nuvolo

Asset Lifecycle Management in Data Centres

How to protect uptime, stay compliant, and extend the life of your critical infrastructure

Asset Lifecycle Management in Data Centres

How to protect uptime, stay compliant, and extend the life of your critical infrastructure.

Data centres (DCs) are the physical home of the digital economy, housing the critical infrastructure that powers the modern world. That role has made them one of the fastest-growing sectors in tech, underpinning everything from online banking and healthcare systems to streaming platforms and AI workloads. Without them, modern businesses and society would simply not function.

$300–$540 billion

The estimated current value of the global data centre industry

Source: Fortune Business Insights

In these environments, even a few minutes of unplanned downtime can carry financial, operational, legal, and reputational consequences that extend well beyond the data centre itself.

Every physical asset, from power distribution and cooling systems to servers, racks, and supporting infrastructure, plays a vital role in maintaining continuous operations. Yet while organisations invest heavily in resilient infrastructure, many still manage these critical assets using disconnected systems, manual processes, and incomplete records.

In this guide, we will explore the complete asset lifecycle within a data centre environment, sharing the best practices, processes, and industry standards that help operators maximise uptime and extend the value of their critical infrastructure.

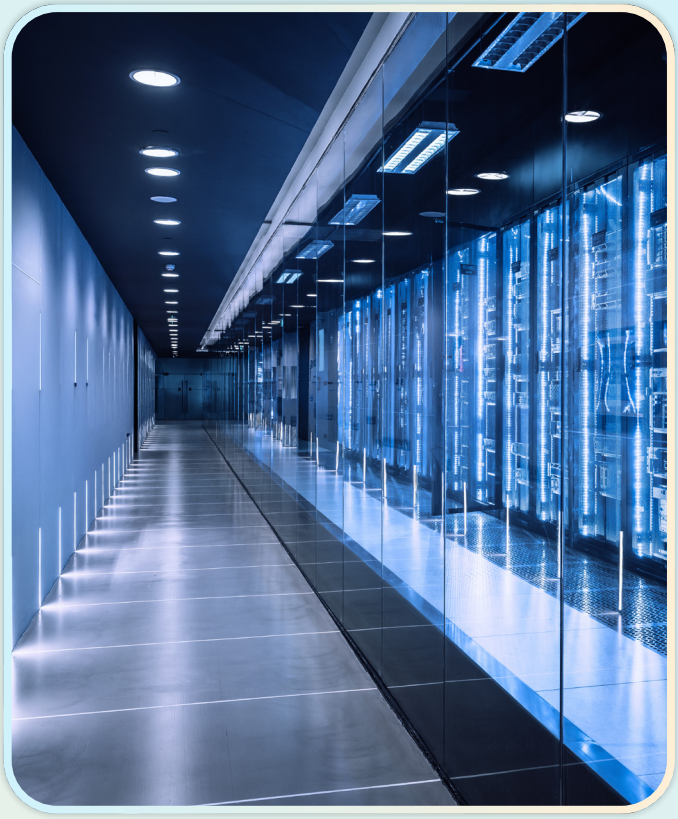
The Cost of Getting It Wrong

Data centres are designed to operate without interruption. They support the vital digital services that so many modern businesses depend on, which is why uptime here is non-negotiable.

Unlike many traditional facilities, data centres cannot pause operations while problems are resolved – so even the smallest outage can have a huge impact on essential services, leading to a breach in regulations, along with financial loss and damaged customer confidence.

What's more, in a competitive market where uptime can be a key differentiator, resilience has become both an operational and commercial priority for data centre providers.

However, despite so many organisations investing so heavily in resilient infrastructure, problems and outages do still occur. Understanding why they happen and the true impact they can have on the business is the first step towards reducing operational risk.



WHAT CAUSES DOWNTIME?

Data centres rely on a complex ecosystem of connected assets, including power distribution, uninterruptible power supplies (UPS) systems, generators, cooling systems, fire suppression, IT equipment, and more. Failure in any one of these areas can quickly affect the entire facility.

According to data from the Uptime Institute's 2025 Data Centre Resiliency Survey, the primary causes of data centre outages are:

Power system failures (54%) - UPS failures, generator failures, local grid instability, and electrical system faults (PDUs, transformers, breakers)

Cooling system failures (13%) – HVAC and chiller failures, poor cooling system design, and airflow obstructions can rapidly create unsafe operating conditions

IT and network failures (23%) – including IT systems (11%), such as hardware failures, software bugs, and database or virtualisation issues; and network problems (12%), such as router/switch failures, misconfigurations, and network congestion

Third-party provider issues (5%) – including colocation provider failures (3%) and other third-party issues (2%), such as telecommunications, CDN, or utility provider disruptions

Power and cooling failures alone account for two-thirds of outages, underscoring how much uptime depends on disciplined maintenance of physical assets throughout their lifecycle.

THE HIDDEN RISK: HUMAN ERROR

Infrastructure failures only tell part of the story: 40% of organisations have experienced a significant, serious, or severe outage caused by human error within the past three years. The leading contributors were staff failing to follow procedure (58%) and incorrect processes (45%) – both up sharply on the previous year – along with installation issues (24%) and maintenance frequency issues (16%).

The trouble is, data centres are becoming more complex, with operators having to manage more assets, dependencies, and operational data than ever before. Insufficient staffing – a factor in 18% of human error-related outages – often means teams can't keep pace with that complexity.

The result is clear: resilient infrastructure alone is no longer enough. Organisations also need complete visibility of their assets, controlled maintenance processes, and disciplined change management to reduce operational risk.

80%

of operators believe better management and processes would have prevented their most recent outage.

Source: Uptime Institute, Annual Outage Analysis Report 2025

THE TRUE COST OF DOWNTIME

The financial impact of downtime within a data centre continues to increase as organisations become more dependent on digital services. Research from the Uptime Institute found that **54%** of significant outages cost more than **$100,000** to remediate, while **20%** exceed **$1 million** in direct recovery costs.

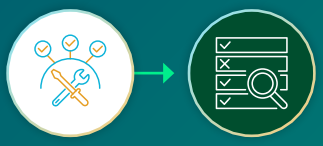
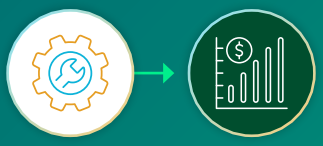
These figures only reflect the immediate cost of an incident. Its real impact is a business risk as much as a technical one, spreading into:

- **Breached Service Level Agreements (SLAs) resulting in financial penalties**
- **Contractual penalties**
- **Lost revenue**
- **Reduced customer confidence**
- **Damage to brand and reputation**
- **Delayed projects and operational disruption**

What Makes Data Centre Asset Management Different?

In a data centre environment, every piece of infrastructure – from electrical systems and cooling equipment to racks, servers, and network hardware – exists for one purpose: keeping digital services running.

This fundamentally changes what asset management is for. In most industries, it's about cost control and equipment durability. For DCs, it's about protecting the organisation's most valuable asset – uptime itself. That is why modern data centres are presented with such a unique set of challenges. Here we can see the key differences:

TRADITIONAL FACILITIES	VS	DATA CENTRES
Failures typically only disrupt the local facilities		Failure can impact business-critical services around the country or even around the globe
Downtime can often be scheduled for maintenance work		Downtime is unacceptable as customers expect continuous availability
The individual assets can be fixed or replaced as needed		In the highly connected infrastructure, failure in one component can quickly affect many others
Takes a maintenance focused approach, asking "how do we keep this asset efficient and cost-effective?"		Takes an availability focused approach, asking "how do we ensure this asset never compromises availability?"
Outages typically cause less operational impact		Outages will have a direct and costly impact on the business
Compliance is crucial but often easier to achieve		Operators must demonstrate compliance within a growing list of international industry standards

THE NEED FOR A SMARTER APPROACH

Many facilities and operations teams still rely on spreadsheets or basic work order systems to manage their assets. While these approaches may work in smaller companies, they struggle to support the scale and complexity of a modern data centre.

Some of the most common challenges of choosing traditional methods include duplicated asset information shared across multiple systems, greater risk of human error, and limited visibility into asset status. Left unresolved, these gaps create unnecessary operational risk – one that only grows as data centres increase in scale and complexity.

Addressing it depends on bringing together maintenance records, work orders, compliance documentation, condition monitoring, and lifecycle data in one connected system – not on infrastructure alone.

> *An Integrated Workplace Management System (IWMS) or Computerised Maintenance Management System (CMMS), deployed consistently across all sites, creates a single source of truth for asset data throughout its lifecycle.*

WHAT AN INTEGRATED SYSTEM DELIVERS

As data centres continue to grow in scale and complexity, integrated asset lifecycle management is becoming a critical operational requirement. Done well, it delivers real benefits for operators:

- **Improved operational visibility**
- **Reduced human error**
- **Predictive maintenance support**
- **Simplified compliance and audits**
- **Extended asset lifespan**
- **Better-informed investment decisions**
- **Protected uptime through proactive asset management**

The Compliance and Standards Landscape

By now, it's clear that effective asset lifecycle management is about far more than maintaining equipment. In modern data centres, it's also fundamental to meeting the growing range of industry standards, regulations, and customer expectations that govern this critical infrastructure.

Non-compliance can be costly, particularly around cooling systems. F-Gas regulations, which govern the refrigerants used in DC cooling infrastructure, are among the most strictly enforced compliance areas globally, with regulators in the EU, UK, and US all empowered to issue substantial fines for breaches.

But the risks extend well beyond fines – non-compliance also brings unplanned downtime, contractual breaches, and reputational damage.

This is why compliance matters so much in a DC context: it provides the governance, consistency, and traceability needed to operate critical infrastructure safely, minimise downtime, and reduce operational risk. Every critical asset must therefore be maintained, tested, and documented throughout its lifecycle – and demonstrating that maintenance has been carried out correctly is just as important as carrying it out in the first place.

THE STANDARDS CURRENTLY SHAPING DATA CENTRE OPERATIONS

Several industry frameworks currently influence how critical assets should be managed throughout their lifecycle, and these include:

SFG20 (UK) – This provides recognised Planned Preventative Maintenance (PPM) schedules and maintenance standards for building services, supporting statutory compliance and industry best practice. Though not a legal requirement internationally, this has become the industry standard

EN 50600 – The European standard defining best practice for the design, operation, and maintenance of data centres, with a strong focus on resilience, availability, and documented lifecycle management

Uptime Institute Tier Certification – A globally recognised certification that assesses the resilience and operational sustainability of data centre infrastructure through documented maintenance, testing, and change management

ISO/IEC 27001 – Requires organisations to maintain secure and controlled asset inventories, maintenance processes, and supporting documentation

ASHRAE Thermal Guidelines – Industry guidance for maintaining best practices in environmental monitoring and cooling performance to maintain safe operating conditions

F-Gas Regulations – Requires organisations to document refrigerant leak testing, servicing, repairs, and the management of cooling systems throughout their operational life

EPA – In the US, offers regulatory guidance on minimising environmental impact by promoting energy efficiency, controlling air emissions, and ensuring compliance with Clean Air Act permitting

Although each framework has a different focus, they all share one common requirement: that organisations maintain accurate, consistent, and auditable records that prove their critical infrastructure is managed safely and in accordance with industry standards.

An integrated asset lifecycle management platform brings this information together in one place, making compliance easier to demonstrate while reducing operational risk, improving governance, and helping protect continuous uptime.

Lifecycle Stages in Practice

Effective asset lifecycle management is about much more than just maintaining equipment when it fails. In a data centre, every stage of an asset's lifecycle must be carefully managed to maximise reliability, support compliance, and minimise the potentially costly risk of downtime.

From installation through to decommissioning, maintaining accurate records and making informed decisions ensures critical infrastructure continues to perform as it should.

1. ASSET REGISTRATION

OBJECTIVE	BEST PRACTICE	DATA CENTRE EXAMPLE	OUTCOME
Create a complete, accurate record of every asset from the moment it enters the facility.	Assign every asset a unique number or identifier for traceability and data integrity Record key information, including location, manufacturer, warranty, and maintenance schedules Store all supporting documentation in a centralised system	A new UPS is installed to support a white space expansion. It is assigned a unique asset ID and linked to its exact location, electrical one-line diagram, warranty, commissioning certificate, maintenance schedule, and spare parts list. Every future inspection, battery replacement, firmware update, and service visit is recorded against this single asset record.	A trusted, single source of information that supports maintenance planning, compliance, audits, and long-term lifecycle management.

2. PREVENTIVE VS. CONDITION-BASED MAINTENANCE

OBJECTIVE	BEST PRACTICE	DATA CENTRE EXAMPLE	OUTCOME
Maintain asset reliability while reducing the risk of unplanned failures and unnecessary maintenance.	Implement preventive maintenance based on manufacturer recommendations Complement scheduled maintenance with condition-based maintenance, using sensors, IoT devices, and monitoring systems to assess the real-time health of critical assets Use data to prioritise interventions, identify emerging issues early, and optimise maintenance schedules	A cooling pump is scheduled for quarterly preventive servicing. At the same time, vibration and temperature sensors continuously monitor its condition. An increase in vibration identifies bearing wear well before failure, allowing engineers to replace the component during a planned maintenance window rather than risk an unexpected outage.	A balanced maintenance strategy that combines planned maintenance with the intelligence of real-time monitoring. This can improve asset reliability, reduce unnecessary interventions, and help to prevent downtime.

3. PERFORMANCE MONITORING AND OPTIMISATION

OBJECTIVE	BEST PRACTICE	DATA CENTRE EXAMPLE	OUTCOME
Continuously assess asset performance to identify risks or maintenance needs before they become failures.	Use IoT sensors to monitor asset health, maintenance history, faults, energy consumption, and operating conditions Analyse trends to identify recurring issues and opportunities for further optimisation Use performance data to refine maintenance strategies and support compliance reporting	Monitoring data shows that one Computer Room Air Handler (CRAH) unit consistently consumes 20% more energy than identical units while delivering lower cooling performance. Maintenance teams discover deteriorating fan efficiency. Cleaning and replacing the worn component improves performance and reduces energy costs.	Greater operational visibility, improved asset performance, and better-informed maintenance decisions.

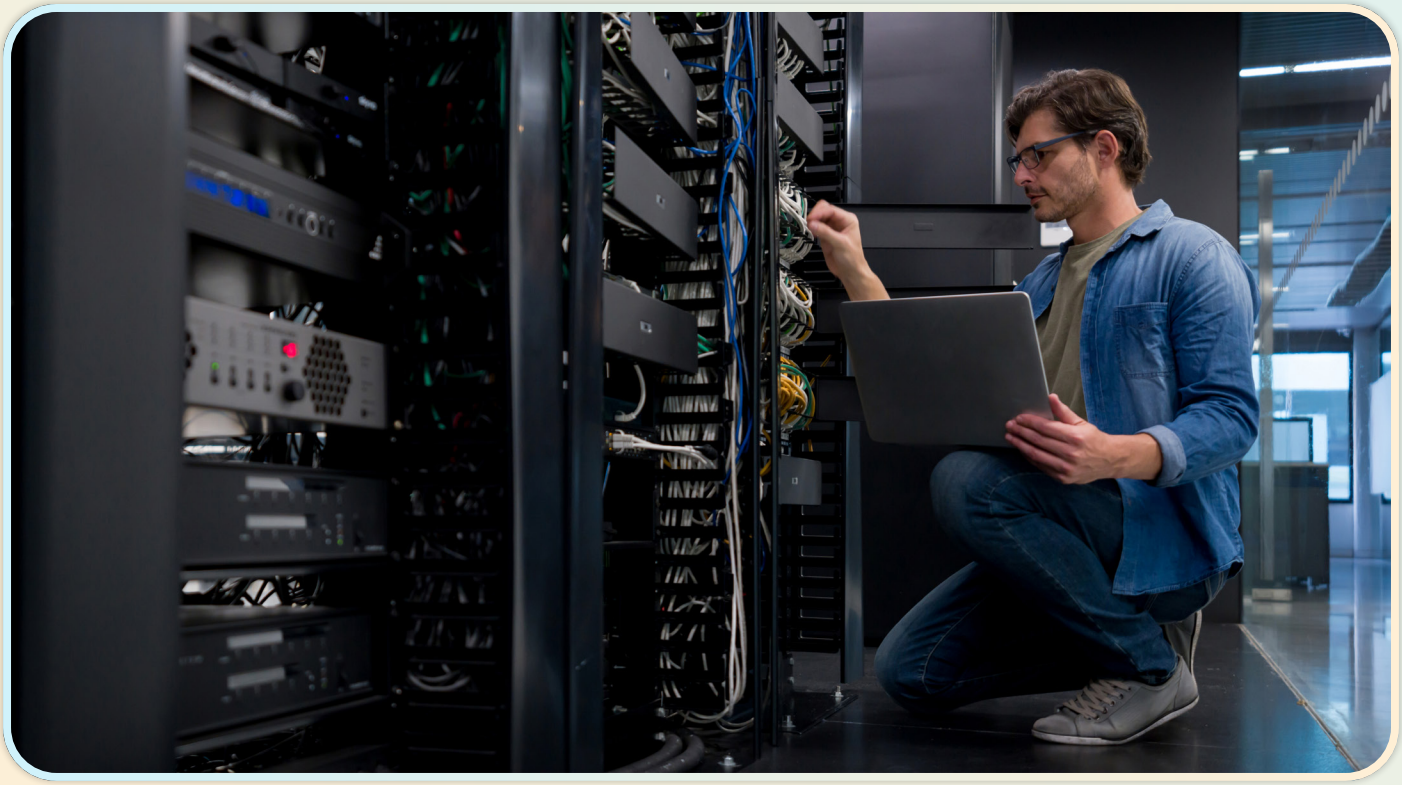
4. DECIDE WHETHER TO REPAIR OR REPLACE

OBJECTIVE	BEST PRACTICE	DATA CENTRE EXAMPLE	OUTCOME
Make informed decisions about whether to repair or replace key assets, balancing operational risk with lifecycle cost.	Continually assess asset condition, maintenance history, reliability, and operating efficiency Consider repair costs alongside energy performance and spare parts availability Use lifecycle data to support proactive replacement planning rather than waiting and reacting only when failures occur	A standby generator has experienced several fuel system failures over the past two years, and replacement parts have become increasingly difficult to source. Lifecycle analysis shows maintenance costs are rising while reliability is declining. Rather than risk failure during a utility outage, the operator schedules replacement during a planned capital investment programme.	Optimised investment, reduced operational risks, and improved resilience of long-term infrastructure.

5. DECOMMISSIONING AN ASSET

OBJECTIVE	BEST PRACTICE	DATA CENTRE EXAMPLE	OUTCOME
Retire assets safely, securely, and in full compliance with regulatory requirements when they are no longer safe, efficient, or cost-effective to operate.	Follow structured procedures for isolation, removal, disposal, or recycling Update asset registers, maintenance histories, and compliance documentation accordingly Ensure replacement assets can be onboarded quickly with minimal operational disruption	A legacy chiller is replaced with a more energy-efficient model. Before removal, engineers isolate all electrical and chilled water connections, archive its complete maintenance history, and record disposal certificates. The new asset is added to the CMMS, capturing the right details upfront, like equipment specs, location, and key attributes. This sets the foundation for everything that comes next: scheduled maintenance, warranty tracking, and long-term asset performance visibility.	A complete audit trail, reduced compliance risk, and a seamless transition to new assets when required.

Managing every stage of the asset lifecycle in one, centralised place gives organisations complete visibility of their critical infrastructure. By connecting asset data, maintenance activities, and operational performance, they can make smarter decisions that strengthen compliance and, ultimately, increase uptime.



How to Implement Asset Lifecycle Management in Data Centres

Implementing Asset Lifecycle Management in data centres requires a structured and strategic approach that aligns the physical infrastructure with maintenance standards and digital monitoring systems.

The objective is to establish a single, accurate source of truth for all assets while improving reliability, efficiency, and operational control. Here's how to successfully implement Asset Lifecycle Management in a data centre.

1. *Know What You Own*

The first step is to complete a comprehensive asset survey. This becomes a baseline of the environment that reflects infrastructure accurately, rather than relying on legacy documentation or outdated spreadsheets:

- A full physical and digital audit must be carried out to identify every asset on-site
- Note equipment type, manufacturer, model, serial number, installation date, and location
- Where possible, include condition assessments too

2. *Create a Single Source of Truth*

Once the survey is complete, all asset data should be consolidated into a centralised system that's consistently maintained across teams. A clean, centralised dataset becomes the foundation for all future lifecycle processes.

3. *Make SFG20 the Maintenance Baseline*

Next, facilities teams should implement SFG20 standards as a baseline for planned maintenance. These predefined maintenance schedules ensure no critical maintenance tasks are missed and that all assets are maintained consistently and in line with recognised best practices.

In data centre environments, this reduces variability between engineers, improves compliance, and strengthens predictability.

4. *Utilise Real-Time Insights*

The next step is to introduce IoT sensors to enhance visibility and monitoring. By tracking environmental and operational conditions such as temperature, humidity, vibration, and power consumption, IoT enables a shift from time-based maintenance to condition-based maintenance.

This improves fault detection, reduces unplanned downtime, and allows for earlier intervention before failures occur.

5. *Integrate with DCIM and ITSM Systems*

Your facilities management system should integrate with DCIM (Data Centre Infrastructure Management) and ITSM (IT Service Management) platforms to unlock further optimisation. For example, use smart workflows in a modern CMMS to auto-route work orders when an alarm is triggered in the infrastructure monitoring system.

- DCIM provides real-time infrastructure visibility, including capacity and performance data
- ITSM connects asset information to operational workflows such as incidents, changes, and service requests
- When fully integrated, these systems create a connected operational environment where asset performance, maintenance history, and service activity are all aligned

The end result is faster decision-making and improved operational resilience.

Conclusion: How Nuvolo Supports Asset Lifecycle Management in Data Centres

Asset Lifecycle Management in modern data centres depends on far more than better record-keeping. It requires connected systems, real-time visibility, and standardised processes that span IT, facilities, and operations.

Nuvolo's Connected Workplace, built on the ServiceNow platform, plays a critical role in unifying and enabling these capabilities.

MANAGE THE FULL ASSET LIFECYCLE IN ONE PLACE

As a single system of record for assets, maintenance, and workplace operations, Connected Workplace allows organisations to manage the full asset lifecycle within one platform, instead of relying on fragmented spreadsheets, disconnected CMDBs, or siloed maintenance tools. It also enables seamless workflow integration between IT and facilities teams, so asset data is no longer isolated from service management processes but linked directly to incidents, change requests, and work orders.

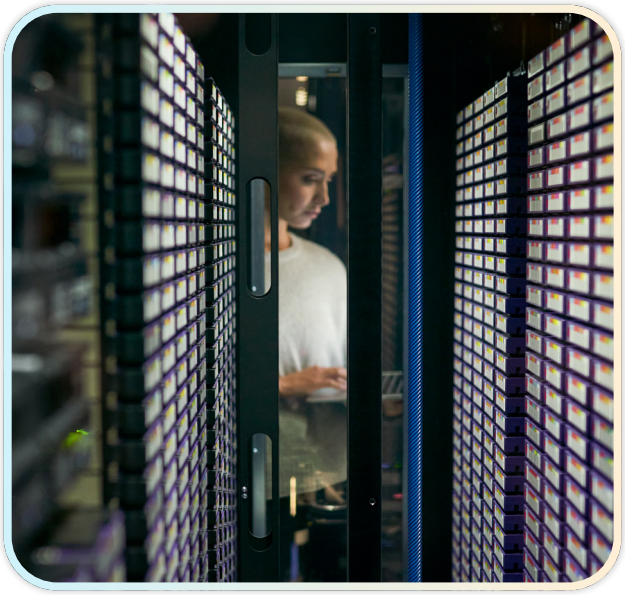
CENTRALISE MAINTENANCE PLANNING

Automation and proactive maintenance capabilities further enhance lifecycle management. Nuvolo's ability to centralise maintenance planning and execution supports predictive and condition-based maintenance, reducing the risk of costly downtime.

MAKE INFORMED LIFECYCLE DECISIONS

The platform also supports IoT and connected infrastructure monitoring, feeding real-time data from physical assets directly into lifecycle decisions.

Together, these capabilities make Nuvolo the operational backbone for Asset Lifecycle Management – connecting people, processes, and technology, and helping data centres move from fragmented, reactive operations to a fully integrated, data-driven model that improves reliability, efficiency, and long-term infrastructure resilience.



Want to know more about Nuvolo Connected Workplace?

VISIT NUVOLO.COM