MODULE 17 · STUDY NOTES

Safety Considerations in the Data Center

Reducing environmental impact, protecting employees, engineering fire detection and suppression, selecting and using PPE correctly, and turning risk assessment into method statements

Overall, a data center is a safe place to work — but that safety is engineered, not accidental. This module treats it as four interlocking domains. **Environmental health and safety (EHS)** looks outward at the data center's footprint on the planet and inward at the people on the floor. **Life safety systems** confront the fire risk that comes with running power-hungry equipment 24/7, layering fire detection, suppression, and the codes that govern both. **Personal protective equipment (PPE)** is the worn last line of defense between an employee and a recognized hazard, chosen task by task. And **risk assessment and method statements** turn all of it into documented, repeatable process — inventorying what can go wrong, how likely and how damaging it is, and exactly how the team will respond. The through-line: a low number of incidents reduces operational risk and increases uptime, so safety is not a cost center but a pillar of availability.

LEARNING OBJECTIVES

- Recognize how data centers are mitigating their environmental impact
- Identify employee safety measures that should be used in a data center
- Recognize the fire detection techniques used in a data center
- Recognize the fire suppression systems used in a data center
- Recognize the fire safety standards used in a data center
- Recognize the purpose of personal protective equipment (PPE)
- Describe appropriate PPE for various tasks
- Identify measures to be taken by employers and employees to ensure correct use of PPE
- Recognize how data center risk assessments help identify potential risk elements
- Identify risk elements and mitigation strategies applicable for a data center
- Outline the creation of risk heat maps and method statements

17.1 Reducing the environmental impact of data centers

As the number of data centers increases, so does their impact on the environment. The growth is dramatic: roughly **50,000** data centers operated worldwide in 2012, and by 2020 there were approximately **8 million** — driven by the adoption of smartphones, the Internet of Things (IoT), and data analytics. Data centers have become a necessity, and their environmental impact can be enormous. That impact takes three main forms.

TABLE 17.1 The three negative environmental impacts

IMPACT	WHY IT HAPPENS
Power consumption	Running 24/7 generates excessive heat, so data centers need effective cooling to hold optimal temperatures — and the cooling and power systems together consume large amounts of energy
Carbon footprint	A shortage of electric power has led some data centers to use fossil fuel and thermal energy, which can increase carbon emissions
Electronic waste	Faster obsolescence of electrical and electronic equipment means more to dispose of; disposal that ignores the prescribed guidelines harms the environment

Because energy demands are diversifying, data centers increasingly turn to alternative and renewable power — **wind power** (turbines), **hydroelectric power** (water), and **solar power** (the sun). Cooling drives similar innovation: some organizations locate facilities near water bodies to help dissipate heat, which in turn demands effective disaster-management planning against floods and hurricanes. Organizations worldwide recognize the benefits of operating in an eco-friendly manner and adopt several mitigating steps.

MEASURES TO REDUCE THE IMPACT

- **Energy-efficient data center designs** — use alternative, green power systems such as wind, solar, and hydroelectric power.
- **Energy-efficient cooling** — continually adjust the control of cooling systems (for example, the fan speed of an air-cooling unit) to maintain a set temperature while reducing energy use; some organizations use **AI systems** to monitor cooling, suggest optimizations, and implement changes after verification by a control system.
- **Adherence to government and agency regulations** — especially to reduce electronic-waste generation.

WORKED EXAMPLE – REDUCING A CARBON FOOTPRINT (KNOWLEDGE CHECK 1)

AnyCompany Inc. wants to reduce its carbon footprint. The correct tactics are to **create energy-efficient designs**, **use alternative green power systems** (such as wind and solar), and **adhere to government and agency regulations** — organizations can also use AI systems to monitor components. The distractors matter for the exam: **elevated floors**, **big data**, and **fossil fuels** are *not* carbon-reduction tactics — fossil fuels increase emissions.

17.2 Employee safety measures

Data centers are generally safe places to work, but certain workplace hazards demand awareness and preventative measures. In addition to EHS compliance, the operations team ensures employee safety in **three ways**: engage the right people to plan for EHS, enhance awareness, and prioritize safety training.

Engage the right people to plan for EHS. When planning and designing a data center, involve the appropriate personnel and draft EHS measures. EHS managers must ensure compliance with the regulations whenever a piece of equipment, a device, or a procedure changes in the working environment, and the appointed personnel must enforce that compliance.

Enhance awareness. The operations team maintains a checklist of potential safety hazards, updating it on any change, upgrade, or decommission of equipment or when rolling out new procedures. The checklist also includes mitigative procedures so employees know how to protect themselves.

TABLE 17.2 The hazard checklist and its mitigations

HAZARD	MITIGATION
Electrical hazards	Use proper PPE when handling cables and equipment; electrocution and high-voltage panels cause fatalities and serious injuries
Powered or manual loading of equipment	Provide proper tools for safe movement of goods — skid lifters, trolleys, and lifting trolleys
Fire hazards	Keep equipment for handling small fires available; provide fire-resistance gear to employees
High decibel noise areas	Use ear plugs and communication devices to protect the ears
Working at heights	Select the right size and type of ladder, keep three points of contact, and use fall-arrest systems (harnesses, lanyards, lifelines) even when regulations do not require it

Prioritize safety training. Training must be ongoing, especially when the data center infrastructure changes, and all employees must be kept current on known and unknown potential risks and common hazards.

COMPONENTS OF SAFETY TRAINING

- **Provide periodic training** — retrain when infrastructure is updated or modified or when new technology or processes are introduced; personnel should be certified annually on data center environmental safety.
- **Accompany personnel** — new employees are always accompanied by trained personnel until they can work on their own.
- **Maintain a logbook** — record all critical and near-miss incidents; prepare a root cause analysis (RCA), communicate it to all employees, and keep an accessible lessons-learned knowledge database.
- **Promote open communication** — during initiation and planning, EHS personnel establish a safety culture so every employee feels like a critical part of operations.
- **Reinforce safety and support** — build a strong culture that reinforces safety and supports the people running the data center.

17.3 Fire detection and suppression systems

Consuming large quantities of power can lead to fire hazards. Fires can spark from digital equipment, cables, air-conditioning equipment, floors, ceilings, and other combustible items, and can cause irreparable damage to data, property, and human lives. A fire safety system must **relate to the data center design**, include **fire detection and suppression** abilities, and — as a recommended practice — provide fire safety at **three levels: the building, the room, and the rack.** To provide full protection, the system must first detect a fire and then suppress it.

TABLE 17.3 Fire detection techniques

TECHNIQUE	HOW IT WORKS	NOTES
Spot detector	Used for early detection; activates when smoke reaches the device	Operates on two principles — ionization and photoelectric light scattering; can be installed in ventilation ducts; chosen by building design and fire-load conditions
Air sampling smoke detector	A piping distribution network continuously extracts room air and sends it to the detector, where it is analyzed for fire risk	Provides the earliest warning of a probable fire hazard
Spot heat detector	Mounted on the ceiling or a sidewall; activates when surrounding heat crosses a predefined limit	Three types: fixed-temperature, rate-of-rise, and rate-compensation

To reduce major collateral damage, a raging fire must be doused immediately — the job of a **fire suppression system.** Three types are used in data centers, and they differ sharply in how kind they are to electronics.

TABLE 17.4 Fire suppression systems

SYSTEM	BASIS	DATA CENTER FIT
Clean agent	Non-water-based; deprives the fire of oxygen to extinguish it; released from a control panel when a set number of designated detectors activate	Widely used; does not harm electronic components, and the data center does not close while it is in use
Sprinkler	The most common water-based type; can be a pre-action (dry) system or a wet system	Water can cause significant damage to IT equipment — using a sprinkler on data center fires is not advised
Water mist	A newer technology that works by atomizing water droplets into a non-conductive mist	Suppresses the fire without significant damage to electrical or IT equipment

> **COMMON PITFALL**
>
> Do not equate common with recommended. The sprinkler is the **most common** water-based suppression type, but because water damages IT equipment it is **not advised** for data center fires. The systems that protect electronics are **clean agent** (oxygen deprivation) and **water mist** (a non-conductive mist).

17.4 Fire safety standards (NFPA)

The **National Fire Protection Association (NFPA)** publishes more than **300** consensus codes and standards intended to minimize the possibility and effects of fire and other risks. A handful are central to data center life-safety.

TABLE 17.5 Key NFPA codes and standards

STANDARD	TITLE AND SCOPE
NFPA 75	Standard for the Fire Protection of Information Technology Equipment — covers protecting IT equipment and IT areas from fire and associated elements such as smoke, corrosion, heat, and water
NFPA 12a	Standard on Halon 1301 Fire Extinguishing Systems — requirements for total-flooding Halon 1301 systems across their life cycle
NFPA 2001	Standard on Clean Agent Fire Extinguishing Systems — requirements for total-flooding and local-application clean agent systems
NFPA 25	Standard for Inspection, Testing, and Maintenance of Water-Based Fire Protection Systems — the baseline for maintaining system integrity and fast, effective response
NFPA 72	National Fire Alarm and Signaling Code — fire detection, signaling, and emergency communications, including mass-notification systems for weather, terrorist, and other emergencies

REMEMBER

- NFPA publishes **300+** consensus fire codes and standards, not just these five.
- Pair each standard with its system: `NFPA 2001` with clean agent, `NFPA 12a` with Halon 1301, `NFPA 25` with water-based systems, `NFPA 75` with IT equipment, and `NFPA 72` with alarm and signaling.
- A separate standard, `NFPA 70E`, governs the arc-rated hood used as PPE for arc-flash work.

17.5 Personal protective equipment – purpose and types

New-age data centers are larger and consume more power, and an emphasis on employee safety contributes directly to maximum availability — an accident can shut down operations. A **low number of incidents reduces the operational risk of working in a data center and helps increase uptime.** PPE is a level of defense from injury while performing potentially hazardous work. The **U.S. Occupational Safety and Health Administration (OSHA)** defines PPE as **items typically worn by a worker to provide protection from recognized hazards** — it is the *final* level of defense against an injury or fatality.

PROTECTION PPE IS INTENDED TO PROVIDE

- Head and face protection
- Eye protection
- Torso and limb protection
- Hearing protection
- Foot protection

The type of PPE is selected based on the task to be performed. PPE typically used by data center employees includes **ear plugs, safety glasses, goggles, face shields, hard hats, and safety shoes**, plus **insulating (rubber) gloves with leather protectors, anti-static wrist straps, cut-resistant gloves, chemical-resistant gloves, insulating sleeves, and flame-resistant (FR) clothing.**

For **arc flashes**, the PPE is **arc-rated clothing**, which shields the employee's body, hands, and feet from electrical arc hazards that can arise while working on energized equipment. It comprises a **jacket** (upper body), **pants** (lower body), and a **beekeeper-style hood** fitted with a face covering (per `NFPA 70E`).

COMMON PITFALL

Insulation protective equipment is **not PPE** — because it is not worn. Items such as **rubber hoods, line hoses, rubber blankets, and hot sticks** are used when performing electrical installations, but they sit outside the definition of PPE. (Note: the standards referenced here are specific to the United States and are not global — refer to the standards applicable to your country or region.)

17.6 Selecting and using PPE correctly

Determining the right PPE means assessing and anticipating the potential risk of the job or task. The appropriate amount safeguards employees: if PPE is **insufficient**, exposure to injury increases; but the **wrong type or too much** PPE can limit an employee's movement or impair their vision. The goal is the *optimal* amount and type, which is why the employer must assess the potential hazards of the task.

ASSESSING POTENTIAL ELECTRICAL HAZARDS

- Three electrical hazard types: **shock hazards, arc-flash hazards, and approach-boundary hazards.**
- The hazard assessment also evaluates other working-area hazards: **proximity to a heat source or an extremely cold source**, the **probability of slipping or falling**, and **small or confined workspaces.**
- A thorough hazard assessment is what lets PPE needs be accurately determined for the task.

TABLE 17.6 Risks specific to a data center and their precautions

TASK	KEY PRECAUTIONS AND PPE
Working with electricity	Data centers increasingly use high voltages; use a formal work order before any work on energized equipment, and use PPE that insulates from shock when working on anything over `50 V`
Heavy item lifting	Use correct PPE including footwear; use correct lifting techniques (keep a straight back); avoid lifting from the floor or carrying loads long distances; use lifting equipment when available; wear gloves that give adequate grip
Water cooling unit maintenance	Identify all electrical, mechanical, hydraulic, chemical, and thermal risks; know the isolation types and the right device; always wear safety shoes and gloves; wear eye/face protection against chemicals, gases, acids, and flying objects
Computer maintenance	Consider all risks (primarily electrical and heat); check all equipment and PPE for damage first; wear an anti-static wrist strap, which safely grounds the person and prevents static buildup

WORKED EXAMPLE – MATCHING PPE TO THE TASK (KNOWLEDGE CHECK)

Protective, grip-enhancing gloves → lifting heavy items. **Safety goggles and chemical-resistant gloves** → water cooling unit maintenance. **Anti-static wrist strap** → computer maintenance. **Arc-rated jacket, pants, and hood** → maintenance on energized equipment. The pattern to remember: the PPE follows the dominant hazard of the task.

EMPLOYER ACTIONS	EMPLOYEE ACTIONS
ensure PPE is used correctly ▪ Provide regular **training** on the correct use of PPE for all tasks; routinely discuss it and make it visible with posters in the work areas ▪ Perform **regular inspection** of PPE to test its fitness for the relevant employees ▪ Maintain **documentation** — a comprehensive assessment of PPE hazards and the process for selecting the PPE that best suits the task and conditions	*follow the guidelines* ▪ Wear proper undergarments: **non-melting flammable garments** (wool, cotton, silk, rayon, or a blend) beneath arc-rated clothing ▪ Avoid wearing **conductive items** and fibers that can melt beneath the protective garments ▪ Use the correct, undamaged PPE for the task and report worn or damaged equipment

COMMON PITFALL

The three employer measures the knowledge check rewards are **use posters to make PPE visible, provide training on correct use, and document the hazard assessment and PPE selection.** Wearing extra PPE for extra safety, applying for a work order, or letting employees skip PPE that inhibits agility are all wrong.

17.7 Risk assessment and the ISO 31000 process

Data centers host some of an organization's most important IT resources, which must stay continuously available and operational. Delivering that availability relies on many systems, procedures, and processes — all susceptible to risk. Identifying risks **upfront** prevents unplanned or unidentified issues from disrupting operations. Three related ideas frame the discipline: **risk** (what can go wrong), **risk assessment** (inventorying which risks are most likely and where they hit hardest), and the **risk management plan** (covering every identified risk with mitigating activities and procedures, so that if a risk occurs employees can neutralize it).

`ISO 31000:2018` — *Risk management — Guidelines*, from the International Organization for Standardization — provides guidelines on how to assess and document risk, and organizations customize them to their needs. The standard outlines **six steps.**

TABLE 17.7 The six-step risk assessment process (ISO 31000:2018)

STEP	WHAT IT INVOLVES
1. Identify the sources of risk	Sources include cybercrime, hardware failures, malware, power failures, physical-territory breaches, earthquakes, and natural disasters; assessments vary by the data center's services and uptime requirements
2. Analyze the areas of impact	Analyze causes and potential consequences — a logical intrusion or malware attack could lead to financial fraud or loss of critical data and reputation; determine whether the source is internal or external
3. Evaluate the likelihood of occurrence	Judge how probable the identified risk is
4. Determine if existing controls prevent it	Check for controls and procedures already in place; the three control types are detective, preventive, and recovery
5. Introduce additional controls	Stakeholders add controls to reduce risk to an acceptable level per regulatory requirements, internal and external stakeholders, and legal necessity — producing a heat map of gross vs. net risk
6. Document the risk assessment	Record the assessment, controls, and residual risks in a sustainable format that captures changes in real time

THE THREE CONTROL TYPES (STEP 4)

- **Detective controls** — regularly check devices for any suspicious activity.
- **Preventive controls** — regularly update antivirus software and patches to prevent a breach.
- **Recovery controls** — tools that scan and remove suspicious elements from the entire network.

17.8 Risk elements and mitigation strategies

When assessing risk for a data center, examine each risk consideration and determine both its **probability of occurrence** and its **impact** if it materializes. Risks fall into two families — and the data center has more control over the internal ones, which arise during normal operations and are somewhat predictable, than over external ones, which are harder to mitigate because there is little control over them.

INTERNAL RISKS	EXTERNAL RISKS
more controllable and predictable	*harder to mitigate — little control*
▪ Fires	▪ Floods and earthquakes
▪ Loss of life or injuries due to accidents	▪ Power grid failures
▪ Non-usage of standard procedures by workers	▪ Pandemics
▪ Internal data theft	▪ Supply chain failures
▪ Skill unavailability	▪ Cybersecurity breaches

TABLE 17.8 Risk mitigation strategies

RISK ELEMENT	MITIGATION STRATEGY
Power failure	Power is mission-critical, and failure causes an immediate disruption to service; mitigate with redundancy of critical supply points, an uninterruptible power supply (UPS), and generators for sufficient backup
Fire	An immediate disruption of service; requires proper equipment to fight small fires plus an automatic alarm
Natural calamities	Service disruption from floods, extreme weather, air contamination, or pandemics; requires a provision for working remotely and management of critical equipment
Security	Internal and external, physical and logical breaches; requires perimeter security, closed-circuit cameras, strong authentication, and data-leakage protection solutions
Other risks	New-technology rollout, management and resources, non-compliance, and operational safety; mitigate by training and refreshing employees, holding them accountable, and monitoring for risks daily

17.9 Risk heat maps and method statements

All risks affect data center operations in some way. The data center creates an **initial risk heat map** outlining the risks and the **probability and impact** if each element materializes. The map compares initial **gross** risk to treated **net** risk, and it is used to build a **business continuity plan (BCP)** — a plan for mitigating potential risks so operations are not disrupted and the business continues as usual.

Once the assessment is complete and controls have been identified to keep risks within tolerable limits, management creates a **method statement.** It defines the **sequence of activities** to complete and the proper management arrangements to perform the overall tasks. Beyond data center-specific rules, restrictions, and training, it captures the **risks identified through risk assessment** (with a net risk score within tolerable limits and the control measures identified) and further detail on **how, who, and when** the safety measures are used. In short, a method statement is a more elaborate risk assessment document.

SECTIONS A METHOD STATEMENT IS OFTEN SPLIT INTO

- Data center details
- Activity and description of risks associated with the work steps
- Date and duration of work
- Responsibility for each work step
- Detailed procedure and control measures, including the steps of actions
- PPE requirements, if any
- Management arrangements and monitoring arrangements
- Emergency procedures, as needed

COMMON PITFALL

The two factors that build a risk heat map are the **probability of the risk materializing** and the **impact of the risk** — not control measures, legal repercussions, or generic operational risk. The map tells the data center which risks are critical and demand attention.

Module summary

- Safety in the data center spans four domains — environmental health and safety, life safety (fire), PPE, and risk assessment and method statements — and fewer incidents mean lower operational risk and higher availability.
- Data centers harm the environment through power consumption, carbon footprint, and electronic waste; organizations mitigate with energy-efficient designs (green power), energy-efficient cooling (including AI-monitored cooling), and adherence to government and agency regulations.
- Employee safety is achieved by engaging the right people to plan for EHS, enhancing awareness through a hazard checklist (electrical, powered/manual loading, fire, high decibel noise, working at heights), and prioritizing ongoing safety training.
- A fire safety system must detect then suppress a fire and protect the building, room, and rack; detection uses spot detectors, air-sampling smoke detectors, and spot heat detectors.
- The three suppression systems are clean agent (non-water, oxygen deprivation, safe for electronics), sprinkler (common water-based but damaging to IT — not advised), and water mist (non-conductive, no equipment damage).
- NFPA publishes 300+ fire codes; know NFPA 75 (IT equipment), 12a (Halon 1301), 2001 (clean agent), 25 (water-based systems), and 72 (alarm and signaling), plus NFPA 70E for the arc-rated hood.
- PPE is items worn to protect from recognized hazards (OSHA); it is selected by task and used in the optimal amount, with arc-rated clothing (jacket, pants, beekeeper-style hood) and insulating PPE for energized work over 50 V.
- Employers ensure correct PPE use through training, posters, regular fitness inspection, and documented hazard/selection assessments; employees follow guidelines such as non-melting undergarments beneath arc-rated clothing.
- Risk assessment follows the six ISO 31000:2018 steps and feeds a risk management plan, mitigation strategies for internal and external risks, a risk heat map (probability × impact, gross vs. net, feeding a BCP), and a method statement that sequences the controls.

Review questions

1. What are the three potential negative environmental impacts of data centers, and what three measures reduce them?

Answer: Impacts: power consumption, carbon footprint, and electronic-waste generation. Measures: energy-efficient data center designs (green power such as wind, solar, and hydroelectric), energy-efficient cooling, and adherence to government and agency regulations.

2. In what three ways does a data center operations team achieve employee safety, and what belongs on the hazard checklist?

Answer: Engage the right people to plan for EHS, enhance awareness, and prioritize safety training. The hazard checklist covers electrical hazards, powered or manual loading of equipment, fire hazards, high decibel noise areas, and working at heights.

3. Compare the three fire detection techniques.

Answer: A spot detector activates when smoke reaches it (ionization plus photoelectric light scattering); an air sampling smoke detector uses a piping network to continuously extract room air for the earliest warning; a spot heat detector is ceiling/sidewall-mounted and triggers when heat passes a preset limit (fixed-temperature, rate-of-rise, or rate-compensation).

4. Why is a sprinkler not the recommended suppression system for a data center, and which systems are preferred?

Answer: Sprinklers are the most common water-based system, but water can cause significant damage to IT equipment, so they are not advised for data center fires. Clean agent (non-water, deprives fire of oxygen) and water mist (non-conductive atomized mist) protect electronics.

5. Match these NFPA standards to their scope: 75, 2001, 12a, 25, 72.

Answer: NFPA 75 — fire protection of IT equipment; NFPA 2001 — clean agent extinguishing systems; NFPA 12a — Halon 1301 systems; NFPA 25 — inspection, testing, and maintenance of water-based systems; NFPA 72 — National Fire Alarm and Signaling Code.

6. What is the risk of using too little or too much PPE, and how is the right level determined?

Answer: Insufficient PPE increases the employee's exposure to injury; the wrong type or too much PPE can limit movement or impair vision. The employer assesses the potential hazards of the task to determine the optimal amount and type.

7. List the six ISO 31000:2018 risk assessment steps.

Answer: Identify the sources of risk; analyze the areas of impact; evaluate the likelihood of occurrence; determine if existing controls can prevent the risk; introduce additional controls to minimize potential risks; and document the risk assessment.

8. What two factors define a risk heat map, and what is a method statement?

Answer: A risk heat map is built from a risk's probability of materializing and its impact (comparing gross to net risk, feeding a business continuity plan). A method statement is a more elaborate risk assessment document that defines the sequence of activities and controls — with net risk within tolerable limits — for performing tasks.