

Where and how a data center operates

Site selection, risk analysis and reliable operations: the fundamentals that determine the real resilience of a critical facility



Introduction

A data center can have the best technical design on the market and still fail systematically if it is located in the wrong place or if its operations are not up to the standard of its infrastructure. Site location and the quality of operations are two variables that technical teams tend to take for granted, when in fact they are the ones that most often determine the real resilience of a critical facility.

This e-book addresses these two dimensions from an operational perspective. The first part analyzes the site selection criteria and the risk map that every professional should know before deciding where to build or where to host their systems. The second part covers the reliable operations model: the DC life cycle, the organizational structure, the procedures and the management tools that turn an infrastructure into a reliable operation.

What you will find in this e-book

IN THIS E-BOOK

The 8 key site selection factors

- A complete taxonomy of natural and human-made disasters
- How to read a risk index
- The DC life cycle and renewal windows
- The organizational structure of operations
- SOP, MOP and EOP: the three types of procedure
- ITIL, CMMS, DCIM and BAS: the management tools
- Minimum mandatory documentation
- Training program by profile

01 CHAPTER

Site location

The most permanent decision

Of all the decisions made over the life cycle of a data center, choosing its location is probably the hardest to reverse. A cooling system can be modernized and a UPS can be replaced, but changing the physical location of a data center is so complex that, in practice, it is the same as building a new one.

That is why site analysis must be thorough, systematic and documented before any investment decision is made. There are eight main factors to evaluate.

1.1 The eight site selection factors

Factor	What to evaluate	Risk if ignored
Access to electrical power	Supplier reliability, circuit redundancy and independent feed routes from different substations	Dependence on a single source; no fallback in the event of a prolonged outage
Access to telecommunications	Availability of multiple carriers and diverse physical fiber routes	Single point of failure in connectivity; no alternative if the fiber is cut
Adjacent properties	Industrial, military, chemical or high-risk facilities in the immediate surroundings	Exposure to fires, explosions or contamination from external sources

Factor	What to evaluate	Risk if ignored
Seismic and ground stability	Soil type, historical seismic activity, proximity to geological faults	Structural damage from earthquakes; collapse of the building infrastructure
Floodplain	Flood history, ground elevation, proximity to rivers or the coast	Catastrophic flooding with no possibility of an operational response
Air quality	Concentration of particles, industrial gases, nearby volcanic or urban activity	Accelerated contamination of hardware; premature corrosion of circuits
Access to water	Availability for cooling systems (chillers, towers) and fire suppression	Limits on cooling technologies; risk in the event of fire
Access to transport	At least two independent access routes from a main road	Personnel or equipment unable to reach the site in an emergency

■ 1.2 Access to power: the most critical factor

Of the eight factors, access to quality electrical power is the one that most determines the viability of the project. The evaluation must go beyond confirming that there is power supply in the area: it must analyze the supplier’s historical reliability, the possibility of feeding the site from two different substations through physically separate routes, and the availability of medium or high voltage to reduce dependence on intermediate transformations.

KEY

Power supply redundancy

Best practice is to have two power feeds from different electrical substations, with completely separate physical routes (including different underground conduits). A site fed from two points of the same substation has no real redundancy: a failure at the substation affects both feeds at the same time.

2

Key takeaway

separate substations, with separate physical routes: the only way to achieve real power redundancy.

02 CHAPTER

The risk map

Know in order to anticipate

Site selection cannot be done without a systematic analysis of the risks associated with the location. These risks fall into two broad categories: natural disasters and human-made (anthropogenic) disasters, caused by human activity. Both categories can act independently or in a chain, and both have the potential to permanently compromise the operation of a data center.

■ 2.1 Taxonomy of natural disasters

Category	Types	Typical impact on a DC
Geological disasters	Earthquakes, volcanic eruptions, landslides	Structural damage to the building, service outages, contamination from volcanic ash
Hydrological disasters	Floods, tsunamis, limnic eruptions	Flooding of facilities, loss of access, irreversible equipment damage
Climatic disasters	Hurricanes, tornadoes, heat waves, droughts, severe storms	Prolonged power outages, physical damage to the building, cooling system failure
Natural fires	Wildfires, lightning strikes	Structural damage, smoke contamination, loss of access
Space weather	Solar geomagnetic storms	Electromagnetic interference, damage to unprotected electrical systems

■ 2.2 Human-made disasters: the threat that is built nearby

Human-made disasters are especially relevant because many of them can be identified and avoided during the site selection phase. A data center located next to an industrial chemical plant, in an airport’s approach path or less than 100 meters from a highway with heavy dangerous-goods traffic is taking on risks that no internal redundancy system can offset.

Human-made hazards fall into two groups:

- **Sociological hazards:** terrorism, organized crime, civil unrest, armed conflict. They determine the physical security requirements and the site’s level of public exposure.
- **Technological hazards:** high-risk industrial facilities, military bases, storage of hazardous materials, transport routes for flammable or explosive substances, proximity to runways.

The risk of adjacencies

WARNING

A real case documented in the manual shows a data center with multiple simultaneous risks within a small radius: a highway less than 100 meters away, a high-risk industrial zone, a runway approach path and an air force base’s munitions storage. None of these risks is visible in a purely technical analysis of the building. Only a geographic and adjacency analysis reveals them.

■ 2.3 Risk indices as a decision-making tool

There are public risk indices that systematically quantify each territory’s exposure to natural and human-made disasters. The INFORM index (Index for Risk Management), developed by the UN and the European Union, is one of the most comprehensive and is publicly available.

These indices make it possible to compare potential locations objectively and to document the site decision with traceable criteria. For a mission-critical data center, consulting risk indices is not optional: it is part of the project’s due diligence process.

Natural disasters trigger each other

KEY

An often underestimated feature of natural disasters is that they can occur in a chain: an earthquake can trigger a tsunami; a drought can cause wildfires which, in turn, degrade air quality. Risk analysis must consider these compound scenarios, not just individual events.

<100 m

Key takeaway

from a highway carrying dangerous goods: a risk that no internal redundancy can offset.

03 CHAPTER

The data center life cycle

Plan for decades, renew every few years

A strategic data center is designed to operate for 20 to 30 years. Over that period, cabling systems last 15 to 25 years, but servers and storage systems are renewed every 3 to 5 years. This asymmetry is key to understanding how a data center should be managed over time.

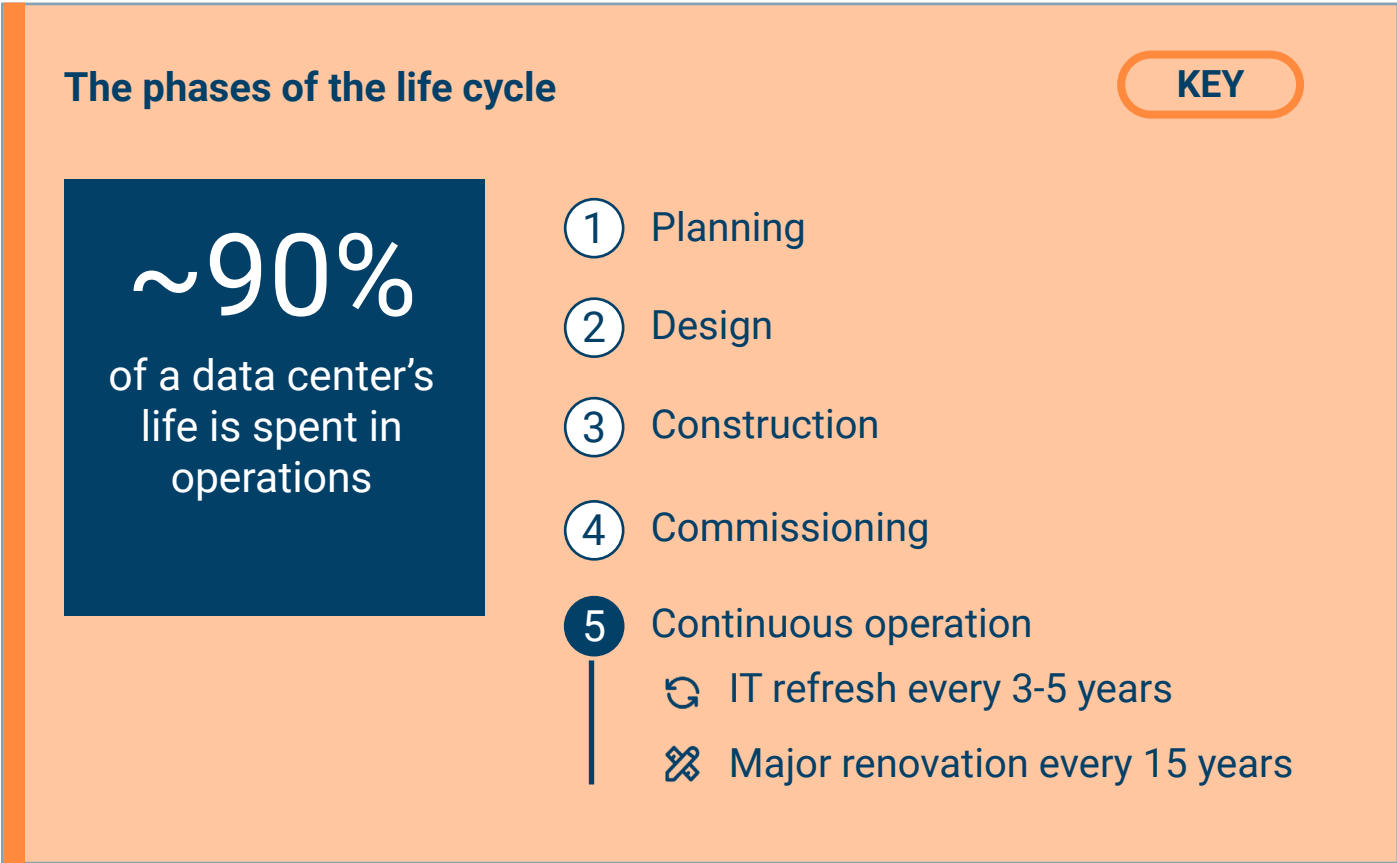
3.1 Service life by infrastructure layer

Layer	Typical service life	Operational implication
Strategic data center (building and infrastructure)	20 – 30 years	Design decisions have an impact lasting decades. Site or capacity errors are very costly to correct
Structured cabling system	15 – 25 years	It must be planned to support multiple generations of IT equipment. Cabling capacity must anticipate future densities
Servers and storage systems	3 – 5 years	The IT refresh cycle is continuous. The infrastructure must be able to absorb changes in density and configuration without major works
Desktop PCs	3 – 5 years	Limited direct impact on the DC infrastructure
Laptops	2 – 3 years	Limited direct impact on the DC infrastructure

■ 3.2 The 5-year renewal cycle

Roughly every 5 years, a well-managed data center should go through a review and renewal cycle that can range from upgrading IT equipment to replacing infrastructure systems (UPS, CRAC/CRAH, switchgear). Roughly every 15 years, a major renovation may be needed, involving significant system replacements and possibly an upgrade of the architecture.

This life cycle has a direct impact on budget planning: a data center without a documented renewal plan is building up technical debt that will at some point materialize as a failure or as obsolescence that compromises its ability to scale.



04 CHAPTER

Reliable operations

The triangle that sustains availability

Data center operations rest on three interdependent pillars: people, procedures and documentation. Management integrates and oversees these three elements. None of them can make up for shortcomings in the other two: an excellent team without procedures produces inconsistencies; perfect procedures without trained staff are worth nothing.

■ 4.1 Organizational structure of operations

Data center operations are organized into two main branches under the direction of IT Operations:

Branch	Function	Sub-areas
Facility Management	Management of the DC's physical infrastructure	Engineering (building, electrical, mechanical) + Maintenance (building, electrical, mechanical)
IT Management	Management of information and telecommunications systems	IT Infrastructure (Telco/Networking, Computing/Storage, Disaster Recovery) + Technical Support (Call Center)

In addition, there are support functions that sit outside the direct chain of command but are essential to operations: the CISO (responsible for cybersecurity), the Physical Security team and the Health & Safety team. These functions must be formally integrated into operational processes, not treated as independent entities.

■ **4.2 The three types of procedure: SOP, MOP and EOP**

One of the most important concepts in data center operations management is the distinction between the three types of procedures. Confusing them or using them interchangeably is one of the most common mistakes in operations teams without formal training.

Type	Full name	Purpose	When it is used
SOP	Standard Operating Procedure	Defines a recurring routine and critical processes. It can be functional or administrative	Routine operations: inspection rounds, opening/closing the room, equipment receipt, visitor management
MOP	Method of Procedure	Detailed step-by-step procedure for a specific intervention. More detailed than an SOP	Planned technical interventions: UPS replacement, CRAC maintenance, changes to the electrical configuration
EOP	Emergency Operating Procedure	Procedure for a potential or known failure mode	Emergencies: UPS failure, fire suppression system activation, unplanned power outage, EPO activation

An EOP that is not practiced does not work

An EOP is useless if staff have not practiced it before the emergency happens. EOPs must include periodic drills with the entire operations team, including scenarios such as UPS failure, fire in the room and accidental EPO activation. The recommended frequency is at least once a year per scenario.

■ **4.3 Operations management tools**

Modern data center operations require specific tools to manage the procedure workflow, asset tracking and control of infrastructure systems. There are four main categories:

Tool	Full name	Main function
ITIL	Information Technology Infrastructure Library	Best-practice framework for asset change management, service level and logging incidents with their causes and consequences
CMMS	Computerized Maintenance Management System	Scheduling, assignment and tracking of all facility maintenance activities. Calculates maintenance management KPIs (MTBF, MTTR)
DCIM	Data Center Infrastructure Management	Maximizes the efficient use of power, cooling and space capacity. Provides real-time visibility of the entire DC infrastructure

Tool	Full name	Main function
BAS	Building Automation System	Software for automated control of building systems (HVAC, lighting, access, security)
DMS	Document Management System	Storage, retrieval and approval workflow for all DC documentation

DCIM: the tool that sees everything

KEY

DCIM is the tool with the greatest operational impact in a modern data center. It brings together power, cooling, space and asset data in a single platform, enabling informed decisions on capacity, efficiency and planning. A DC without DCIM operates partly blind: it can manage systems individually, but it has no visibility of how the infrastructure behaves as a whole.



Key takeaway
drill a year, at least, for each emergency scenario.

05 CHAPTER

Documentation and training

The DC’s institutional memory

Data center documentation is not a bureaucratic requirement: it is the institutional memory that makes operations consistent, auditable and transferable. A data center that operates without up-to-date documentation is permanently at risk of critical knowledge residing only in people, not in systems.

5.1 Minimum mandatory documentation

A data center’s documentation system must keep an up-to-date record of the following:

- **As-built drawings:** updated plans that reflect the actual state of the facility, not the original design.
- **Asset database:** a complete inventory of all equipment with its technical specifications, installation dates and warranties.
- **Scope of preventive maintenance work:** a detailed description of all planned maintenance tasks.
- **Maintenance schedule:** a calendar of all preventive interventions with assigned owners.
- **Rules for working in critical facilities:** safety rules and specific procedures for working in energized or high-availability environments.

- **Security program:** physical security and cybersecurity policies and procedures.
- **Commissioning checklist:** a start-up checklist for each system.
- **Procedures and processes:** a complete library of SOPs, MOPs and EOPs.
- **Reports:** historical records of incidents, maintenance and audits.

The most dangerous document

WARNING

An outdated as-built drawing is one of the most dangerous documents in a data center. When staff work on a system based on a drawing that does not reflect reality, the risk of error is at its highest. Keeping as-built drawings updated after every change is not optional: it is an operational obligation.

■ **5.2 Training program by profile**

Staff training must be differentiated according to each role’s profile and responsibilities. The manual distinguishes two main levels:

Profile	Training content
Field technicians and engineers	• Fundamentals and best practices • Operating theory of the main equipment and systems • Training modules for SOPs and MOPs • Drills for EOPs • Exams by training level
Managers and supervisors (in addition)	• Data Center Management • Data Center Energy Efficiency • Data Center Operations • Data Center Design Awareness • Continuous training and attendance at industry conferences

Training is not a one-off event at onboarding: it is an ongoing process. Changes to the infrastructure, new systems, regulatory updates and lessons learned from incidents must all be reflected in updates to the training programs.

Conclusion

Resilience starts before the first rack is installed

A resilient data center is not built with redundant technology alone. It is built by choosing the right location, understanding the risks of its surroundings, establishing structured operations and documenting every decision. These are the disciplines that technical teams most often underestimate, and the ones that most often determine the actual outcome.

Site location is permanent. Operations are continuous. Documentation is cumulative. None of the three can be improvised in the middle of an emergency: they must be in place long before any unplanned event occurs.

KEY

The five principles of a well-located, well-operated DC

1. Site selection requires an analysis of eight physical factors and a map of natural and human-made risks. A location with multiple simultaneous risks cannot be offset by internal redundancy.
2. Natural disasters trigger each other. Risk analysis must consider compound scenarios, not just individual events.
3. SOP, MOP and EOP are three different documents with different purposes. Confusing them is an operational risk.
4. An EOP that is not practiced does not work. Drills are mandatory, not optional.
5. Outdated as-built drawings are as dangerous as a system without redundancy. Documentation must reflect the actual state, not the original design.