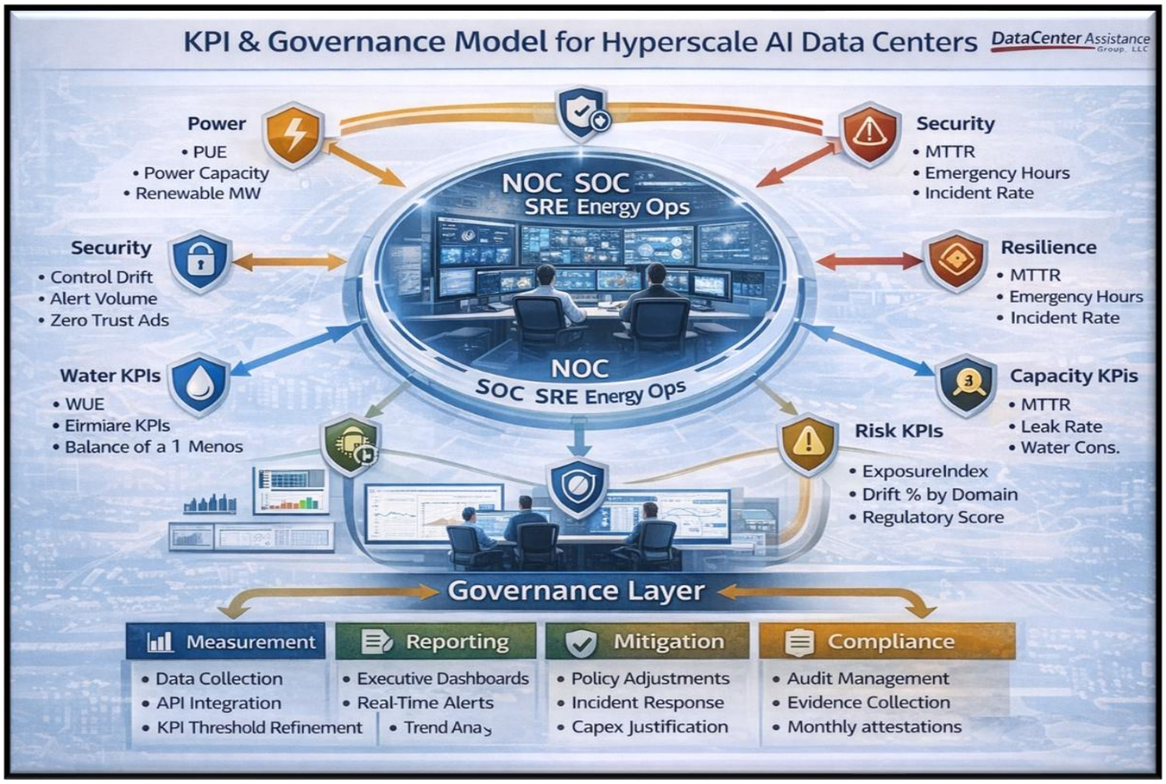


Figure 7: KPI & Governance Model for Hyperscale AI Data Centers

Operational KPI Categories:

- Power Usage Effectiveness (PUE)
- Water Usage Effectiveness (WUE)
- Carbon Usage Effectiveness (CUE)
- GPU Utilization Rate
- MTTR / MTBF
- Compliance Drift Rate
- Risk Exposure Index

8. Implementation Roadmap (5-Phase Model)

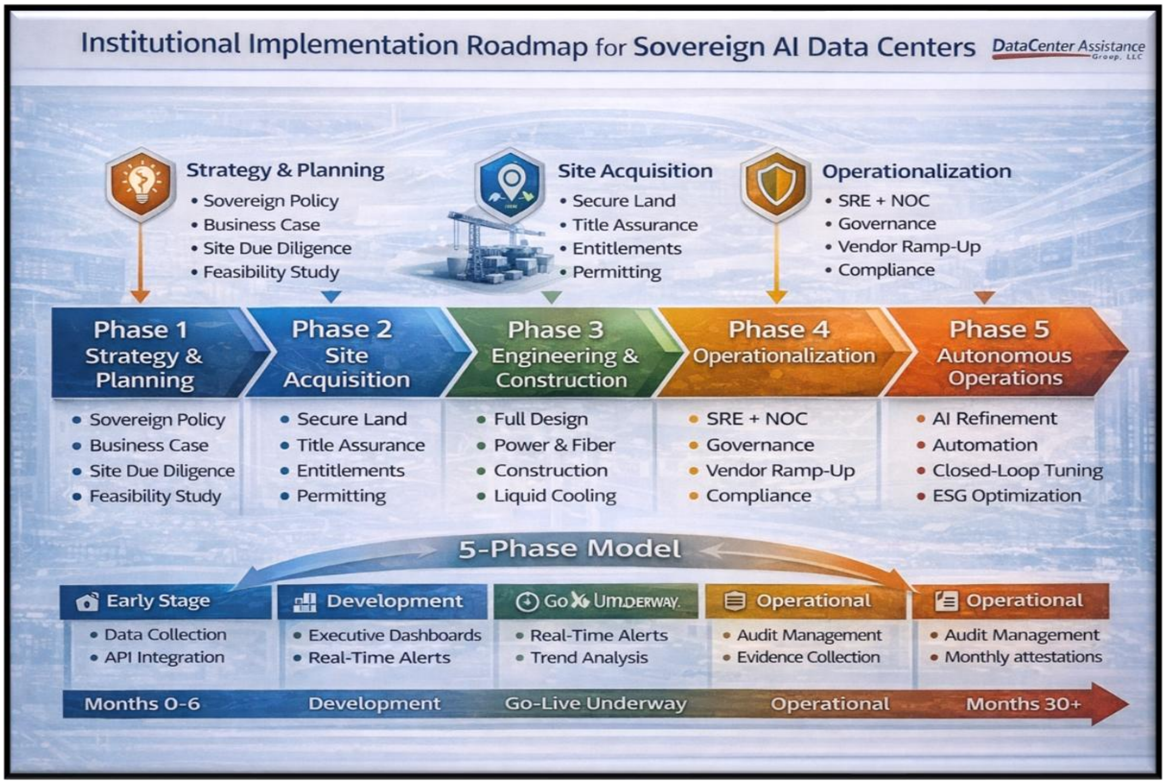


Figure 8: Institutional Implementation Roadmap (5 Phase Model)

Phase 1 – Energy & Feasibility Commitment

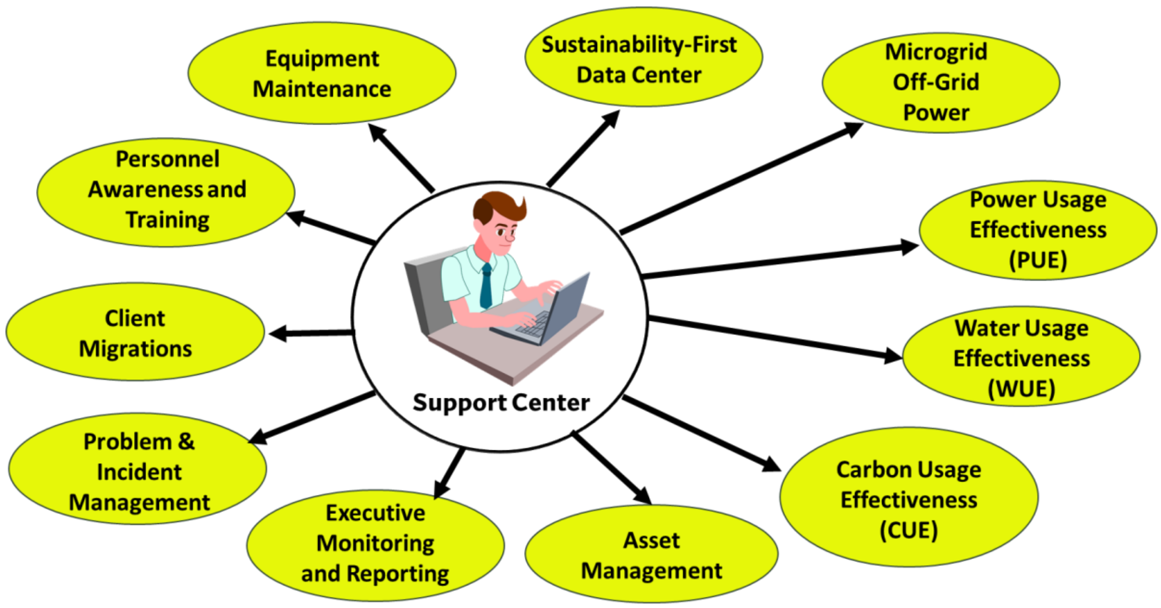
Phase 2 – Engineering Design & Regulatory Approval

Phase 3 – Construction & Commissioning

Phase 4 – AI Fabric Integration & Testing

Phase 5 – Continuous Optimization & Governance Automation

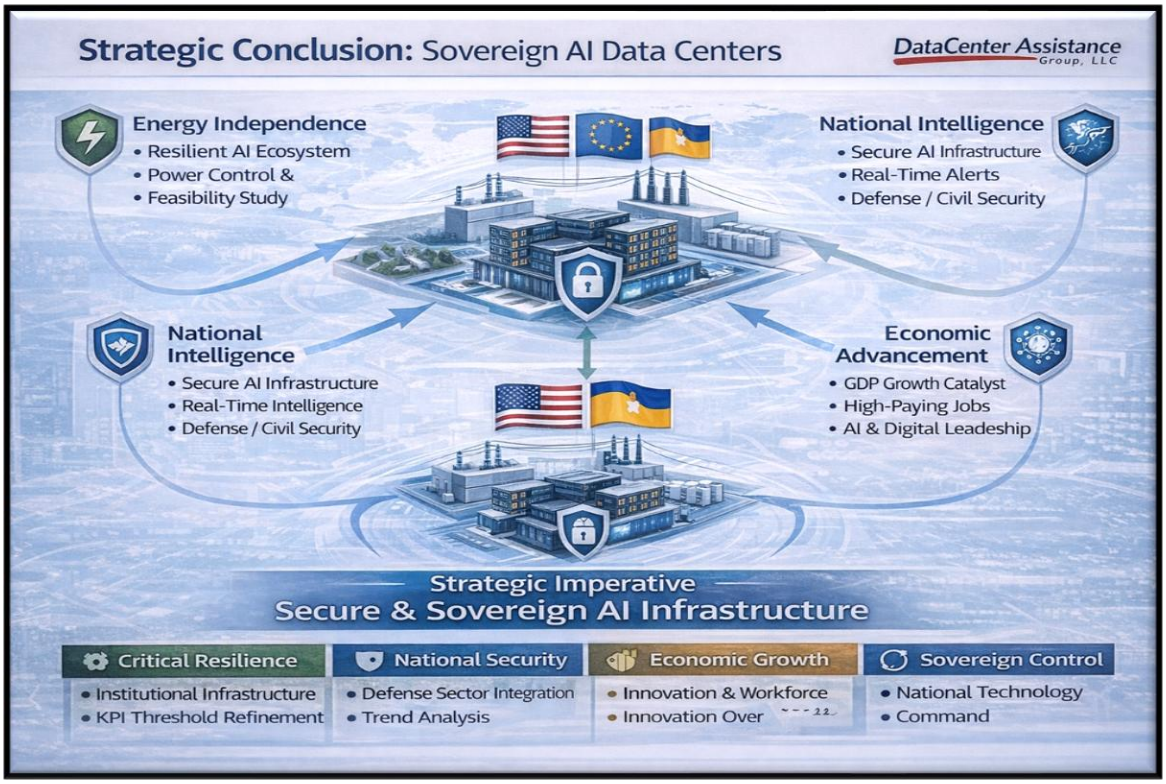
9. Managing & Reporting on Data Center Operations



The Support Center will have the capability to monitor the operation of all components within the data center environment, so that rapid responses can be taken to correct issues within predefined times based on criticality. All single-points-of-failure will be eliminated to support continuous operations by bypassing failing components until they can be repaired or replaced.

Component Maintenance schedules will be monitored along with encountered problems. Personnel will be directed to failing components with instructions on how to diagnose and mitigate encountered problems. A problem database will be developed to quickly address repeat problems. Unfamiliar problems when resolved will be added to the problem database to optimize problem resolutions going forward.

10. Strategic Conclusion



Hyperscale AI data centers must be engineered as sovereign-grade, energy-intensive, regulatory-aligned infrastructure systems. Data Center Assistance Group, LLC provides governance-integrated advisory to align engineering execution with resilience, compliance, and national AI strategy.

Microgrid Architecture for Sovereign Hyperscale AI Campuses

Strategic Rationale

Hyperscale AI campuses (100–500+ MW) cannot rely solely on external grid stability.
A sovereign AI facility must behave as:

A semi-autonomous energy island capable of controlled separation and rapid recovery.

Microgrid capability transforms the facility from a grid-dependent consumer into a grid-interactive asset.

1. Microgrid Architecture Overview

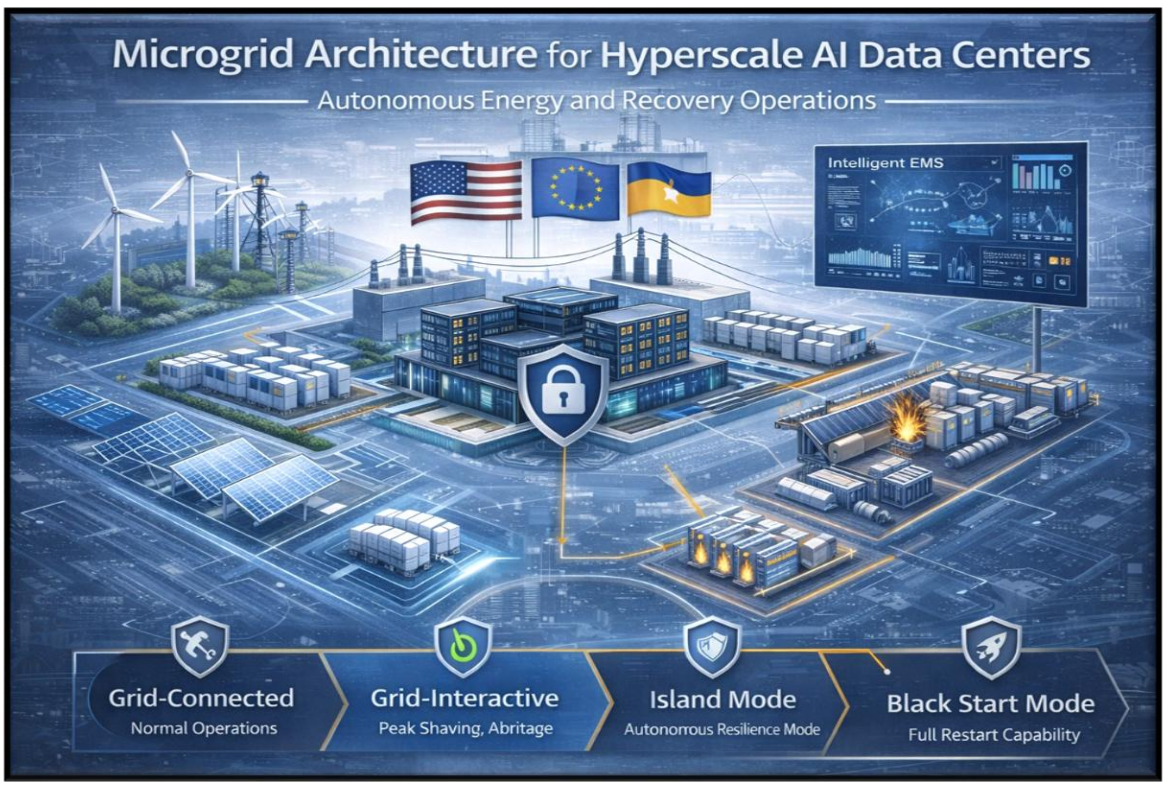


Figure 9: Microgrid overview.

Works under the following conditions:

1. **Connected to the** Grid – Normal Operations.
2. **Interactive with the Grid** – Load sharing to save energy during peak hours.
3. **Island Mode** – to support data center off grid in autonomous mode.
4. **Black Start Mode** – ability to start data center operation off grid through battery power, when continuous power through self-generation mode.

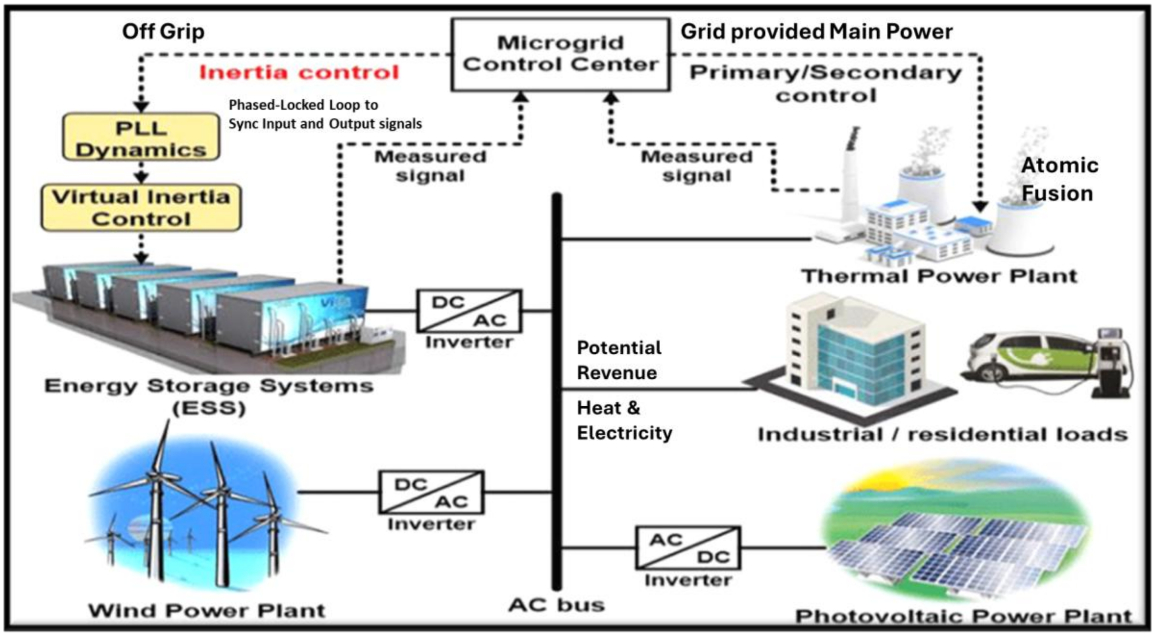


Figure 10: Microgrid Operations

Core Components

1. Dual utility feeds (Separated to reduce blast impact).
2. Onsite substation with islanding switchgear (allow for standalone off grid).
3. Battery Energy Storage System (BESS) store solar and wind.
4. Dispatchable generation (gas turbines / reciprocating engines).
5. Renewable integration (solar, wind via PPA or onsite).
6. Intelligent Energy Management System (EMS).
7. Load prioritization logic (critical AI clusters vs non-critical loads).

2. Microgrid Operating Modes

Mode	Description	Investor Implication
Grid-Connected	Normal operations	Lowest cost energy
Grid-Interactive	Peak shaving, arbitrage	Revenue opportunity
Island Mode	Full autonomous operation	Sovereign resilience
Black Start Mode	Restart from total outage	Mission critical

3. Black Start & First Recovery Techniques

This is the section investors and regulators care about most. Restarting data centers off grid when power is lost. Provides uninterrupted power supply to production data centers.

3.1 Black Start Capability

Black start = ability to restart without grid power.

Sequence Model

1. BESS energizes control systems (Batteries provide power).
2. Start primary onsite generation (Backup Generators pick up load).
3. Stabilize frequency and voltage (Power Stabilization & Load Balancing).
4. Sequentially energize:
    - Substation bus
    - UPS systems
    - Cooling plant
    - Network core
    - GPU clusters
5. Re-synchronize to grid when available.

3.2 -Tiered Load Recovery Hierarchy

AI facilities must not attempt full cold restart simultaneously.

Recovery Priority Order

1️⃣ Energy control systems
2️⃣ Cooling plant primary loop
3️⃣ Core network fabric
4️⃣ Security systems (SOC/NOC)
5️⃣ GPU cluster tranche 1 (mission critical workloads)
6️⃣ Remaining GPU clusters
7️⃣ Non-critical administrative systems.

This prevents inrush current collapse and thermal shock.

3.3 Recovery Time Objectives (Executive Model)

System	Target RTO
Control Systems	< 1 minute
Cooling Primary Loop	< 5 minutes
Network Core	< 10 minutes
Critical GPU Cluster	< 20 minutes
Full Campus	< 60–90 minutes

For sovereign AI classification, sub-30-minute recovery of critical clusters is ideal.

ESG Sustainability Framework for Hyperscale AI

ESG in hyperscale AI is not marketing. It is:

- Regulatory.
- Capital market driven.
- Insurance driven.
- Geopolitical driven.

4. Energy Sustainability Model

4.1 Renewable Integration

Components:

- Long-term renewable PPAs (Power Purchase Agreements).
- Onsite solar, or wind, where feasible.
- BESS smoothing of intermittency.
- Heat reuse for district heating (resell to public utility if possible).
- Carbon intensity real-time tracking (CUE – Carbon Usage Efficiency).

Carbon & Efficiency KPIs

Metric	Target
PUE - Power Usage Efficiency	< 1.2
WUE – Water Usage Efficiency	Minimized regional baseline
CUE – Carbon Usage Efficiency	Year-over-year reduction
% Renewable	60–100% long-term
Scope 2 Emissions	Transparent reporting

4.3 Water Sustainability Strategy

Hyperscale liquid cooling increases water risk exposure.

Mitigation:

- Closed-loop cooling systems.
- Non-potable water source.
- Air-to-liquid hybrid models.
- Water recycling systems.
- Regional water impact studies.

ESG-Aligned First Recovery Protocol

When outage occurs:

ESG-Compliant Recovery Principles

1. Prioritize renewable-backed generation first.
2. Avoid diesel unless necessary.
3. Dispatch BESS before fossil backup.
4. Maintain emissions reporting during outage.
5. Log and report recovery metrics.

This becomes a capital-market trust signal.

Microgrid Revenue Opportunity Layer

A sovereign AI campus microgrid is not just protection.

It can:

- Participate in demand response markets.
- Sell ancillary services.
- Provide grid stabilization.
- Perform peak arbitrage.

This improves project IRR and reduces net LCOE.

Integrated Risk Reduction Impact

Microgrid + ESG reduces:

- Grid outage exposure.
- Insurance premiums.
- Regulatory penalties.

- Political risk.
- ESG capital cost spread.
- Sovereign dependency risk.

Investor Narrative Framing

Position this as:

“Resilient Energy-Integrated Sovereign AI Infrastructure with Autonomous Recovery Capability.”

This language resonates with:

- Infrastructure funds.
- Sovereign wealth funds.
- National security stakeholders.
- ESG-driven institutional investors.

Financial Information Tables

Assumptions

Parameter	Value	Units
Campus Capacity	250	MW
IT Load Utilization	75	%
CapEx per MW	9000000	USD
Power Cost per kWh	0.065	USD
Annual Operating Cost % of CapEx	8	%
GPU Revenue per MW per Year	15000000	USD
Project Life	15	Years
Discount Rate	10	%

CapEx (Capital Expenditures) Expenditures

Category	Cost (USD)
Land Acquisition	$150,000,000.00
Substation & Grid Interconnect	$600,000,000.00
Building & Shell	$800,000,000.00
Cooling Plant	$450,000,000.00
Electrical Systems	$500,000,000.00
IT Infrastructure (GPU/Network)	$1,200,000,000.00
Security & Monitoring	$100,000,000.00
Contingency (10%)	$380,000,000.00
Total CapEx	$4,180,000,000.00

Operating Model

Category	Annual Cost (USD)
Power Cost (250MW @ 75% load)	$106,762,500.00
Staffing	$45,000,000.00
Maintenance	$120,000,000.00
Water & Cooling Ops	$60,000,000.00
Insurance & Compliance	$25,000,000.00
Total Annual OpEx	$356,762,500.00

Revenue Model

Parameter	Value
Revenue per MW	$15,000,000.00
Total MW	$250.00
Utilization	$0.75
Annual Revenue	$2,812,500,000.00

IRR & NPV (Internal Rate of Return &Net Present Value)

Metric	Value
Initial Investment	$4,180,000,000.00
Annual Revenue	$2,812,500,000.00
Annual OpEx	$356,762,500.00
Net Annual Cash Flow	$2,455,737,500.00
Discount Rate	0.1
NPV (15 Years)	-$1,947,511,363.64
IRR (Simplified Approximation)	Use Excel IRR function with full cashflow schedule

Sensitivity Analysis

Variable	Low	Base	High
Power Cost per kWh	0.05	0.065	0.09
Utilization Rate	0.6	0.75	0.9
Revenue per MW	$12,000,000.00	$15,000,000.00	$18,000,000.00
CapEx per MW	$8,000,000.00	$9,000,000.00	$11,000,000.00

Sovereign AI Infrastructure Capital Raise Executive Summary

Investment Thesis

The rapid acceleration of AI demand requires sovereign grade hyperscale infrastructure. This program proposes a 250MW AI data center campus engineered for energy resilience, regulatory alignment, and long-term institutional returns.

Capital Structure Overview

- Total Estimated CapEx: ~$4B
- Debt Target: 60% Infrastructure Financing
- Equity Target: 40% Institutional + Strategic Capital
- Project Life: 15 Years
- Target Equity IRR (Internal Rate of Return): 18–24% (Base Case)

Revenue Model

- GPU-as-a-Service contracts
- Enterprise AI cluster leasing
- Government sovereign AI workloads
- Strategic AI partnerships

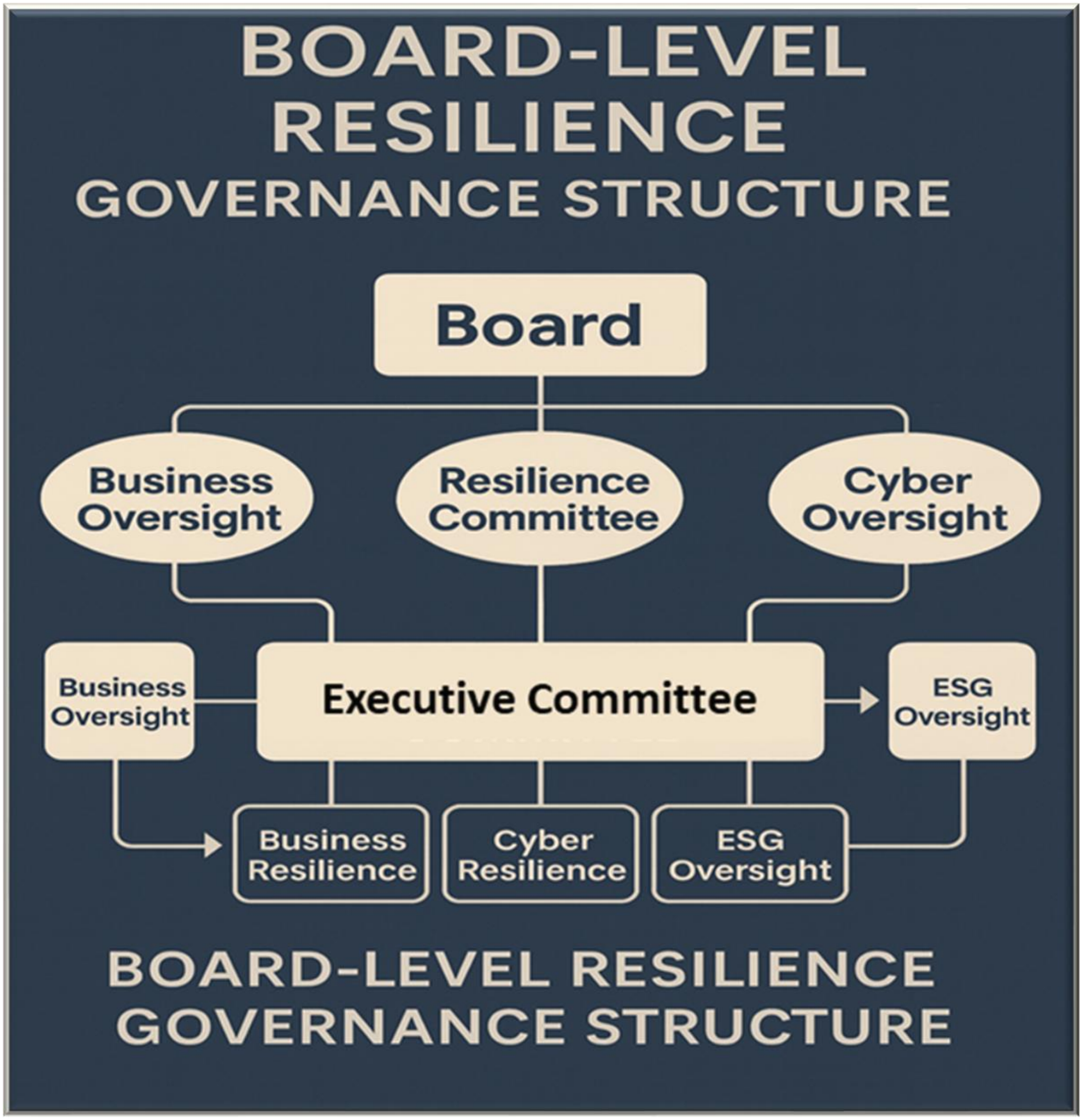
Risk Mitigation

- Dual utility feeds + BESS
- Long-term power purchase agreements
- Vendor diversification for GPUs
- Regulatory governance integration
- Predictive maintenance & SRE oversight

Strategic Positioning

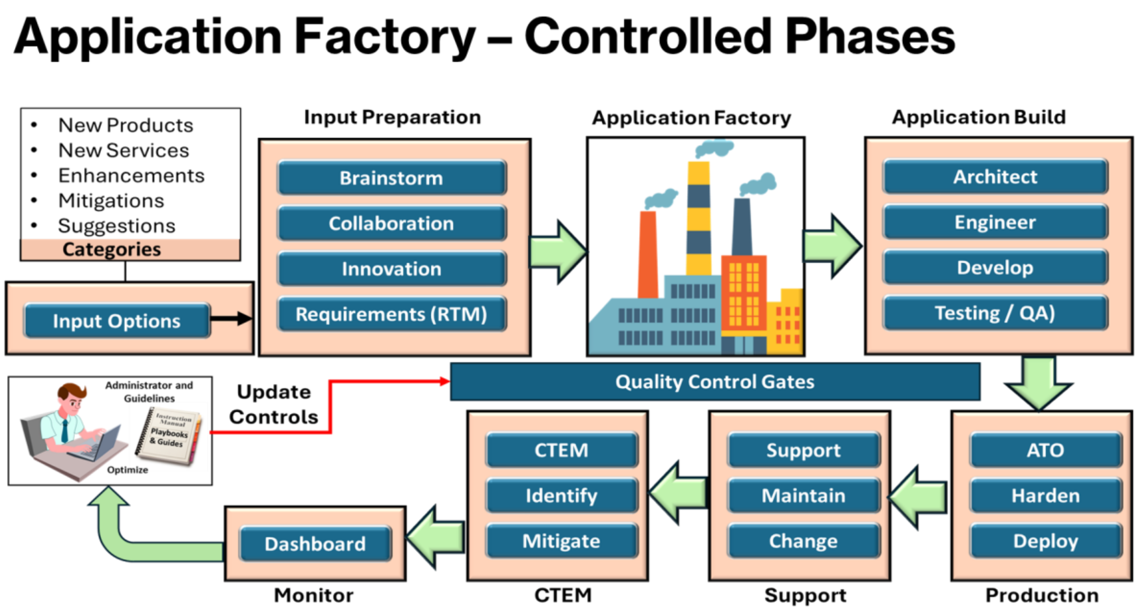
Positioned as Sovereign AI Infrastructure, this campus integrates energy independence, data residency compliance, and national security alignment. Designed to meet institutional investor criteria for resilience, ESG, and regulatory oversight.

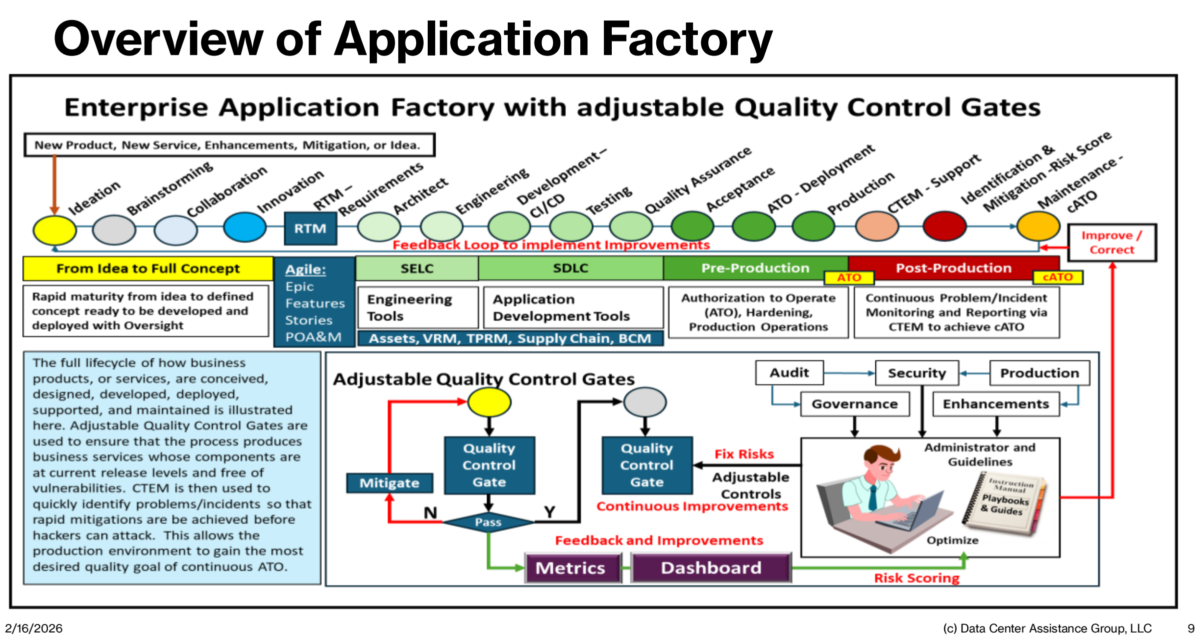
Executive Mandates



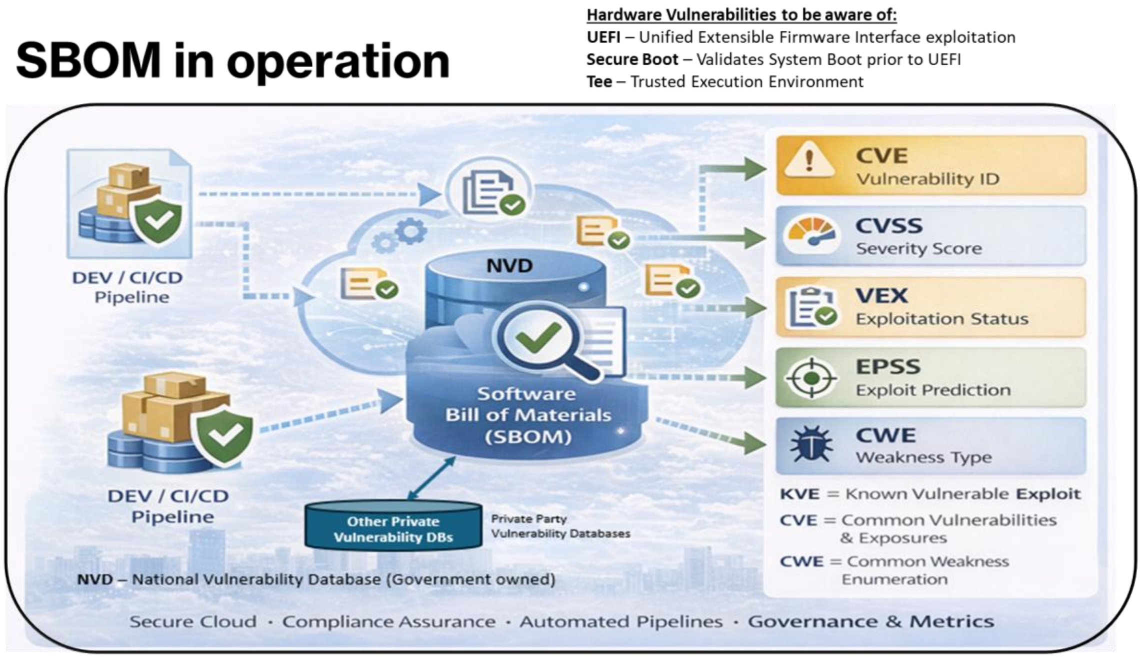
Due Diligence and Fiduciary Responsibility

Application Factory with Adjustable Quality Control Gates

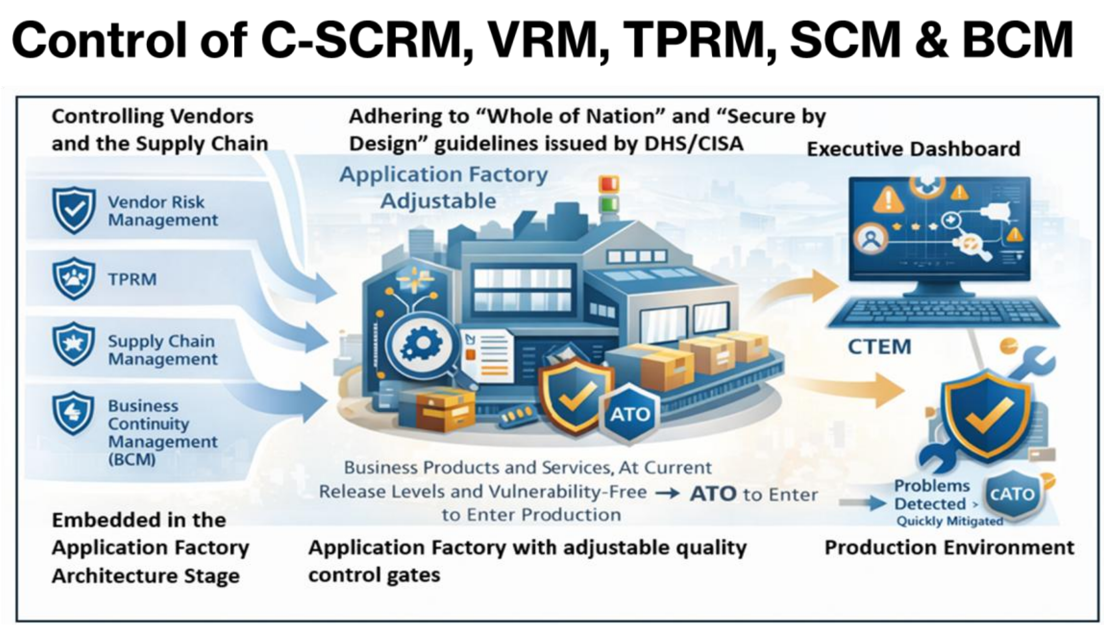




SBOM in Operation



Vendor Risk Management and Supply Chain Management



Quantum Readiness and Post-Quantum Cryptography

The Quantum Threat to Data Security

- **Quantum computers** will break current encryption standards
- **Data encrypted today** can be stolen and stored for decryption later ("harvest now, decrypt later") by Hackers
- **Only Post Quantum Cryptography** (PQC) can protect your data, but only if you convert to PQC before data is stolen.
- **Protect** your critical infrastructure, financial systems, supply chains, and sensitive data at risk
- **Timeline:** Quantum computers capable of breaking RSA encryption within 5-10 years

Quantum Computing Threat

Current encryption methods like RSA and ECC will be vulnerable to quantum algorithms.

Developing a Quantum-Readiness Roadmap

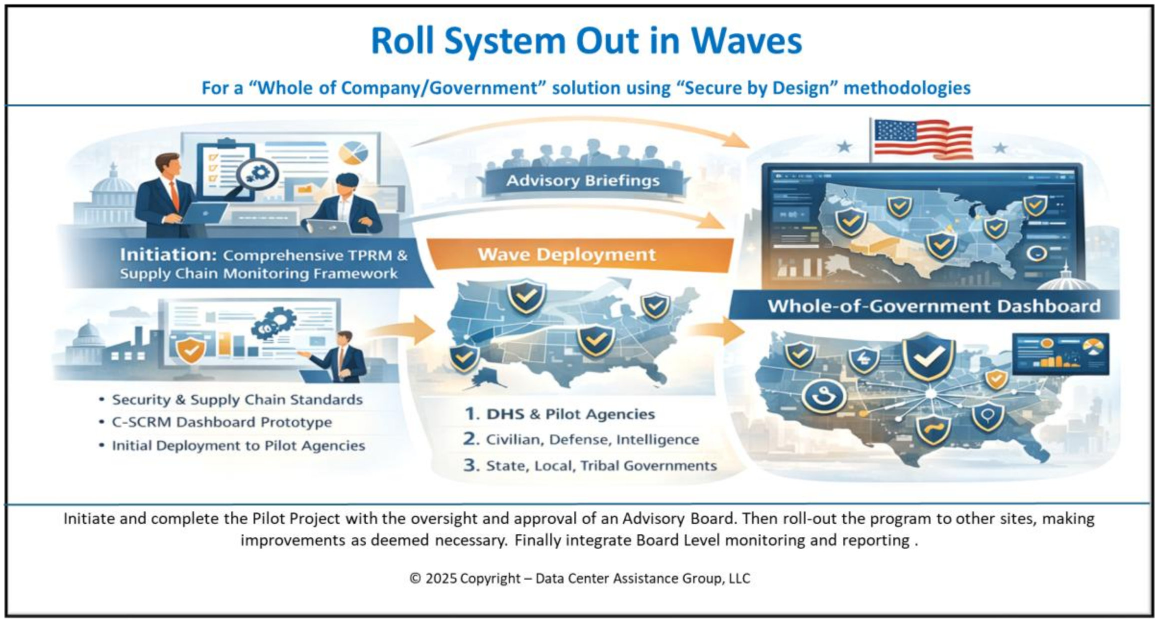
> Shor's Algorithm can factor large numbers exponentially faster than classical computers, breaking encryption that secures your data today. Grover's Algorithm can rapidly crunch numbers

CISA Post Quantum Readiness Report

Pilot System – Phase I

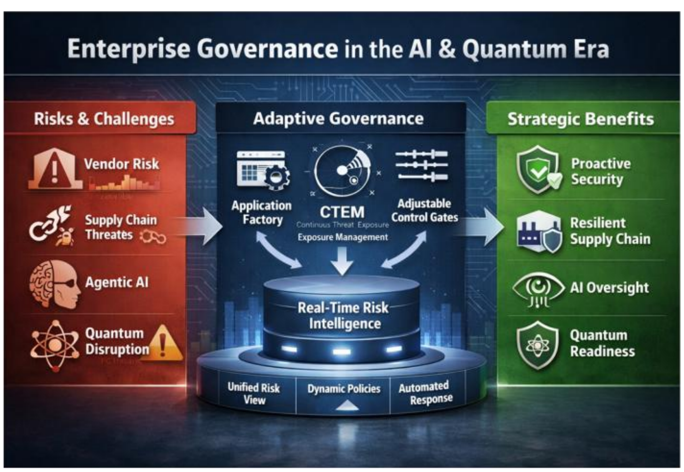
1. eDiscovery – Inventory & Configuration
2. Risk Assessment and Vendor Identification.
3. Prioritize and sequence mitigation.
4. Define Vendor onboarding requirements.
5. Define Vendor Contract and SLA.
6. Onboard or reject vendors.
7. Monitor & Maintain Vendor approvals.

Roll-Out in Waves – Phase II



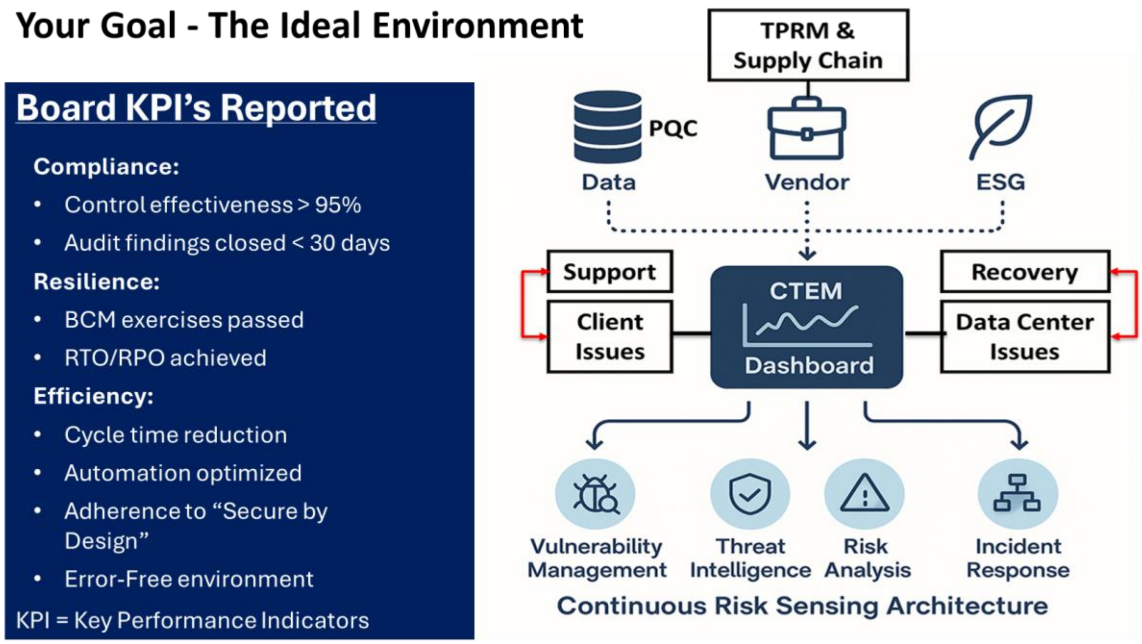
Final System – Fully Implemented – Phase III

Fully implemented Enterprise Governance in AI and Quantum Era with Application Factory



- **Continuously Achieve Due Diligence and Fiduciary Responsibilities (Dashboard).**
- **Implement Application Factory with Adjustable Quality Control Gates and CTEM to fully automate security & compliance.**
- **Provide Real-Time Risk Monitoring and Controls (Vendor, Vulnerability, PQC, etc.).**
- **Automated Security protection.**
- **Automate Dynamic Policies.**
- **Automated Responses for continuous optimization.**
- **Quantum Readiness and use of ML/AI automation.**

The final Deliverable – Your Ideal System



Completed project includes:

1. Hyperscale AI Data Center
2. Application Factory with Adjustable Quality Control Gates.
3. All Board Level Requirements fulfilled.
4. Continuous application delivery mechanism with all services contained in a fully encapsulated and controlled environment.
5. ATO and cATO achieved, with CTEM and continuous monitoring.
6. Quantum Ready environment.
7. Vendor and Supply Chain Management.
8. Vulnerability Management with Hardened Production environment.
9. Documentation, Awareness, and Training provided to staff.
10. Single system to provide all your needs, capable of being automated via Agentic AI Agents for optimized workflow and adherence to compliance requirements.