Topic 5B: Physical Security, Protocols & Hazardous Materials

A building does not protect itself. Facility managers are responsible for the systems, procedures, and physical measures that keep occupants safe and assets secure. Topic 5B covers three areas where that responsibility is most direct: physical security systems, security protocols and incident management, and environmental health and hazardous materials. Each area requires both technical knowledge and sound judgment. Together, they define how a well-run facility manages risk every day.

5.3 Physical Security Systems

Physical security is one of the most visible parts of a facility manager's job. Occupants notice when access control works smoothly. They notice when cameras are in place. They also notice when systems fail or gaps appear. **Physical security systems** are the hardware, software, and infrastructure that control who enters a building, detect unauthorized activity, and deter threats before they grow. Facility managers who understand these systems can build layered protection, manage vendors well, and respond quickly when something goes wrong.

Access Control Systems

Access control is the process of managing who can enter a building, a floor, or a specific room — and when. Modern access control systems replace traditional keys with electronic credentials. These credentials can be issued, changed, or removed without replacing any hardware. When an employee leaves, their access can be cut off instantly. When a contractor needs short-term entry to a restricted area, access can be set for a defined window and turned off when that window closes.

Credential Type	How It Works	Security Level	Typical Use Case
Proximity Card	Cardholder holds card near reader; system grants or denies based on assigned access rights	Moderate	Standard employee access across most commercial facilities
Smart Card	Same reader interaction as prox card but stores more data and uses stronger encryption	Moderate–High	Organizations requiring enhanced data security or multi-function credentials
Mobile Credential	Smartphone app delivers credential wirelessly to reader	Moderate–High	Facilities eliminating physical card issuance and tracking

Credential Type	How It Works	Security Level	Typical Use Case
Keypad / PIN	Numeric code entered at reader grants entry	Low	Low-security areas or backup access where card readers are impractical
Biometric Reader	Scans physical trait (fingerprint, iris, face) to confirm identity; cannot be transferred	High	Data centers, server rooms, executive spaces requiring strong identity assurance

TABLE 5.5 | ACCESS CONTROL CREDENTIAL TYPES

Access control systems are managed through a central software platform that logs every entry and exit event. This **audit trail** is a critical security and compliance tool. If an incident occurs, investigators can pull the log and see exactly who entered which space and when. Facility managers use the same data to spot unusual patterns — such as a card used outside of normal hours — that may signal a security concern before it becomes a serious problem.

Linking access control to the BAS and the CMMS improves both security and operations. A BAS link can adjust lighting and HVAC in a space when access is granted, saving energy in low-use areas. A CMMS link ties contractor access directly to active work orders, so credentials expire when the job is done. These connections turn access control from a standalone tool into a core part of how the building runs.

CCTV and Video Surveillance

Closed-circuit television, or **CCTV**, is one of the most widely used security tools in commercial facilities. A well-designed video surveillance system serves two purposes. First, it deters bad actors who know they are being recorded. Second, it provides recorded evidence when an incident occurs. Facility managers are responsible for covering the right locations, storing footage for the required time, and keeping camera hardware in working order.

Camera placement is the foundation of an effective CCTV system. The goal is to cover key points with no blind spots: building entrances and exits, parking areas, loading docks, elevator lobbies, stairwells, and areas where high-value assets are stored. Cameras should capture clear images of faces and license plates — not just motion. A camera aimed at the top of a person's head has limited value. Overlapping coverage between nearby cameras ensures that one camera failure does not leave a gap.

Modern CCTV systems use **IP cameras** that send footage over the building's data network to a central **network video recorder**, or **NVR**. IP systems offer higher image quality than older analog systems and allow remote viewing from any approved device. **Pan-tilt-zoom**, or **PTZ**, cameras can be directed remotely to follow activity in real time. They work well at large open areas like parking lots and loading docks. Fixed cameras are simpler and more reliable for doorways and corridors where the field of view stays the same.

Footage retention is an important policy decision. Most organizations keep video for 30 to 90 days before it is overwritten. Some regulated industries require longer periods. Facility managers must confirm that storage capacity matches the retention policy and that the system is actually recording — not just showing a live feed with no storage behind it. Regular checks, including reviewing a sample of recorded footage, confirm the system is working as intended.

Camera maintenance is an ongoing task. Outdoor cameras face weather, vandalism, and dirty lenses. Indoor cameras can be blocked by new furniture, signs, or plants. A quarterly inspection of every camera — checking image quality, field of view, and recording function — catches problems before they become security gaps. Camera maintenance records should be tracked in the CMMS like any other building equipment.

Intrusion Detection and Perimeter Security

Access control and CCTV focus on people who use normal entry points. **Intrusion detection systems** address people who do not. These systems monitor the building envelope — doors, windows, walls, and rooflines — for unauthorized entry and trigger an alarm when a breach is detected. They allow the building to be watched around the clock, even when no security staff are on site.

Device Type	Technology	What Triggers the Alarm	Best Use Setting
Door and Window Contacts	Magnetic sensors on the door/window frame and sash	Opening while the system is armed	Entry points, perimeter doors, ground-floor windows
Motion Detectors (PIR)	Passive infrared sensors detect body heat moving through a protected zone	Movement in a monitored area	Large open interiors — lobbies, warehouses, open-plan floors
Glass Break Detectors	Acoustic sensors tuned to the frequency of shattering glass	Sound of glass breaking	Ground-floor windows; areas where contact sensors alone are insufficient

TABLE 5.6 | INTRUSION DETECTION DEVICE TYPES

Perimeter security extends protection to the area around the building. Fencing, gates, lighting, and landscaping all play a role. A well-lit perimeter removes the cover that intruders rely on. Thorny plants along building edges make window access harder. **Security lighting** — including motion-activated fixtures at entry points and parking areas — is one of the most cost-effective perimeter tools available. It is also a visible deterrent.

Intrusion systems are typically monitored by a central station that notifies security staff or law enforcement when an alarm fires. Facility managers must balance sensitivity and false alarms. A system set too loosely misses real events. A system set too tightly creates

constant false alarms that cause staff to stop taking them seriously. Reviewing alarm history with the monitoring provider and adjusting sensor sensitivity over time keeps the system working without creating alarm fatigue.

Perimeter security also covers utility entry points: electrical vaults, gas meter locations, telecommunications rooms, and roof access hatches. These points are easy to overlook but present real risk if left unsecured. They should be part of the access control program, locked when not in active use, and checked regularly as part of the facility's security audit cycle.

Visitor Management Systems

Every person who enters a commercial building is either someone whose identity and access rights are already known — or someone who is not. The second group — visitors, contractors, delivery workers, and guests — is a security challenge that many facilities manage poorly. A **visitor management system** is the process and technology used to track, control, and record the movement of non-employees through the facility.

At the most basic level, visitor management means signing in at a front desk and getting a paper badge. This approach has real weaknesses. Paper logs are hard to search, easy to falsify, and give no real-time view of who is in the building. **Digital visitor management platforms** close these gaps. A visitor pre-registers online before their visit. On arrival, they check in at a kiosk, their identity is confirmed, and a printed badge with a photo and expiration time is issued. The host is notified right away. When the visitor leaves, the departure is recorded.

Digital platforms can also screen visitors against **watchlists** before issuing a badge. This step takes only seconds but adds a real layer of screening to the check-in process. Some systems link directly to access control and issue a temporary credential that gives the visitor access only to the areas they need — and only for the length of their visit.

Contractor management is a separate part of visitor management that needs extra attention. Contractors working on building systems often need access to mechanical rooms, electrical vaults, and other sensitive areas. A contractor management program confirms that each company holds current insurance and valid licenses before granting access. Individual workers should carry valid identification and receive credentials tied to a specific work order. Access should expire when the project ends.

In an emergency — a fire evacuation, shelter-in-place, or lockdown — knowing exactly who is in the building is critical. Digital visitor management systems produce an instant occupant list that security teams and emergency responders can use to account for everyone on site. Organizations using paper logs or no system at all face a serious gap right when accurate information matters most.

Physical Barriers and Bollards

Not all security threats come from someone walking through a door. Vehicle impacts — whether intentional or accidental — require physical barriers that access control and cameras cannot stop. **Physical barriers** are hardened structures built to absorb or redirect impact energy and keep vehicles away from pedestrian areas, building entrances, and critical infrastructure. Facility managers at buildings with public entrances or high-

occupancy spaces must assess whether barriers are needed and ensure that installed barriers meet current standards.

Bollards are the most common physical barrier in commercial settings. A bollard is a short, sturdy post placed in front of an entrance, sidewalk, or parking zone to block vehicle access. They come in two main types. **Fixed bollards** are anchored in concrete and offer the highest level of protection. **Removable or retractable bollards** can be lowered to allow approved vehicles — delivery trucks, emergency responders, maintenance vehicles — and raised again when that access is done. Retractable bollards are common at service entrances and loading areas where controlled vehicle access is needed.

Bollard selection and placement should follow guidance from groups such as **ASTM**, which publishes crash-test ratings for barrier systems. A bollard's rating shows the vehicle weight and speed it can stop. Spacing between bollards matters just as much as the bollard itself. Gaps that are too wide let a vehicle pass between posts. Posts placed too close together can create hazards for people using mobility aids.

Beyond bollards, facility managers use **Jersey barriers**, **landscape planters**, **raised curbing**, and **security gates** to build layered protection at vehicle entry points. Planters and decorative barriers do double duty — they improve the look of an entrance while adding impact resistance. Many urban buildings use concrete-filled planters to create a buffer between the street and the entrance without the industrial look of exposed bollards.

Facility managers review barrier condition as part of the broader security audit. Over time, barriers can be damaged by minor vehicle impacts, corroded by weather, or weakened by nearby construction. A barrier that looks intact on the outside may no longer perform as designed. Regular inspection — checking anchors and surface condition — keeps the perimeter protection at the level the building's security plan requires.

REFLECTION QUESTION

> A facility manager is reviewing a security audit report and finds that three cameras covering the main loading dock have not been recording for two weeks due to a storage system failure. The cameras still show a live feed at the security desk, so the issue went undetected. What changes to the facility's CCTV management practices would prevent this from happening again?

5.4 Security Protocols & Incident Management

Physical security systems are only part of the picture. The policies and procedures behind those systems are what make them work. **Security protocols** define how a facility responds to threats, manages access, and handles incidents when they occur. Without clear protocols, even the best hardware investment falls short. Systems record events. People must know what to do when those events happen.

Developing and Implementing Security Policies

A **security policy** sets the rules that govern how people interact with the building's security systems and controlled spaces. Without a written policy, security decisions get made on the fly — and usually poorly. A clear policy gives everyone the same expectations and removes guesswork when a situation comes up.

Good security policies share a few traits. They are specific enough to guide behavior but broad enough to cover a range of situations. They use plain language that all staff can follow — not just security professionals. And they are reviewed on a regular schedule so they stay current as the building, the organization, and the threat environment change.

Facility managers typically write security policies with input from HR, legal, and senior leadership. HR makes sure policies align with employment practices. Legal confirms they meet applicable laws. Leadership buy-in matters because policies only work when they are enforced from the top down. A policy that managers ignore sends a clear signal to everyone else that the rules do not apply.

Once a policy is approved, it must reach all staff. New employees should get security training as part of onboarding. Existing staff need a refresher whenever a policy changes. Training records must be kept so the organization can show that everyone was informed. A policy that no one knows about offers no protection.

Policy enforcement is where many security programs break down. Tailgating, propped doors, and unescorted visitors are common violations that become accepted habits over time. Addressing these behaviors early and consistently is far easier than trying to fix a culture of non-compliance after it has taken hold. Facility managers who hold the line on small violations build a culture where the bigger rules are followed too.

Threat Assessment and Planning

A **threat assessment** is a structured process for identifying the risks a facility faces and judging how serious each one is. It looks at the building's location, occupancy, operations, and history to build a clear picture of what threats are most likely and what the impact would be if they occurred. Every commercial building faces some level of risk — from theft and vandalism to workplace violence and severe weather — and every facility benefits from understanding those risks clearly.

The process starts with listing potential threats. These fall into broad groups: criminal activity such as theft and vandalism; workplace violence from current or former employees; external threats such as protests or targeted attacks; and environmental threats including severe weather and utility failures. Each threat is rated on two factors: how likely it is to happen, and how serious the impact would be if it did.

These ratings feed into a **risk matrix** that ranks threats by their combined score. High-likelihood, high-impact threats get the most resources. Low-likelihood, low-impact threats may be accepted with little or no mitigation. The matrix gives facility managers and leadership a clear tool for deciding where to invest in security and where the current level of protection is enough.

Threat assessments work best when done by a team. Facility management, security staff, HR, and operations leadership all bring useful perspective. Outside security consultants are often brought in for an objective view. The assessment should be updated at least once a year and after any major change — a new tenant, a renovation, or a nearby security incident.

Assessment findings drive the creation of **security plans** — written documents that describe the specific measures in place to address each identified threat. A security plan is not the same as a security policy. The policy sets the rules. The plan describes the physical

systems, staffing, response steps, and training programs that carry out those rules. Together, a policy and a plan give a facility a complete framework for managing security risk.

Incident Response Protocols

Even the best security program cannot prevent every incident. What sets well-run facilities apart is how they respond when something goes wrong. **Incident response protocols** are step-by-step procedures that tell security staff, facility managers, and occupants exactly what to do when a security event occurs. Writing these procedures down and practicing them in advance is the difference between a controlled response and a chaotic one.

Protocols cover a range of event types. **Unauthorized access** — someone entering a restricted area without valid credentials — calls for identifying and stopping the individual, reviewing access logs, and finding out how the breach happened. **Theft or vandalism** requires securing the scene, notifying law enforcement, preserving evidence, and pulling camera footage. **Workplace violence** or an **active threat** requires calling law enforcement right away, activating a lockdown or evacuation, and sending clear instructions to all occupants.

Every protocol depends on a clear **notification chain**. When an incident occurs, who gets called first? Who decides to evacuate or lock down? Who speaks to the media or to law enforcement? These questions must be answered before an incident happens and rehearsed so everyone knows their role. Under stress, people do what they have practiced. If they have never run through the notification chain, the response will be slow.

> A protocol that only exists on paper has not been tested and cannot be trusted.

Facility managers play a direct role in incident response. They control the building systems that support it — access control locks, public address systems, elevator recall, and lighting. They also manage the physical space: opening emergency exits, guiding occupants to assembly areas, and working with first responders when they arrive. This requires both technical knowledge of the building and the ability to stay calm under pressure.

Protocols must be tested through regular drills. Drills reveal gaps — a public address system with poor coverage, an assembly area that is too small, a notification chain with a missing contact. Each gap found in a drill is a problem fixed before a real incident makes it critical. Drill results should be recorded and used to update protocols.

Post-Incident Documentation

When a security incident ends, the work is not done. **Post-incident documentation** is the process of recording what happened, how the team responded, and what the outcome was. Good records serve several purposes. They create a legal file. They support insurance claims. They provide the material for a lessons-learned review. And they build the knowledge base that makes the next response better.

Every security incident should result in a written **incident report**. The report must be specific — vague phrases like “appropriate action was taken” are useless to anyone who reads the report later. Every incident report must include:

- Date, time, and location of the event
- Names of all people involved
- Factual account of what happened and in what order
- Actions taken by security and facility staff
- Any injuries or property damage sustained
- Steps taken to return to normal operations

For serious incidents — those involving injury, law enforcement, or major property damage — the report should be followed by a formal **after-action review**. This is a structured meeting that brings together everyone involved in the response. The goal is not to assign blame. The goal is to find the specific factors that shaped the outcome and decide what changes would improve the next response.

After-action reviews often surface issues that were not obvious during the incident. A communication gap that seemed minor may have delayed a key notification. A decision that felt right under pressure may look different with full information. Findings should become specific action items with assigned owners and due dates. Following through on those items is what turns a review into a real improvement.

Incident records must be kept according to the organization's retention policy and any legal requirements. Some incidents trigger reporting rules — workplace injuries go on the OSHA 300 Log, and certain environmental events may require agency notice. Facility managers must know which rules apply to their facility and make sure the right reports are filed on time.

Security Audits and Performance Metrics

A security program that is never measured will drift. **Security audits** and **performance metrics** give facility managers the tools to check whether the program is working, find where it is falling short, and make the case for the resources needed to fix problems. Without regular measurement, security investments are hard to justify and security failures are hard to see coming.

A **security audit** is a structured review of the facility's physical systems, policies, procedures, and records. It checks whether access control hardware works correctly, whether camera coverage meets the design standard, whether response protocols are current and tested, and whether staff training is complete. Audits can be done by the facility team or by an outside security consultant. External audits add value because they bring an independent view and are less likely to miss familiar problems.

Audits should happen at least once a year and after any major security incident or physical change to the building. The audit produces a written report that lists findings, rates each one by severity, and recommends corrective actions. Open findings must be tracked until they are resolved. Leaving findings unaddressed weakens the audit process and creates liability if an incident later occurs in an area that was already flagged.

Performance metrics provide ongoing visibility between formal audits. Common metrics include the number of security incidents per month, average alarm response time, the percentage of access control devices that are online, camera uptime rates, and staff training completion rates. Each metric tells a specific story about program health. Tracking

them over time shows trends — a rising incident count in one area, a falling training rate — that call for investigation and action.

Sharing metrics with building owners and senior leadership builds confidence in the program and supports budget requests. A facility manager who can show a year-over-year drop in incidents, strong camera uptime, and a fully trained staff has made a clear case that the security investment is working. Data-driven security management is not just good practice — it is the language that decision-makers respond to most directly.

FIGURE 5.3 | SECURITY OPERATIONS MONITORING WORKSTATION

REFLECTION QUESTION

> A facility manager conducts an annual security audit and finds that 20 percent of access control readers show intermittent failures, response time to after-hours alarms averages 11 minutes against a 5-minute target, and the last full security drill was held 18 months ago. How should the facility manager prioritize these findings, and what steps would address each one?

5.5 Environmental Health & Hazardous Materials

Commercial buildings contain materials and substances that can harm people if they are not managed correctly. Some hazards are built into the structure itself — asbestos in ceiling tiles, lead paint on older walls. Others come from daily operations — cleaning chemicals, maintenance supplies, and waste materials. **Environmental health and hazardous materials** management covers the programs that identify these hazards, control exposure, and make sure waste and spills are handled according to the law. This subtopic covers the five areas that every facility manager must understand and actively manage.

Asbestos and Lead Paint Management Programs

Asbestos is a mineral that was used widely in building construction through the late 1970s. It appeared in floor tiles, ceiling tiles, pipe insulation, roofing materials, and joint compound. When asbestos-containing materials are cut, drilled, or broken, they release tiny fibers into the air. Inhaling those fibers can cause serious lung diseases, including mesothelioma and lung cancer. There is no safe level of asbestos exposure.

Facility managers in buildings built before 1980 must assume asbestos may be present until a formal survey proves otherwise. A licensed inspector collects samples from suspected materials and sends them to an accredited lab. The results go into an **asbestos management plan** that records the location, condition, and amount of all confirmed asbestos in the building. This plan must stay current and be available to workers, contractors, and emergency responders.

Not all asbestos requires removal. Material that is in good condition and left undisturbed poses low risk and is often best managed in place. This is called an **operations and maintenance**, or **O&M**, program. An O&M program sets rules for working near asbestos — no drilling, cutting, or sanding without checking the plan first. When materials must be disturbed for renovation or repair, a licensed **abatement contractor** removes them under controlled conditions before any other work begins.

Lead paint presents a similar challenge. Lead was common in paint until it was banned for residential use in 1978. Many older commercial buildings still have lead-based paint on walls, trim, windows, and doors. Lead exposure is most dangerous when paint is flaking or being sanded, because it releases dust that can be inhaled or swallowed. Facility managers must conduct a **lead paint assessment** in older buildings and keep records of where lead paint exists and what condition it is in.

Intact lead paint in good condition is usually managed in place. When surfaces require maintenance or renovation, workers must follow **lead-safe work practices** that limit dust, use containment, and ensure thorough cleanup. Contractors who disturb lead paint in pre-1978 buildings must be certified under the **EPA Renovation, Repair, and Painting Rule**, or **RRP Rule**. Hiring uncertified contractors for this work creates serious regulatory liability.

Mold Assessment and Remediation

Mold grows wherever moisture and organic material meet. In a commercial building, it can appear behind walls, under flooring, in ceiling spaces, and in HVAC ductwork after a water event. Mold releases spores that cause allergic reactions, asthma attacks, and breathing problems. For facility managers, mold is both a health issue and a building science issue — it cannot be fixed without addressing the moisture source that feeds it.

The first sign of a mold problem is often a musty smell or a dark stain on a surface. Both call for quick investigation. A **mold assessment** finds the extent of growth, identifies the moisture source, and guides the cleanup plan. Small areas — generally less than 10 square feet — can often be handled by trained facility staff using guidelines such as the **IICRC S520 Standard for Professional Mold Remediation**. Larger areas need a qualified industrial hygienist or mold remediation professional.

Effective mold remediation follows a clear order (Figure 5.4):

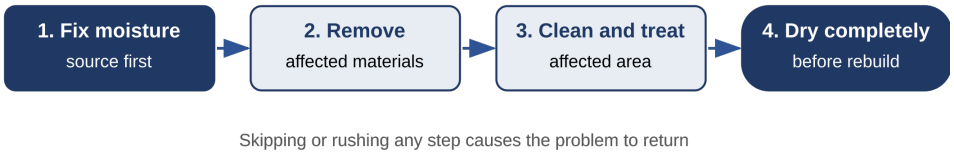

FIGURE 5.4 | MOLD REMEDIATION SEQUENCE

Prevention costs far less than remediation. Responding to water events within 24 to 48 hours stops most mold before it starts. Facility managers should have a clear water event protocol: assess moisture, remove standing water, run dehumidification equipment, and monitor humidity until the area returns to normal. Keeping indoor relative humidity below 60 percent across the building provides ongoing mold prevention.

After any major mold remediation, a **post-remediation verification** confirms the work was successful. This involves a visual check and air sampling to compare spore counts inside the treated area to outdoor levels. A clean result gives building owners and occupants confidence the problem is resolved. All records of the event, the remediation, and the verification should be kept as part of the building's environmental health file.

Hazardous Waste Management: RCRA

Commercial facility operations produce waste that cannot go in the trash. Used oil, spent fluorescent lamps, batteries, solvents, and pesticides are classified as **hazardous waste** under federal law. Pouring waste down a drain, putting it in a dumpster, or leaving it on site creates real environmental harm and exposes the organization to serious penalties. The primary federal law covering hazardous waste is the **Resource Conservation and Recovery Act**, or **RCRA**, administered by the EPA.

RCRA uses a **cradle-to-grave** framework. The organization that creates the waste is responsible for it from the moment it is generated until it is properly treated or disposed of. That means correctly identifying hazardous wastes, labeling and storing them properly, keeping required records, and using only licensed transporters and disposal sites. That responsibility does not end when the waste leaves the building.

> **REGULATORY REQUIREMENT**
>
> RCRA's cradle-to-grave framework holds the waste generator responsible from the moment hazardous waste is created until it reaches a licensed disposal facility. That responsibility travels with the waste — it does not transfer to the transporter or the disposal contractor.
>
> Facility managers who use unlicensed transporters, store waste improperly, or fail to receive a signed manifest copy within 35 days remain liable under federal law. The EPA enforces RCRA violations with significant civil and criminal penalties.

Facilities are grouped under RCRA by how much hazardous waste they produce each month — from Very Small Quantity Generators (VSQGs) with the fewest requirements to Large Quantity Generators (LQGs) with the most. But quantity alone does not tell the full story. A hospital and an office building of the same size may both be LQGs, but for very different reasons. Healthcare facilities generate pharmaceutical and laboratory waste. Data

centers produce large volumes of battery and cooling system waste. Manufacturing operations contribute solvents, process chemicals, and metal-bearing waste. Facility managers must know both their generator category and the specific waste streams their operations produce. Generator categories, accumulation time limits, and common waste streams by facility type are summarized in **Table A.4** in the Appendix.

Waste must be stored correctly on site. Containers must be in good condition, closed when not in use, and labeled "Hazardous Waste" with a description of the contents. Storage areas must be inspected regularly and kept away from drains and ignition sources. Most generator categories cap how long waste can stay on site before it must be shipped out. Missing those deadlines is a common and costly compliance violation.

Facility managers should work with a licensed **hazardous waste disposal contractor** for regular pickups. Each shipment requires a **uniform hazardous waste manifest** — a tracking document that follows the waste to its final destination. Copies must be kept on file. If a signed copy from the disposal facility does not arrive within 35 days, the generator must investigate. This system ensures waste reaches a proper facility rather than being dumped illegally.

Chemical Storage and Spill Response

Every facility stores chemicals. Cleaning products, lubricants, fuels, paints, and refrigerants are present in most commercial buildings. How they are stored determines how much risk they create. Poor storage leads to accidental reactions, fires, spills, and exposure incidents that are entirely preventable.

The foundation of good chemical storage is **segregation by hazard class**. Chemicals that react dangerously must never be stored together. Flammable liquids must stay away from oxidizers. Acids must be kept from bases. Facility managers use SDS information and compatibility charts to determine safe storage arrangements. Storage areas should be labeled by hazard class, and access should be limited to trained staff.

Flammable and combustible liquids need special handling. They must be stored in approved flammable storage cabinets. Quantities kept in work areas should be limited to daily use amounts. Larger volumes belong in dedicated storage rooms with proper ventilation, bonding and grounding equipment, and appropriate fire suppression. Local fire codes set limits on how much flammable liquid can be stored in different building areas. Facility managers must know and follow those limits.

A **spill response program** prepares the facility to contain and clean up a chemical release quickly. Spill kits should be placed at or near chemical storage and use areas. Each kit contains absorbent materials, personal protective equipment, containment tools, and disposal bags suited to the chemicals stored nearby. Staff who work around hazardous chemicals must be trained to use the kits and follow the spill procedures for their area.

When a spill occurs, three steps must follow in order:

- **Protect people** — evacuate the area if needed; keep anyone without proper equipment out
- **Contain the spill** — stop the spread before it reaches drains or other areas

- **Clean up and dispose** — treat spill material as hazardous waste; follow disposal procedures

Some spills trigger regulatory reporting requirements. Facility managers must know the reporting thresholds for the chemicals in their buildings and be ready to notify the right agencies without delay.

Environmental Compliance Reporting

Managing environmental hazards well is only part of the job. Facility managers must also document their work and report to regulatory agencies on a schedule set by law. **Environmental compliance reporting** covers the records, notices, and reports that federal, state, and local rules require. Failing to report — even when environmental performance is sound — creates legal liability and invites regulatory scrutiny.

The most common reporting requirement for commercial facilities is the annual **Tier II report** under the **Emergency Planning and Community Right-to-Know Act**, or **EPCRA**. Facilities that store hazardous chemicals above certain amounts must file by March 1 each year. The report lists every covered chemical on site, its quantity, its location, and its hazard type. This information goes to state and local emergency planners and the local fire department so they know what to expect if they respond to an incident.

Facilities that discharge water through stormwater systems or cooling towers may need permits under the **Clean Water Act**. A **stormwater pollution prevention plan**, or **SWPPP**, describes how the facility keeps pollutants out of runoff. Some facilities need a permit under the **National Pollutant Discharge Elimination System**, or **NPDES**. Facility managers must know which discharge permits apply and keep up with their monitoring and reporting requirements.

Refrigerant management is another compliance area. The **Clean Air Act** sets rules for handling, recovering, and disposing of refrigerants. Technicians who work on equipment with regulated refrigerants must be certified. Leaks must be tracked, and facilities with large systems must repair leaks within set time limits. Records of all refrigerant purchases, recoveries, and disposals must be kept.

A **compliance calendar** lists every required report, its due date, the data needed, and who is responsible. It turns regulatory deadlines into a managed workflow and shows regulators that the facility treats compliance as a priority. Facility managers who build and follow a compliance calendar reduce the risk of missed deadlines and the penalties that come with them.

Key Points

- Asbestos and lead paint in pre-1980 buildings require a formal assessment plan before any renovation work begins
- Mold cannot be solved without first fixing the moisture source that allows it to grow
- RCRA holds the waste generator responsible from creation to final disposal regardless of who transports the waste
- Chemical storage safety depends on segregation by hazard class and properly maintained spill response kits

- A compliance calendar turns regulatory reporting deadlines into a managed, auditable workflow

Reflection Question

A facility manager at a 1965 office building is planning a renovation that will involve removing ceiling tiles and drilling into walls in several areas. No asbestos survey has ever been conducted. What steps must the facility manager take before any renovation work begins, and what risks does skipping those steps create?

Module Summary

Module 5 examined the facility manager's direct responsibility for the health, safety, and security of every person inside the building. Subtopic 5.1 established indoor environmental quality as an active management discipline — tracking air pollutants, meeting ASHRAE ventilation standards, and building monitoring programs that catch problems before occupants feel them. Subtopic 5.2 translated OSHA's legal framework into operational programs: HazCom, LOTO, confined space entry, and the inspection and incident documentation practices that keep those programs honest. Topics 5.3 and 5.4 moved from the physical layer — access control, surveillance, intrusion detection, barriers — to the procedural layer, where threat assessments, incident response protocols, and security audits turn hardware investments into a functioning security program. Subtopic 5.5 closed the module with the environmental hazards embedded in the building itself and in daily operations — asbestos, lead, mold, hazardous waste, and the compliance reporting obligations that follow each one. The operational systems that protect occupant health, safety, and security all depend on the work management infrastructure examined in Module 6 — from the CMMS work orders that track LOTO completions to the CAFM data that supports security zone mapping.

Learning Outcomes

1. Identify IEQ parameters and describe operational strategies to maintain healthy indoor environments
2. Explain key OSHA compliance requirements applicable to facility operations
3. Describe the components of a physical security system and manage security protocols
4. Develop a hazardous materials management plan for a commercial facility