

Data Center Regulations

The codes, standards, and regulations that govern a data center — and the certifications, process documentation, audits, industry guidelines, and best practices that prove and sustain compliance

A data center houses the computer systems and equipment an organization uses to store, process, and disseminate data — systems critical to daily business continuity and full of information that is often private. Because so much rides on them, codes, standards, and regulations are an integral part of a data center's operational process: they raise operational capability while protecting safety and security, and non-compliance can cost a data center millions of dollars a year and expose it to other threats and risks. This module works through the whole compliance landscape — first the three easily confused terms (codes, standards, and regulations) and the areas they govern, then the actual codes (NFPA, OSHA, EPA), the design and operational standards (ANSI/BICSI 002, ANSI/TIA 942-A, EN 50600, the Uptime Institute Tier Standard, and the ISO family), and the certifications a data center should hold. It covers the day-to-day facility regulations, the 12-step process-documentation procedure, and the audits that keep everything honest. Lesson 2 then reframes the same territory as industry guidelines organized into four focus areas and closes with the best practices a well-run data center follows. Unless otherwise noted, the guidelines and best practices here are relevant to data centers in the United States.

LEARNING OBJECTIVES

- Recognize the codes and regulations applicable in a data center
- Recognize the key considerations of process documentation and audits in data centers
- Identify common industry guidelines for data centers
- Identify common best practices for data centers

18.1 Codes, standards, and regulations

Codes, standards, and regulations are an integral part of a data center's operational process. The three words are used loosely in conversation but mean different things. *Codes* are regulations, enforced often by a group of governmental entities, that evolve industry best practices. *Standards* ensure that organizations adhere to accepted professional practices — including construction techniques, maintenance of equipment, personnel and data safety, and documentation. *Regulations* are government-defined practices that protect the public and enforce certain ethical standards for professionals to follow. For example, the **International Standards Organization (ISO)** issued the standard guideline **ISO 9000**, which lists guidelines for building quality systems in an organization.

KEY TERMS

Code

A regulation, enforced often by governmental entities, that evolves industry best practices.

Standard

Ensures organizations adhere to accepted professional practices — construction, equipment maintenance, personnel and data safety, and documentation.

Regulation

A government-defined practice that protects the public and enforces ethical standards for professionals.

Compliance is not optional. Without it, a data center might lose millions of dollars a year and open itself to other kinds of threats and risks. And although these codes and regulations guide better operational capabilities with safety and security, it can sometimes be genuinely challenging to comply. Appropriate codes and standards must be followed precisely when designing a new data center or advancing an existing one.

AREAS OF A DATA CENTER GOVERNED BY CODES

- Conceptual design and space planning
- Building construction
- Physical security and data security
- Mechanical, electrical, and plumbing (MEP)
- Fire protection
- Facility operations
- Maintenance and procedures

COMMON PITFALL

Codes, standards, and regulations are not interchangeable. On the exam, watch the source of authority: codes are enforced by governmental entities to evolve best practices, standards define accepted professional practice, and regulations are government-defined rules to protect the public. Confusing the three is a common distractor.

18.2 Codes for a data center

Codes for a data center's design and organization can vary from **nationwide codes to resident (local) codes**, and the organization determines which codes its data center follows. A data center may need to abide by fire codes, construction codes, energy codes, health codes, and more. These compliance codes and regulations are carefully framed to provide better operational capabilities while taking care of the various aspects of a data center, and they should be adhered to and implemented with proper consultation.

TABLE 18.1 Common codes and the agencies behind them

CODE / AGENCY	WHAT IT DOES
NFPA — National Fire Protection Association	International nonprofit devoted to eliminating death, injury, and property/economic loss due to fire, electrical, and related hazards
ECCCNYS — Energy Conservation Construction Code of New York State	Protects public health, safety, welfare, and the environment by setting minimum standards for the design, construction, and occupancy of buildings in New York
Building energy code	Sets minimum energy-efficiency requirements for new and renovated buildings, reducing energy use and emissions over the building's life; the IECC and ANSI/ASHRAE/IES Standard 90.1 are the referenced model standards
OSHA — Occupational Safety and Health Administration	Maintains health industry standards and sets legal requirements for employers to ensure a safe working environment; provides training, outreach, education, and assistance
EPA — Environmental Protection Agency	Develops and enforces environmental regulations and governs emission standards to reduce environmental risks and protect human health

The engineering-operations takeaway: the applicable set is chosen deliberately — from nationwide down to local — and then implemented precisely, with consultation, from the earliest design phase onward.

18.3 Standards for a data center

A high-quality data center provides a higher level of protection, mitigates various risks, and ensures better uptime while abiding by the law. **Data center design and infrastructure standards** provide guidelines, best practices, and recommendations that are applicable across all types of data centers — and here again, **full compliance instead of minimum compliance is important**.

TABLE 18.2 Design and infrastructure standards

STANDARD	WHAT IT REVOLVES AROUND
ANSI/BICSI 002-2014	Implementation and best practices for all phases of planning, designing, constructing, and authorizing a data center — plus maintenance, fire protection, and security norms
ANSI/TIA 942-A 2014	The telecommunications infrastructure standard designed for data centers: cabling and networking, electrical layout, mechanical devices and parts, and architectural system
EN 50600	The first European-wide, transnational standard giving comprehensive specifications for planning, construction, and operation of a data center — construction, power supply, air conditioning, cabling, and security systems
Uptime Institute (UI) Tier Standard	Globally recognized standard for reliability and performance, allowing different performance levels across a data center's layers. Note: AWS does not use the UI to certify data centers

EN 50600 is a series of standards, not a single document. Each part addresses a specific concern, from general features to environmental impact to security monitoring.

TABLE 18.3 The EN 50600 series

STANDARD	COVERS
EN 50600-1	All the general features
EN 50600-2-1	The data center's design and construction
EN 50600-2-2	The rules for power distribution layout
EN 50600-2-3	The data center's impact on the nearby environment
EN 50600-2-4	The various aspects of telecommunication cables and layout
EN 50600-2-5	The required security for data center monitoring
EN 50600-2-6	Overall management information systems, with added operational parameters

When a data center becomes ready for operations, **operational standards** apply — the guidelines that define the rules of conduct for routine processes in a fully functioning facility. Standard operating procedures (SOPs) put them into practice.

OPERATIONAL STANDARDS

- **ISO 9000** — international standards on quality management and quality assurance; helps companies document the elements needed for an efficient quality system.
- **ISO 14000** — a family of standards for environmental management; helps organizations minimize environmental impact, comply with laws, and continually improve.
- **ISO 27001** — an international standard on how to manage information security.
- **PCI DSS** — security standards that secure credit and debit card transactions against theft and fraud and safeguard cardholders' sensitive data.

COMMON PITFALL

The Uptime Institute Tier Standard is real and globally recognized, but AWS does not use it to certify its data centers — a fact the module calls out explicitly. And these operational standards apply according to the type of business domain and its operations; they are not a one-size-fits-all checklist.

18.4 Certifications and attestations

Beyond codes and standards, there are several **certificates and attestations a data center should hold**. Complying with data-security and integrity requirements makes a data center more reliable and more loyal to its customers, and remaining transparent — providing proof of security and transparency — lends support to a data center's quality.

TABLE 18.4 Certifications and attestations to know

CERTIFICATION	WHAT IT CHECKS
SSAE 18 — now called ISAE 3402	For service organizations; ensures that a company is honest in its financial reporting
SOC 2 Type II	Inspects the policies and procedures for data security, availability, integrity, privacy, and confidentiality
ISO/IEC 27001:2013	A risk assessment and management process that checks an organization for vulnerabilities and risks and provides guided training for information security
PCI DSS 3.2	Created to manage and secure financial data and keep privacy/security checks on credit card payments; mandatory if a card is processed by a company or vendor
LEED and ENERGY STAR	Eco-friendly green building certifications; many states require some level of LEED, Green Globes, ENERGY STAR, ASHRAE 90.1, or IECC energy codes, but green certifications are optional for a data center

COMMON PITFALL

Do not treat every certification as mandatory. Green certifications such as LEED and ENERGY STAR are considered optional for a data center, whereas PCI DSS is mandatory whenever a card is processed. Confusing optional with mandatory is a classic knowledge-check trap.

18.5 Facility regulations for daily operations

Many of the codes and standards, in turn, list specific **regulations that data centers must follow in their day-to-day operations**. These fall into four groups: security, safety and evacuation, receiving new equipment, and building rules and regulations.

TABLE 18.5 Sample day-to-day data center regulations

AREA	REPRESENTATIVE REGULATIONS
Security	Single point of entrance at the main security desk; check-in/check-out logging for every visit; access denied to unauthorized persons; alarms on doors held or forced open; all personnel consent to be monitored and recorded
Safety and evacuation	On emergency horns and strobes, evacuate in an orderly fashion and wait at a designated area until all are accounted for against the access list; no re-entry until the event leader permits; fire-safety and response training with drills at roughly 6-month intervals
Receiving new equipment	All equipment enters and leaves through a receiving department that checks, verifies, and records it, with a goods-in/out log; no cardboard, plastic wrap, or flammable materials permitted into the data hall
Building rules	Work under the raised floor is approved and supervised by facility management; non-smoking facility; food and drink confined to authorized areas; weapons and alcohol strictly prohibited; report any violation or improper activity

COMMON PITFALL

Personal electronic devices are tightly restricted. Batteries holding acid are not allowed anywhere on the data center floor, and mobile phones are not permitted in critical areas such as the data hall because they are a security risk — even though maintenance items like screwdrivers, cables, testing equipment, cameras, and two-way radios may be brought in when they are integral to the work.

18.6 Process documentation, certificates, and audits

With a large number of standards and codes to follow, adopting a **process to document how codes are maintained** helps a data center comply accurately. A step-by-step documentation procedure organizes people and processes for consistency, performance, overall quality, and process automation.

TABLE 18.6 The 12-step process-documentation procedure

STEP	FOCUS
1. Recognize and title the process	Identify each process to document, with its purpose and a brief description
2. Interpret the scope	State crisply what is included and excluded
3. Elaborate on process limits	Define the starting and ending points, the initiator, and how completion is identified
4. Ascertain the process output	Identify the result the process achieves at successful completion
5. Ascertain the process input	List the resources required to perform each step
6. Analyze the process steps	Brainstorm the full flow start to end, including the people who perform it
7. Use a sequential approach	Log the steps in order for a well-formed process flow
8. Explain who is required	Assign roles and responsibilities by job title rather than by name
9. Use a visual approach	Provide a flowchart for a clear understanding of all steps
10. Note exceptions	Record variations from the normal flow and the steps they require
11. Include control points	Point out risk areas and add monitoring and improvement measures
12. Evaluate and test the process	Review with everyone involved and test for efficiency and glitches

A data center must **earn certificates for compliance from the planning and design phase onward**, and this is where a common point of confusion arises. International and national certified organizations are authorized to help data centers comply with the codes and standards set by various compliance bodies; they act as **mediators** between the compliance body and the data center, working closely with the facility to understand its infrastructure and obtain the required legal code certificates.

WHO ACTUALLY ISSUES THE CERTIFICATE

A data center is not a certifying body. It only receives a certificate to demonstrate compliance. The consulting organization — the mediator — is the certified body that knows all the codes and has been certified by a specific board to conduct audits. In short: an accredited organization issues the data center a certificate of compliance after every compliance audit.

CODE-MAINTENANCE AUDITS

- An integral part of any system, ensuring safety and efficiency through compliance with different codes and standards.
- Conducted on a **regular basis** to avoid risks, by a dedicated team of **3 to 5 people from each department**.
- Impartiality is ensured by not allowing people from the same department to conduct the audit on themselves.
- The audit team inspects all the safety equipment and program material.
- The objective is to keep a check on safety, the health of employees, and fire hazards.

ON-SITE (WORKPLACE) SAFETY AUDITS

- Aim at inspecting compliance with **OSHA** standards — ergonomics, personal protective equipment, blood infections, hearing, and use of respirators.
- Ensure a good working environment with the sound health of individuals in the workplace.
- Conducted more often than other inspections — every week or every month — so the workplace is always ready for a random or scheduled annual audit.
- Guided by four questions: Does the program include all regulations and industry practices? Are all program requirements in place? Is there documented proof of all compliances? Are employees well-trained to ensure safety?

COMMON PITFALL

The recurring exam point: the data center is never the certifier, and an audit team never audits its own department. An accredited third-party organization issues the certificate of compliance after each audit, and impartial 3-to-5-person teams drawn from outside the audited department run the code-maintenance audits.

18.7 Industry guidelines by focus area

Lesson 2 reframes the same compliance territory as **industry guidelines** a data center should follow to ensure security, business continuity, and regulatory compliance. Industry guidelines related to data center design fall into four focus areas: **information security, physical design and operation, audits, and service management**. Information security relates to protecting data of all types; physical design and operation covers construction, safety, and environmental requirements; audits cover auditing, reporting, and assurance processes; and service management focuses on the systems that ensure high-quality service.

TABLE 18.7 Industry guidelines mapped to focus areas

FOCUS AREA	GUIDELINE	WHAT IT DOES
Information security	HIPAA	Protects individually identifiable health information; HIPAA-compliant data centers comply with third-party audits, secure network connections and the physical location, and prioritize cybersecurity
Information security	ISO/IEC 27001	Requires a comprehensive information security management plan with security risk identification, assessment, and mitigation processes
Information security	PCI DSS	Increases the security of payment cards and cardholder data; covers payment application data security, encryption, secure software, and use of PINs
Physical design & operation	ANSI/BICSI 002-2014	Sets standards for planning, designing, constructing, and authorizing data centers, plus maintenance, fire protection, and security norms
Physical design & operation	ANSI/TIA 942-A 2014	Guidelines on telecommunications infrastructure, site location, architectural/physical structure, electrical and mechanical infrastructure, fire safety, and physical security
Physical design & operation	ISO 14000	Sets criteria for environmental performance by establishing guidelines for an environmental management system
Audits	SAS 70	Provides guidelines for independent audits, including auditing controls over information technology and related processes
Audits	SSAE 18	Enhances the usefulness and quality of service organization control (SOC) reports; sets requirements for how auditors and staff collaborate — risk assessments, regular review, mitigation, and preventive action
Audits	ISAE 3402	Sets standards related to SOC reports that outline an organization's internal controls
Service management	ISO 9000	Sets criteria for quality by establishing guidelines for a quality management system
Service management	ISO 20000-1	Specifies requirements for establishing, implementing, maintaining, and improving a service management system

COMMON PITFALL

Sorting questions turn on the focus area. Remember the pairings: information security (HIPAA, ISO/IEC 27001), physical design and operation (ISO 14000, ANSI/BICSI 002-2014), audits (SAS 70, SSAE 18, ISAE 3402), and service management (ISO 9000, ISO 20000-1). The audit-related guidelines and the SOC report chain (SAS 70 → SSAE 18 → ISAE 3402) are easy to misfile under information security.

18.8 Best practices for data centers

The best practices related to data centers are numerous, technical, and important. They give an engineering-operations technician a sense of the considerations that go into optimizing a data center and its operations. The best practices fall into categories including **load, fire safety, physical structure, equipment, environment, air distribution and cooling, and sustainability and energy efficiency**.

COMMON DATA CENTER BEST PRACTICES

- **Load** — Consider the initial and future load during the design phase, especially for partial and low-load conditions.
- **Fire safety** — Data centers present fire hazards; follow all fire codes and requirements across physical systems, structure, and safety protocols and processes.
- **Physical structure** — Adhere to all construction and facility-related codes for building materials, architecture, accessibility, and so forth.
- **Equipment** — Group similar equipment together to lower power consumption; arrange units with similar load densities and temperature requirements so cooling can be focused and optimized.
- **Environment** — Consider the data center's impact (pollution, energy consumption, waste) and minimize negative impact wherever possible.
- **Air distribution and cooling** — Purposeful, technically sound air distribution and cooling is critical to efficiency and availability.
- **Sustainability and energy efficiency** — Use energy and environmental resources efficiently so operations remain sustainable into the future.

WHY GROUPING EQUIPMENT MATTERS

Rather than scatter servers across the floor, group similar types together. Placing units with similar load densities and temperature requirements in the same area concentrates the heat they produce, which lets the cooling effort be focused and optimized instead of spread thinly across the whole hall — lowering overall data center power consumption. It is a single decision that improves both the equipment and air-distribution-and-cooling best-practice categories at once.

COMMON PITFALL

When a knowledge check asks which items are common best practices, choose from the real categories — load, equipment, air distribution and cooling, fire safety, physical structure, environment, and sustainability. Plausible-sounding distractors such as utilities, water use and recycling, or heating infrastructure are not on the module's list.

Module summary

- Codes, standards, and regulations differ by source of authority: codes are enforced by governmental entities to evolve best practices, standards define accepted professional practice, and regulations are government-defined rules to protect the public. Non-compliance can cost millions a year.
- Codes range from nationwide to local. Key agencies: NFPA (fire/electrical hazards), ECCCNY and building energy codes (IECC, ANSI/ASHRAE/IES 90.1), OSHA (safe workplace and health standards), and EPA (environmental regulations and emissions).
- Design and infrastructure standards apply across all data centers, and full compliance beats minimum compliance: ANSI/BICSI 002-2014 (all phases), ANSI/TIA 942-A 2014 (telecommunications), EN 50600 (first European-wide standard, series -1 through -2-6), and the Uptime Institute Tier Standard — which AWS does not use to certify its data centers.

- Certifications to know: SSAE 18 (now ISAE 3402) for honest financial reporting, SOC 2 Type II for data-handling policies, ISO/IEC 27001:2013 for risk and information security, PCI DSS 3.2 (mandatory for card processing), and the optional green certifications LEED and ENERGY STAR.
- Facility regulations span security (single entry, check-in/out, monitoring), safety and evacuation (orderly evacuation, drills roughly every 6 months), receiving equipment (logged, no flammable packaging in the data hall), and building rules (no smoking, weapons, or alcohol; mobile phones barred from the data hall).
- A 12-step procedure documents processes to maintain codes. A data center is not a certifying body — an accredited mediator organization issues a certificate of compliance after each audit.
- Audits keep compliance honest: code-maintenance audits run regularly by an impartial team of 3 to 5 people from outside the audited department; on-site OSHA safety audits run weekly or monthly against four questions on programs, requirements, documented proof, and training.
- Lesson 2 sorts industry guidelines into four focus areas — information security (HIPAA, ISO/IEC 27001, PCI DSS), physical design and operation (ANSI/BICSI 002, ANSI/TIA 942-A, ISO 14000), audits (SAS 70, SSAE 18, ISAE 3402), and service management (ISO 9000, ISO 20000-1) — and best practices into load, fire safety, physical structure, equipment, environment, air distribution and cooling, and sustainability.

Review questions

1. Define code, standard, and regulation, and explain why compliance matters.

Answer: A code is a regulation enforced by governmental entities to evolve best practices; a standard ensures organizations follow accepted professional practices; a regulation is a government-defined practice to protect the public and enforce ethical standards. Compliance matters because without it a data center can lose millions of dollars a year and face other threats and risks.

2. Match each standard to what it governs: ANSI/BICSI 002-2014, ANSI/TIA 942-A 2014, and EN 50600.

Answer: ANSI/BICSI 002-2014 covers best practices for all phases (planning, design, construction, maintenance, fire protection, security). ANSI/TIA 942-A 2014 is the telecommunications infrastructure standard (cabling, electrical layout, mechanical parts, architectural system). EN 50600 is the first European-wide standard for planning, construction, and operation, delivered as a series (-1 through -2-6).

3. Is the Uptime Institute Tier Standard used by AWS to certify its data centers?

Answer: No. The UI Tier Standard is a globally recognized reliability and performance standard, but AWS does not use it to certify its data centers.

4. Who issues a data center's certificate of compliance, and when?

Answer: An accredited, certified organization that acts as a mediator between the compliance body and the data center. It issues the certificate of compliance after every compliance audit; the data center itself is not a certifying body.

5. What keeps a code-maintenance audit impartial, and who conducts it?

Answer: A dedicated team of 3 to 5 people conducts it on a regular basis, and impartiality is ensured by not allowing people from the department being audited to audit themselves. The team inspects all safety equipment and program material to check safety, employee health, and fire hazards.

6. Which certification is mandatory, and which are optional — PCI DSS or LEED/ENERGY STAR?

Answer: PCI DSS is mandatory whenever a company or vendor processes a card. LEED and ENERGY STAR green certifications are considered optional for a data center.

7. Name the four industry-guideline focus areas and give an example guideline in each.

Answer: Information security (HIPAA or ISO/IEC 27001), physical design and operation (ANSI/BICSI 002-2014, ANSI/TIA 942-A 2014, or ISO 14000), audits (SAS 70, SSAE 18, or ISAE 3402), and service management (ISO 9000 or ISO 20000-1).

8. List several categories of data center best practices.

Answer: Load, fire safety, physical structure, equipment, environment, air distribution and cooling, and sustainability and energy efficiency — for example, grouping equipment with similar load densities and temperatures so cooling can be focused and optimized.
