Mission-Critical, Now AI-Critical

Why Facility Management Owns the Next Phase of Data Center Operations

How artificial intelligence is transforming data center operations, resilience, energy strategy, workforce readiness, and the facility manager's role in mission-critical environments

The Bottom Line

The data center industry’s hardest AI problem is not computing, cooling, or power. It is governance — the discipline of running physical infrastructure, digital systems, energy strategy, and operational risk as one coordinated environment. That is facility management work. The organizations that recognize this and restructure around it will operate the next generation of data centers. The organizations that don’t will lose control of theirs.

Prepared by: Ebony D. Wilson, Logic

August 2026

Executive Summary

Artificial intelligence is putting unprecedented pressure on the data center as a building. Rack densities that used to top out at 5 to 10 kilowatts now exceed 50 to 130 in AI training environments. Power, cooling, water, and grid coordination are becoming public-facing issues with regulatory and reputational consequences. And the systems that monitor all of it — BMS, EPMS, DCIM, CMMS, IT telemetry — sit in five separate platforms, owned by four different teams, governed by three different vendors. This paper argues that the discipline required to operate inside that complexity is facility management discipline, and that the next phase of data center operations will be defined less by which AI tools an organization buys than by whether its facility leadership has the standing, the data, and the governance to use them well.

AI affects data center management in two ways. First, AI workloads are changing the physical requirements of the facility: denser compute, more heat, greater power availability requirements, and new cooling architectures. Second, AI tools are becoming part of the management layer itself, enabling predictive maintenance, energy optimization, anomaly detection, digital twins, capacity planning, and automated decision support. The facility manager is now positioned at the intersection of building systems, IT infrastructure, utility constraints, cybersecurity, sustainability reporting, and enterprise risk.

The opportunity is significant, but it is not automatic. AI-enabled operations require trusted data, disciplined governance, cyber-aware system integration, workforce upskilling, and a clear understanding of what should be automated versus what should remain human-controlled. The organizations that gain the most value will be those that treat AI not as a software overlay, but as a management capability embedded into asset strategy, operations, commissioning, maintenance, procurement, energy planning, and executive reporting.

This white paper outlines the major impacts of AI on data center management and offers a practical framework for facility leaders preparing to operate in a higher-density, higher-accountability, AI-enabled future.

Key Takeaways for Facility Management Leaders

Management Area	AI Impact
Power and capacity	AI workloads intensify demand forecasting, grid coordination, power quality management, and capital planning.
Cooling and thermal performance	Higher rack densities accelerate adoption of liquid cooling, hybrid cooling, thermal modeling, and real-time airflow optimization.
Operations and maintenance	Predictive analytics shift teams from calendar-based maintenance to condition-based, risk-prioritized interventions.
Resilience and risk	AI improves anomaly detection and scenario planning, but also introduces governance, cybersecurity, and overreliance risks.
Workforce	Facilities, IT, energy, security, and sustainability teams need shared operating language and expanded technical fluency.
Sustainability reporting	AI increases energy intensity while improving performance reporting.

The New Data Center Reality: AI as Both Demand Driver and Operating Tool

The data center has always been a convergence point for real estate, power, cooling, network, and physical security. AI raises the stakes across all of those domains. Training and inference workloads require dense clusters of specialized processors, high-speed interconnects, and tightly controlled thermal environments. At the same time, enterprise and public-sector dependence on digital services means that downtime, degraded performance, or constrained capacity can quickly become a business continuity issue.

The International Energy Agency reported that electricity demand from data centers increased sharply in 2025, with AI-focused data centers growing even faster than the sector overall [1]. Uptime Institute's 2025 global survey similarly describes an industry facing rising costs, worsening power constraints, staffing pressure, supply-chain delays, and the challenge of modernizing facilities to support AI [2]. These dynamics make clear

that AI is not simply increasing data center demand; it is changing the operational context in which facilities are planned, staffed, financed, and managed.

For facility managers, the central question is shifting from "How do we keep the facility running?" to "How do we operate a high-density, data-rich, energy-constrained environment with enough intelligence to anticipate risk before it becomes disruption?"

Stop Maintaining Calendars. Start Maintaining Risk.

Most data centers already produce the data they need to run AI-enabled operations. They just can't get to it. BMS, EPMS, DCIM, fire and life safety, CMMS, IT telemetry, utility feeds, weather, and access logs sit in separate systems, owned by separate teams, on separate refresh cycles, with separate definitions of basic terms like "asset," "criticality," and "event." Until that fragmentation is resolved, every AI investment is a wrapper around a foundation that doesn't agree with itself. The work of unifying it is not glamorous. It is also non-negotiable.

In maintenance, this means moving beyond fixed intervals and alarm-driven response. AI models can analyze vibration, temperature, humidity, pressure, amperage, breaker behavior, battery health, pump performance, and chiller efficiency to identify early indicators of degradation. Instead of treating all preventive maintenance tasks equally, teams can prioritize work by asset criticality, probability of failure, operational consequence, and maintenance window availability.

The value for FM leaders is not only reduced downtime. It is better labor allocation, fewer emergency callouts, improved spare parts planning, and a clearer business case for capital renewal. AI does not replace disciplined asset management; it strengthens it by turning operational history into forward-looking insight.

Power Is No Longer an Engineering Question. It Is a Strategy Question.

AI growth has made power availability one of the defining constraints in data center strategy. Historically, facility teams managed power as a reliability and capacity issue within the boundaries of the site. Increasingly, they must manage it as a strategic resource connected to utility interconnection timelines, transmission constraints, market pricing, renewable procurement, backup generation, battery storage, and corporate carbon commitments.

This is especially important because the public conversation around AI infrastructure is intensifying. Electricity demand from data center expansion is now being linked to utility planning, local rate impacts, grid modernization, and permitting decisions. Facility leaders must be prepared to explain not only how much power a site uses, but how intelligently that power is managed.

AI can support this shift through load forecasting, automated demand response, power quality analytics, peak shaving strategies, microgrid optimization, and scenario modeling. For example, AI tools can help compare the operational and financial implications of shifting noncritical workloads, sequencing equipment start-up, using battery storage during peak tariff periods, or coordinating maintenance with lower-risk load windows. The facility manager's role expands from equipment steward to energy strategist.

Cooling Architecture Moves from Efficiency Project to Core Business Risk

AI workloads are driving higher thermal loads and challenging the limits of traditional air-cooled environments. While air cooling will remain important for many spaces and supporting electrical infrastructure, high-density AI deployments are accelerating liquid cooling, rear-door heat exchangers, direct-to-chip cooling, immersion cooling, and hybrid architectures. Uptime Institute's AI infrastructure survey found that many owner/operators

hosting AI workloads are upgrading both power distribution and cooling systems to support these new requirements [3].

The facilities implication is profound. Cooling is no longer a back-of-house efficiency issue. It is a capacity, reliability, maintenance, safety, water, and workforce issue. Liquid cooling introduces new requirements for fluid management, leak detection, water treatment, heat rejection, service procedures, vendor coordination, emergency response, and commissioning discipline. It also changes the skills required of facilities teams and the interface between IT hardware design and building infrastructure.

AI can help by improving thermal modeling, optimizing chiller plant operation, identifying stranded capacity, detecting airflow recirculation, predicting hot spots, and supporting dynamic cooling strategies based on actual workload behavior. However, the technology must be paired with strong operating procedures. A model may recommend a setpoint change; the facility team must understand whether that change is safe, compliant, and appropriate for the specific risk profile of the site.

Digital Twins and the Rise of the Data-Driven Facility

Digital twins are becoming a practical bridge between facility design, commissioning, operations, and capital planning. In a data center context, a digital twin can integrate asset data, electrical topology, cooling zones, environmental conditions, maintenance history, capacity models, and live operational telemetry. When paired with AI, the twin becomes more than a visualization tool; it becomes a decision-support environment.

For example, facility teams can simulate the impact of adding high-density racks, taking a chiller offline, delaying a UPS replacement, changing redundancy assumptions, or responding to a utility constraint. They can also compare current operating conditions against design intent and commissioning baselines. This supports a more disciplined approach to change control, especially in live environments where small infrastructure changes can have cascading effects.

For FM professionals, the digital twin also supports executive communication. Rather than describing infrastructure risk in abstract terms, teams can show capacity thresholds, failure scenarios, cost impacts, and operational dependencies in a way that connects facilities decisions to enterprise outcomes.

Sustainability, ESG, and the Measurement Challenge

In light of recent concerns around the proliferation of data centers and their impact on our environment, modern AI data centers will need to evolve past surface level efficiency metrics and implement comprehensive environmental stewardship. PUE and WUE should not be the only tracked metrics. Organizations should measure carbon free energy matching, embodied carbon, refrigerant management, circular economy oractices, biodiversity impacts, watershed stress, waste diversion, and community environmental indicators. AI has the potential to optimize renewal integration, battery storage, microgrids, water conservation, and carbon aware workload scheduling while providing transparent, auditable ESG reporting.

AI portends a sustainability conundrum for data centers. AI workloads increase energy consumption and intensifies scrutiny of water, land, emissions, and grid impact. That being said, a smart and responsible use of AI has the opportunity to improve efficiency by identifying waste, optimizing cooling, improving maintenance, supporting carbon aware workload scheduling in concert with providing transparent, auditable ESG reporting.

Creating a balance within these spaces will largely depend on management discipline. Facility leaders and their teams will need to employ robust measurement across efficient power and water usage, carbon intensity, equipment use, renewable energy matching, embodied carbon considerations, and lifecycle replacement decisions. While components of this reporting can be automated by AI, it will be critical that the underlying data is accurate, auditable, and governed

It is at this intersection where IFMA's digital transformation themes become extremely relevant. The facility managers in these spaces will need to evolve their responsibilities to breaking down data silos and leveraging technology to improve performance, resilience, and sustainability outcomes. It is with this effort that AI will become a vehicle to reward the organizations that made investments in data standards, asset registries, system integration, and operational governance.

Cybersecurity and Operational Technology Governance

AI-enabled data center management depends on connected systems. That connectivity introduces risk. Building automation, DCIM, EPMS, CMMS, access control, video systems, IoT sensors, and vendor platforms may all become part of the operational data environment. As those systems become more integrated and algorithmically assisted, cybersecurity and operational technology governance become core FM responsibilities.

The facility manager does not need to become a cybersecurity engineer, but must understand the governance questions: Who owns the data? Which systems can connect? Which vendors can access operational platforms? How are model recommendations validated? What happens if a model is wrong? How are changes logged? What systems remain manually operable? What is the escalation path during an incident?

Sidebar: Eight Governance Questions Every FM Should Be Able to Answer

These questions should be answered before AI-enabled tools are allowed to influence operational decisions. They convert the cybersecurity and OT governance discussion from a general risk theme into an actionable readiness check that facility leaders can use with IT, engineering, vendors, and executive sponsors.

1. Who owns the operational data, and who is accountable when it's wrong?
2. Which systems are authorized to connect to the operational data environment, and who approves new connections?
3. Which vendors can access operational platforms, under what conditions, and with what audit trail?
4. How are model recommendations validated before they affect operations?
5. What happens if a model is wrong, and who has authority to override it?
6. How are changes to AI-influenced control logic logged and reviewed?
7. Which systems must remain manually operable in the event of AI, network, or vendor failure?
8. What is the escalation path during an incident, and who is authorized to invoke it?

In mission-critical environments, AI governance should include human-in-the-loop controls, role-based access, model monitoring, vendor risk management, disaster recovery planning, cybersecurity training, and clear boundaries between advisory automation and autonomous control. The goal is not to slow innovation; it is to protect uptime, safety, and trust.

The Facility Manager Is the Only Role with Standing to Run This

Data centers that are AI enabled will require a more integrated work force model. Electrical, mechanical, IT, controls, cybersecurity, procurement, sustainability, and finance teams must work from both shared assumptions and data. Traditional lines of demarcation between facility operations and digital infrastructure are becoming less relevant because the performance of one directly impacts the other.

The AI-enabled data center requires a more integrated workforce model. Electrical, mechanical, IT, controls, cybersecurity, procurement, sustainability, and finance teams must work from shared assumptions and shared data. Traditional boundaries between facility operations and digital infrastructure are becoming less useful because the performance of one directly affects the other.

This is where the FM role becomes load-bearing. Critical capital programs fail at intersections — between people and systems, between facilities and process, between engineering judgment and enterprise governance, between the field crew and the executive dashboard, between the way a program was sold and the way it actually has to run on Tuesday morning. AI multiplies those intersections. Denser physical infrastructure, more interconnected digital systems, faster decision cycles, higher consequences when any of it goes wrong. Most organizations don't have a function whose job description includes the seams. The facility manager already does. They own the asset, they own the risk, they own the relationships across IT, engineering, vendors, operations, and the executive suite, and they are accountable when the building doesn't do what the business needs it to do. AI doesn't change that accountability. It raises the cost of exercising it without the right data, governance, and authority in place.

Looking outward from just the management of the actual data center and understanding that the modern data center has become a resource that impacts more than the business company requires industry leaders to look at different models of resourcing. Expanding the Facility Manager role, OR establishing a dedicated Community and Government Engagement function to coordinate environmental compliance, permitting, relationships with utilities, local and state agencies, emergency management, and surrounding communities will be essential. This function should proactively communicate sustainability initiatives, participate in resilience planning, monitor community concerns, support environmental justice objectives where applicable, and maintain the organization's social license to operate.

From the field. On a recent capital program supporting a critical infrastructure client, our team was brought in to govern a multi-vendor environment in which the building management system, the asset management system, and the operations work-order platform each described the same physical equipment differently. The chiller in the BMS was named one thing, tagged another way in the asset register, and ticketed against a third identifier in the CMMS. None of it was wrong. None of it was reconciled. When the program later attempted to introduce predictive analytics on that equipment, the model had no stable spine of identity to attach to. The fix was not technical — it was governance. A single source of asset truth, a single change-control protocol, a single accountable owner per system, and a weekly cross-functional review until the three systems agreed. This pattern, in our experience, is the single most common reason data centers struggle to operationalize AI. The technology is not the constraint. The discipline is. The lesson for AI-enabled data centers is direct: predictive tools are only as useful as the operating discipline beneath them. Before a model can forecast risk, the organization must first agree on what the asset is, who owns the data, which system is authoritative, and how corrections are governed over time.

The workforce challenge is readiness. Teams will need training in data literacy, AI-assisted decision-making, liquid cooling operations, controls integration, cybersecurity awareness, and sustainability metrics. Organizations should not assume that AI adoption will reduce the need for skilled labor. In many cases, it will increase the value of experienced operators who can interpret recommendations, recognize abnormal conditions, and make sound decisions under pressure.

The Logic AI Readiness Maturity Model for Data Center Facility Leaders

The maturity model should be presented as both a self-assessment tool and a business development bridge. It gives operators a simple way to locate their current state, identify the next defensible step, and recognize where Logic can support the governance, data reconciliation, decision-rights design, and operating routines required to move from fragmented readiness to strategic AI-enabled operations.

Most organizations approach AI readiness as a technology buying cycle. The result is software ahead of governance, dashboards ahead of decisions, and pilots ahead of operating discipline. The maturity model below is designed for facility leaders who want to take a different path: assess where their organization sits today, identify the next defensible level, and avoid jumping ahead of the foundation. Each level builds on the one before it. Skipping levels — deploying optimization models on top of a fragmented data environment, for example — is the most common cause of failed AI initiatives in mission-critical facilities.

Level	Stage	What Good Looks Like	Common Failure Mode
Level 1	**Foundational**	Asset inventory, criticality rankings, system drawings, maintenance history, sensor coverage, and capacity data are accurate, current, and reconciled across systems. A single source of asset truth exists.	Buying analytics tools before the underlying records are reliable. Models inherit the data's flaws and produce confident wrong answers.
Level 2	**Governed**	Data ownership, quality standards, integration rules, retention requirements, cybersecurity controls, and vendor access protocols are documented and enforced. Decision rights between FM, IT, engineering, and the executive suite are explicit.	Governance documents that exist on paper but not in operating routines. Charters without weekly review cadences are theater.
Level 3	**Targeted**	Two to four high-value AI use cases are deployed against named operational pain points (predictive maintenance for critical assets, cooling optimization, energy forecasting, alarm reduction). Each has a measurable baseline, a defined owner, and a kill criterion.	Pilot proliferation. A dozen demos that nobody owns, none of which moves a real operating metric.
Level 4	**Operationalized**	AI outputs are used in daily operations reviews, monthly performance meetings, risk reviews, capital planning, and sustainability reporting. Human-in-the-loop thresholds are defined: which recommendations are automated, which require operator approval, which require engineering review.	Treating AI recommendations as authoritative. The operator who can no longer overrule the model has lost the most important safety control in the room.
Level 5	**Strategic**	Operational intelligence informs portfolio-level decisions: capital	Scaling beyond what governance can support. New use cases

		sequencing, site selection, utility coordination, workforce planning, and ESG strategy. Avoided downtime, reduced energy intensity, and improved capital prioritization are tracked and reported to the executive level.	without new governance is how Level 5 collapses back to Level 2.

Conclusion: AI Will Not Replace Facility Management; It Will Redefine Its Strategic Value

AI is transforming data center management because it changes both the demand profile of the facility and the tools available to manage it. The physical environment must now support denser, hotter, more power-intensive, and more business-critical workloads. At the same time, AI gives facility leaders new ways to see, predict, optimize, and communicate operational performance.

The organizations that succeed will not be those that simply add AI tools to existing workflows. They will be those that modernize their management model: cleaner data, stronger governance, deeper collaboration between facilities and IT, more resilient energy and cooling strategies, and a workforce prepared to operate with both technical confidence and sound judgment.

For IFMA members and World Workplace attendees, the message is clear: AI is not only a technology issue. It is a facility management issue, an energy issue, a resilience issue, a workforce issue, and a leadership issue. The future of data center management will belong to facility leaders who can connect these dimensions and turn intelligence into disciplined, measurable operational performance.

Facility Management AI Use Case Matrix

Use Case	Primary Benefit	Data Required	FM Governance Question
Predictive maintenance	Reduced unplanned downtime	CMMS, sensor history, asset criticality	Who approves model-driven maintenance changes?
Cooling optimization	Lower energy use and improved thermal stability	BMS, DCIM, environmental sensors, workload data	What setpoint ranges are safe and approved?
Capacity planning	Better capital timing and rack deployment decisions	Power, cooling, floor loading, IT demand forecasts	How are assumptions validated before commitments?
Energy forecasting	Improved utility coordination and cost control	Utility tariffs, load history, weather, battery/generator data	Who owns energy market and demand response decisions?
Incident analytics	Faster root-cause identification	Alarms, tickets, event logs, operator notes	How are lessons learned captured and institutionalized?

FM Decision Authority Map: Who Owns What in an AI-Enabled Data Center

AI governance becomes operational only when decision rights are visible. This map is intended to help facility leaders move beyond general alignment and clarify who recommends, approves, is consulted, and is informed when AI-influenced insights affect cooling, maintenance, vendor access, incident response, capital planning, or cross-system integration.

R = Recommends • A = Approves • C = Consulted • I = Informed. Roles vary by organization; this map is a starting structure, not a prescription.

Decision	FM	IT/OT	Engineering	Vendor	Executive
Approve setpoint changes recommended by an AI cooling model	**A**	C	C	R	I
Defer or accelerate a model-flagged predictive maintenance action	**A**	I	C	R	I
Authorize a vendor to access operational platforms	C	**A**	I	I	I
Override an AI recommendation during an incident	**A**	I	C	I	I
Commit capital based on AI capacity forecasts	R	C	C	I	**A**
Approve cross-system data integration architecture	C	**A**	R	R	I

Recommendations for Facility Leaders

Implement an Environmental and Community Engagement Program Conduct recurring stakeholder meetings, environmental KPI dashboards, regulatory readiness reviews, and public facing sustainability reporting to strengthen trust whilst reducing permitting and compliance risk

Create an AI governance charter for critical facilities. Define data ownership, decision rights, cybersecurity controls, human approval thresholds, vendor responsibilities, and escalation paths before expanding AI-enabled automation.

Prioritize power and cooling readiness before software ambition. AI tools cannot compensate for inadequate infrastructure. Validate electrical capacity, redundancy, thermal performance, and cooling architecture against current and anticipated workloads.

Invest in the data foundation. Clean asset records, calibrated sensors, accurate one-line diagrams, current sequence-of-operations documents, and disciplined maintenance data are prerequisites for reliable AI outputs.

Upskill the operating team. Build literacy in data interpretation, AI recommendations, liquid cooling, controls, cybersecurity basics, and sustainability metrics.

Use AI to improve executive visibility. Translate operational performance into business language: risk reduction, avoided downtime, energy cost management, capacity enablement, and capital prioritization.

Sidebar: A 30/60/90-Day Plan for the FM Leader Starting on Monday

For facility leaders, AI readiness does not begin with a platform selection. It begins with a disciplined first 90 days: assess the systems and data foundation, govern the decision environment, and prove value through one measurable use case before expanding automation more broadly.

First 30 days — assess. Walk every operational system: BMS, EPMS, DCIM, CMMS, fire and life safety, access control, and any IT telemetry feeding facility decisions. For each, document the owner, the data refresh cadence, the integration points, and the most recent calibration date. Sit down with the IT leader who runs the OT side of the house and produce a one-page joint statement of what you each consider to be authoritative source data. If that statement reveals disagreements, you have found the work.

Days 31–60 — govern. Draft an AI governance charter covering data ownership, vendor access, model validation, human-in-the-loop thresholds, and incident escalation. Run it through one tabletop exercise — a simulated cooling anomaly during a peak load event — and watch where the charter fails to specify who decides. Fix those gaps before the charter is finalized. Establish a weekly cross-functional operating review (FM, IT, engineering, vendor liaisons) with a standing agenda no longer than four items.

Days 61–90 — demonstrate. Pick one use case — predictive maintenance on a single critical asset class, or alarm reduction on the loudest BMS subsystem — and run it for 30 days against a measurable baseline. Report the result to the executive level in business language: avoided callouts, alarm volume reduction, technician hours redirected. Use that conversation to secure mandate and budget for the next use case. The goal of the first 90 days is not to deploy AI broadly. It is to prove that the FM organization can be trusted to govern it.

References

[1] International Energy Agency. "Data centre electricity use surged in 2025, even with tightening bottlenecks driving a scramble for solutions." April 16, 2026. https://www.iea.org/news/data-centre-electricity-use-surged-in-2025-even-with-tightening-bottlenecks-driving-a-scramble-for-solutions

[2] Uptime Institute. "Global Data Center Survey Results 2025." 2025. https://uptimeinstitute.com/resources/research-and-reports/uptime-institute-global-data-center-survey-results-2025

[3] Uptime Institute. "AI Infrastructure Survey 2025." 2025. https://nextdc.com/hubfs/Uptime%20Institute%20AI%20Infrastructure%20Survey%202025.pdf

[4] International Energy Agency. "Energy and AI." 2025. https://www.iea.org/reports/energy-and-ai

[5] IFMA Knowledge Library. "The Future of Facility Management." March 25, 2025. https://knowledgelibrary.ifma.org/the-future-of-facility-management/

[6] IFMA IT Community. "Advancing Facilities Management with a Digital Thread – White Paper." March 3, 2025. https://it.ifma.org/advancing-facilities-management-with-a-digital-thread-white-paper/

[7] IFMA. "IFMA Publishes White Paper on Key Emerging Topics Shaping the FM Industry." September 27, 2023. https://www.ifma.org/news/whats-new-at-ifma-new/ifma-publishes-white-paper-on-key-emerging-topics-shaping-the-fm-industry/

[8] Data Center Dynamics. "Chilling out in 2025: A year in data center cooling." January 23, 2026. https://www.datacenterdynamics.com/en/analysis/chilling-out-in-2025-a-year-in-data-center-cooling/

[9] ASHRAE Technical Committee 9.9 (Mission Critical Facilities, Data Centers, Technology Spaces, and Electronic Equipment). *Thermal Guidelines for Data Processing Environments*, latest edition. American Society of Heating, Refrigerating and Air-Conditioning Engineers. https://tc0909.ashraetcs.org

[10] Lawrence Berkeley National Laboratory. "United States Data Center Energy Usage Report" and related research on data center power and water efficiency methodology. https://datacenters.lbl.gov

[11] National Institute of Standards and Technology. *NIST Special Publication 800-82, Revision 3: Guide to Operational Technology (OT) Security*. September 2023. https://csrc.nist.gov/pubs/sp/800/82/r3/final

About the Author

Ebony D. Wilson is a Senior Program Management and PMO leader at Logic, where she directs program governance and delivery on critical capital and operations engagements across the technology, utility, public-sector, and regulated-infrastructure markets. Her work concentrates on the places where program ambition meets operational reality: enterprise governance design, change management, cross-functional execution, and the translation of technology investment into measurable performance outcomes for the businesses that depend on it.

Ebony currently serves as Portfolio Lead on Logic's PMO Governance and Systems practice, where she is responsible for partnering with clients to design the governance structures, decision rights, and operating systems that hold their most critical programs together. Across her career she has supported program structures spanning utility infrastructure modernization, public-sector technology rollouts, regulated-environment compliance programs, and cross-functional PMO build-outs for organizations operating at the intersection of physical assets and digital systems. She brings to this paper a working perspective shaped less by theory than by what actually breaks when programs are under-governed: data lineage that doesn't survive a vendor change, escalation paths that fail at 2 a.m., and capital plans that lose their footing the moment a single forecast assumption proves wrong.

She wrote this paper for facility management leaders who are now expected to operate inside that same pressure — and who, in her experience, are uniquely positioned to lead it.

About Logic

Logic is a program and project management and project controls firm headquartered in San Diego, California. The firm specializes in embedded delivery on critical capital programs — the engagements where a single missed coordination step, a stale data point, or an unowned decision can cascade into eight-figure consequences. Logic's clients include investor-owned utilities, public agencies, and regulated infrastructure owners across California and the western United States.

What Logic does is straightforward to describe, and difficult to execute well: we operate at the intersections that most organizations don't have a function for. Between people and systems. Between facilities and process. Between engineering judgment and enterprise governance. Between the field crew and the executive dashboard. Between the way a program was sold and the way it actually has to run. These are the seams where critical capital programs most often fail, and they are precisely the seams that AI-enabled data center management is now multiplying — denser physical infrastructure, more interconnected digital systems, faster decision cycles, and higher stakes when any of it goes wrong.

That positioning is the basis for Logic's perspective in this paper. We are not a hyperscaler, not an OEM, not a software vendor with a product to defend. We are the firm that gets called when a critical environment needs the people, the data, the process, and the governance to behave as one operating system rather than four uncoordinated ones. That is the discipline facility management leaders are now being asked to extend into AI-enabled data centers, and it is the discipline this paper was written to support.

For more on Logic's program management, project controls, change management, and stakeholder engagement practices, visit www.logicco.com or contact Andrew Yoshimura, Founder and CEO, at andrew@logicco.com.