JOIN THE WORKPLACE REVOLUTION

From Risk to Resilience

How Nordic facility management is shifting in a high-risk era

COOR

Facility Management is evolving into a strategic force for company resilience

Facility Management has evolved significantly from its' traditional role as a background support function. Since I stepped into the role of CEO at Coor Service Management, I have come to learn just how integrated and dynamic this field has become. Today, FM often serves as a vital enabler across many complex areas – ranging from workplace experience to AI and technology integration.

Over recent years, there has been a notable shift of security and resilience moving higher up the agenda. FM-professionals are often confronted with a broad spectrum of threats, including climate-related events, cyber risks, utility failure and more. To many organizations the risks are accumulating, becoming increasingly interconnected and more complex to address.

FM's role in this will require new capabilities, but also new alliances with functions both within and outside the organization. It's about more than just incident response – it's about overseeing business continuity, ensuring swift adaptability and preparedness, while protecting both people and assets. An integrated and strategic approach is essential for building environments where individuals and organizations not only feel safe but can also thrive, even in times of uncertainty.

With this report, Coor wants to shed light on the evolving risk landscape, its' impacts on FM, and key opportunities for strengthening company resilience. I hope the insights provided will help you address future challenges and build stronger, more secure organizations.

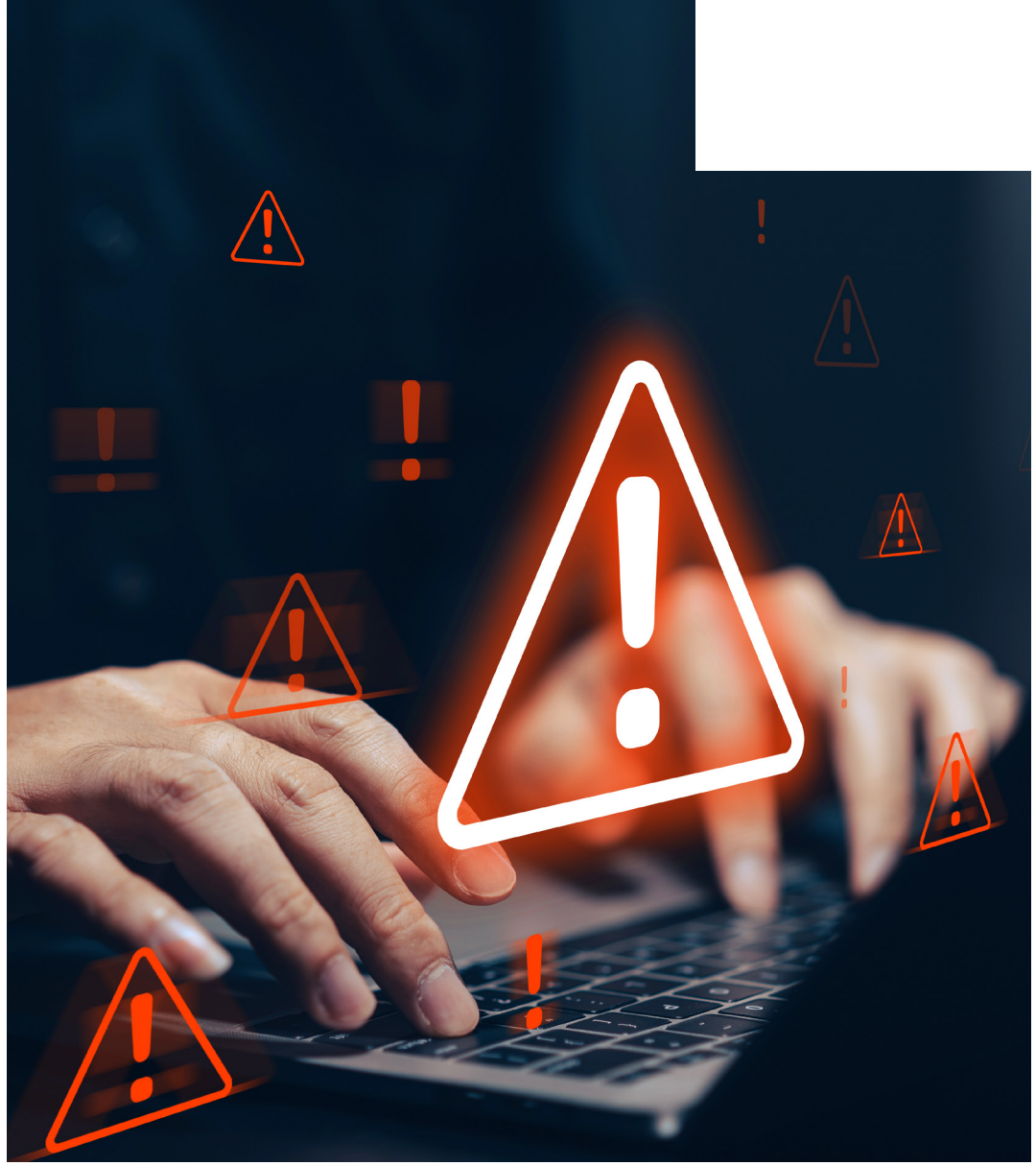
Ola Klingenborg
CEO, Coor

Content

1

Is your Real Estate and FM Built for Today's Threats?

Real estate and Facility Management have long been on the front-line of defence against threats facing the physical workplace, but in recent years the scale, speed and severity of the security threats facing companies, operations and corporate real estate is unprecedented.



From global pandemics and fractious geopolitics to extreme weather and digital vulnerability, the past five years has seen real estate and facilities management (REFM) teams battling against external threats from every direction. These threats are not only increasing in frequency but also shifting in form. From espionage and breaches in smart building systems to political activism and power grid disruptions, real estate and facilities leaders are being tested on multiple fronts.

According to a global research report by consultancy firm Verdantix[1], executives are taking broader action to reinforce buildings against both physical and cyber threats. More than 60% say they are strengthening physical security management plans (up from 46% in 2022) while 65% are bolstering cybersecurity efforts.

In response to this changing landscape, Coor conducted a comprehensive survey of 580 office workers and 575 REFM decision makers across the Nordic region. The findings reveal a market on high alert. Resilience to external risks and threats now ranks among the highest organisational concerns for REFM leaders across the Nordics, second only to health and safety compliance.

Cybersecurity, infrastructure failures, and environmental disasters top the list of threats, while confidence in organisational preparedness remains high – perhaps deceptively so. Despite this optimism, significant capability gaps persist in crisis planning, coordination, and strategic response. →

35%

of REFM leaders report weaknesses in crisis planning

32%

in unclear roles and responsibilities

[1] Verdantix, 2025. Global Corporate Survey: Real Estate Technology Budgets, Priorities & Preferences For 2025

Meanwhile, employees paint a very different picture of workplace priorities. While cyber incidents and health-related events are also high on their radar, personal safety con-cerns such as bomb threats and vandalism vary significantly depending on whether they work in urban or rural offices. Notably, only 11% of employees identified safety and access control as a top priority for workplace improvement, ranking it lower than noise levels, quiet areas, and better indoor air quality.

This divergence between organisational resilience planning and individual experience highlights a widening perception gap. For real estate leaders, the task ahead is not only to defend infrastructure from rising threats but to build trust among occupants and con-nect macro-level strategy with day-to-day comfort and wellbeing.

Across the Nordic region, national and sectoral differences present further divides. Denmark showed the highest levels of concern for workplace threats with 57% of decision makers reporting that threat levels have increased in the past two years; Sweden and Norway sit in the middle with 51% of decision makers saying threat levels have in-creased and Finland expressed the least with 47% claiming threat levels have increased. Technology organisations were the most sensitive to safety and compliance, while organisations with their main facilities in mid-city locations felt the increase in risk most.

As new roles emerge in cybersecurity, emergency response and cross-depart-mental governance, the future of REFM lies in navigating this complexity with confi-dence, clarity and collaboration. This report explores how Nordic organisations are meeting the challenge, where vulnerabilities remain, and how REFM teams of the future are becoming foundational for organisations in responding, mitigating and preventing future threats. ■

52%

Incresed threat level over last 2 years

Perceived by REFM decision makers in the Nordics

2026 top priorities related to company real estate and workplace

According to REFM decision makers in the Nordics (selected areas out of long-list of possible priorities)

2

A New Age of Risk

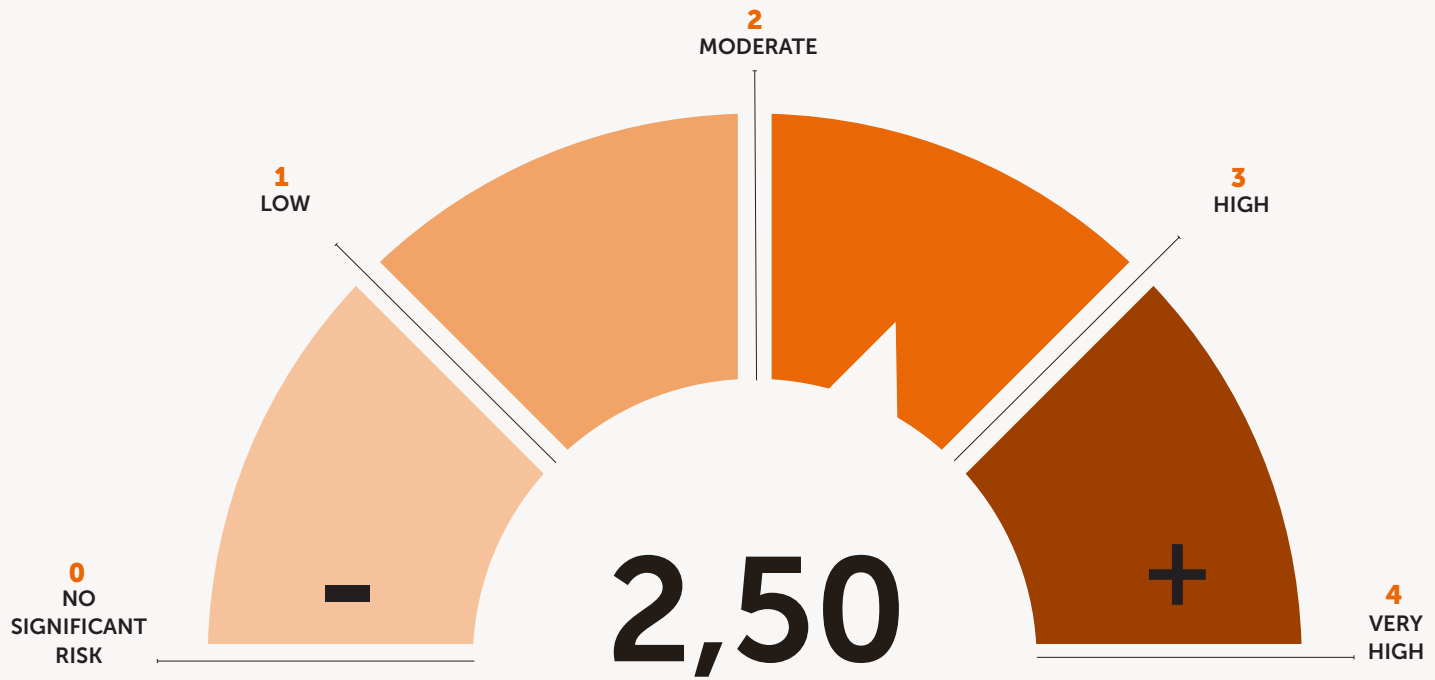
We have entered an era of heightened risk. Natural disasters, cyberattacks, political unrest, and pandemics have now become part of the operating environment for every organisation. For REFM professionals, this signals a profound shift in both mindset and responsibility.

Traditional approaches built around cost-efficiency and operational maintenance are being supplemented by a growing need to anticipate and respond to a diverse range of threats. This chapter explores seven key categories of emerging external risks that are likely to impact the future role of Facility Management:

1. **Environmental and natural disasters** – with extreme weather becoming more common, organisations will need to build resilience in their physical real estate portfolios as well as operational preparedness to keep individuals safe.
2. **Crime and vandalism** – as buildings become more open and multifunctional, physical security is under renewed pressure. At the same time, many companies see a significant risk related to espionage, individual targeted attacks and organised crime.
3. **Terrorism and civil unrest** – geopolitical volatility is exposing new vulnerabilities in workplace access, safety, and brand reputation.
4. **Cyber and technological threats** – the convergence of digital and physical systems, and the increasing emergence of AI, is placing greater risk on vulnerable cyber security systems.
5. **Infrastructure and utility failures** – as systems become more electrified, they are subject to power grid disruptions. This risk is turning energy resilience and contingency planning into board-level concerns.
6. **Regulatory and compliance risks** – rising scrutiny, new legislation and directions around security and privacy are increasing the risk of incompliance.
7. **Health and biological threats** – post-pandemic, health resilience has maintained as a continued threat against infections and viral outbreaks. →

Model: Risk index per category

Perceived risk severity to company organization
(Weighted score of 0-4, Nordic REFM decision makers)



The risk profiles for different organisations are increasingly diverse, shaped by sector, geography, and operational context. The spectrum of potential threats is wide-ranging, and the degree of exposure varies considerably across different environments. For instance, the vulnerabilities facing a high-density urban office building will be different to those of a rural manufacturing facility.

In addition, some companies are subject to existing national security and preparedness regulations such as the Protective Security Act to safeguard critical information and infrastructure. These companies are often in critical infrastructure sectors, such as finance, defence and government, and they are more advanced in their strategies and structures for dealing with these threats. →

REFM Commonplace	Areas expanding FM role
• Structural flood- and snow proofing	• Facility resilience policies
• Power and HVAC-back-up systems	• Monitoring sensors and alert systems
• Service continuity (e.g. snow/ice removal, hygiene, catering)	• On-site staff protocols and drills
• Emergency signage and evacuation route marking	• Emergency vendor support
	• Risk assessment and audit reviews

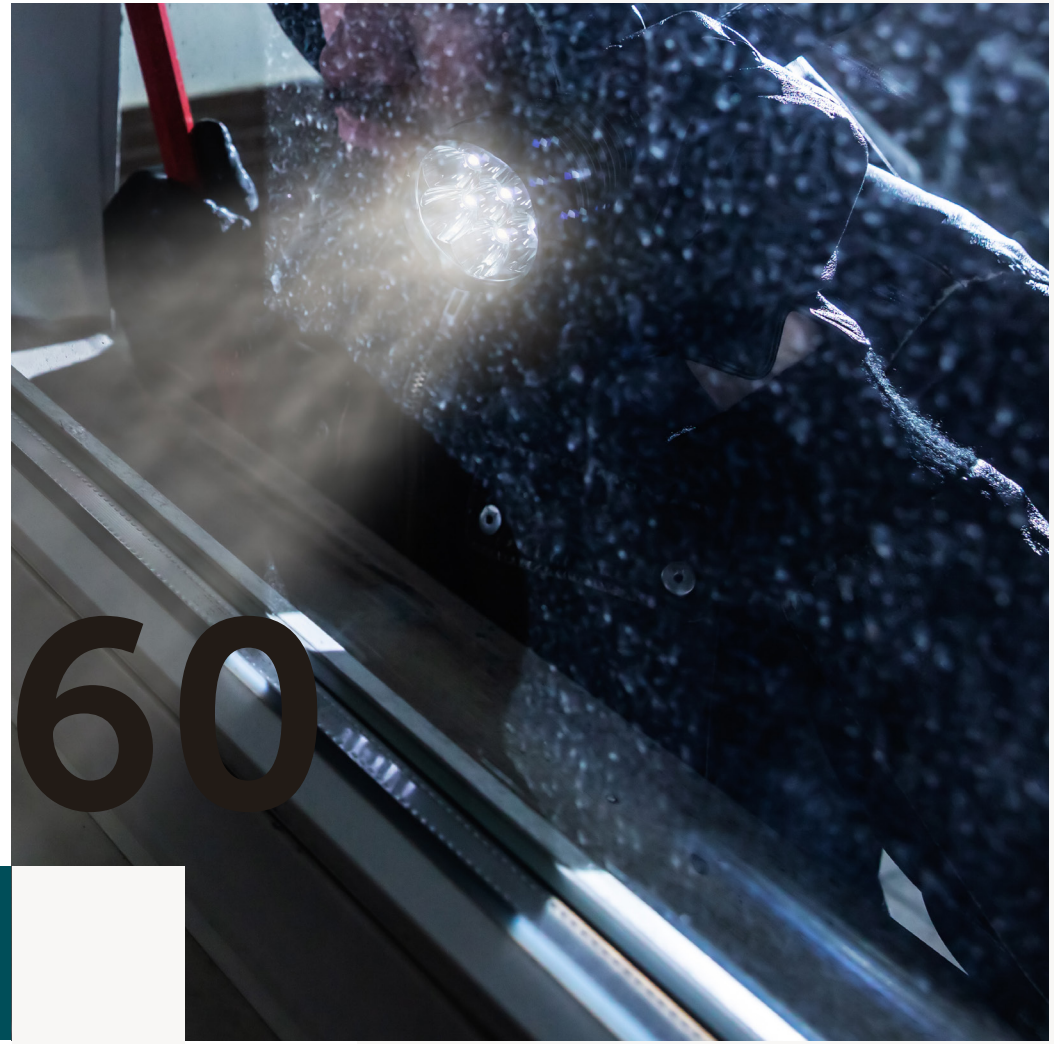
Environmental and Natural Disasters

Extreme weather is accelerating. The UN World Meteorological Organisation recorded 151 record-breaking climate events in 2024, including 25 in the Nordics[2]. This volatility is pushing FM from 'just-in-time' operations towards 'just-in-case' resilience planning. According to our survey, 54% of Nordic REFM leaders view natural disasters as a serious threat.

The challenge is global a global one. The real estate company JLL estimates 37% of commercial real estate – equivalent to US$580 billion – sits in the ten most climate-vulnerable cities. For FM, system and infrastructure resilience has become a core responsibility. Investment is required in both emergency response systems and longer-term climate adaptation. Continuity planning is also expanding beyond internal teams to include local emergency services and external partners.

Two-thirds (64%) of decision makers believe they are prepared for natural disasters, but with weather extremes set to intensify, resilience is now a strategic priority. For FM, the implication is clear: ensure structural redundancy, develop robust continuity plans, and forge partnerships that extend resilience beyond the walls of the building. ■

[2] World Meteorological Organisation, 2024. Extreme Weather Events 2024.



2,60

Crime and Vandalism

Workplaces are becoming more open and multifunctional – and, as a result, more vulnerable. Threats now range from petty theft to targeted sabotage and organised crime, particularly at logistics hubs, public sites, and critical infrastructure. Individuals can also be targets, requiring stronger personal protection.

According to our survey, 57% of REFM leaders see crime and vandalism as a serious risk, making it the third biggest threat on the 'Threat Index' scale. The risk rises to 59% in industry and manufacturing sectors and 61% in large cities. FM teams are responding by broadening beyond physical security technology: introducing vendor vetting, sharing crime-pattern intelligence, and training frontline staff, such as receptionists, in security protocols.

Safety can no longer just rely on locks and cameras. FMs must integrate with law enforcement, manage vendor integrity, and build staff capabilities to keep workplaces safe while remaining accessible. ■

REFM Commonplace	Areas expanding FM role
• Locks, alarms, and CCTV coverage • Access points and perimeter lighting • Reception desk and visitor logging • Incident reporting procedures	• Integrated access control and cross-functional data intelligence • Guard patrol coordination and incident reporting tools • On-site vendor security vetting and background checks • Collaboration with police and local safety networks • Employee awareness and de-escalation training

Terrorism and Civil Unrest

From activism and targeted violence to terrorism and civil unrest, organisations are increasingly exposed to the political and social tensions shaping today's world. According to Allianz's 2025 Risk Barometer, political violence remains one of the top 10 global business risks. Since 2017, more than 800 significant anti-government protests have taken place across 150 countries, with over 160 major events recorded in 2024 alone. Around 18% of these lasted more than three months, disrupting business continuity and amplifying uncertainty[3].

Unlike natural disasters, the location, scale, and duration of acts of terrorism are harder to predict, making it more difficult for organisations to develop reliable contingency strategies. The consequences extend beyond physical damage. Terrorist activity can lead to significant business interruption, denial of access, social disruption and long-term reputational harm. Facilities and security teams are increasingly responsible not only for securing buildings and safeguarding employees, but for preserving brand integrity and ensuring uninterrupted operations.

In the Nordics, senior REFM leaders are seeing this shift firsthand. Over half (55%) of decision-makers report terrorism and civil unrest as a serious concern. In a series of interviews with a panel of senior REFM decision makers, one respondent from a major manufacturing plant reported that disruption from activists occasionally led to the company needing to collaborate with police, HR, and security personnel in real time. Another decision-maker from a large Nordic bank reported that recent incidents have prompted a reconfiguration of site lockdown routines and heightened alert levels, commenting that "we're afraid terrorism can use activist fronts to attack our real estate".

Many organisations are now moving from reactive confrontation to proactive 'controlled transparency' – striking a careful balance between protecting staff and maintaining openness. As the political climate continues to intensify, workplaces must build greater resilience not just to withstand unrest, but to operate safely and confidently within it. ■

[3] Allianz Commercial, 2025. Political violence and civil unrest trends 2025

REFM Commonplace	Areas expanding FM role
• Lockdown procedures for premises • Assembly point designation • Event-specific access control	• Enhanced perimeter security and crowd management • Security coordination with public authorities • Crisis communication protocols and drills for staff • Monitoring tech for real-time public threat alerts

2,46

2,81

Cyber and Technological threats

As workplaces become more connected, the cyber threat landscape is expanding rapidly. Cybersecurity is no longer the domain of IT alone; it now intersects with physical infrastructure, building systems, and operational continuity. A breach can compromise access control as easily as it can leak sensitive data.

According to our survey, 66% of REFM leaders rank cyber and technology risks as their most pressing concern – placing it at the top of the Threat Index. Interviews with senior leaders highlighted risks around both external fraud and insider threats, particularly in high-security industries such as banking and manufacturing. Several organisations have established dedicated cybersecurity units within IT, yet FM is increasingly integrated into these efforts, for example by pursuing ISO certifications to strengthen facility-linked protection.

The latest *Nordic Threat Landscape 2024* report by cyber intelligence company SOCRadar underscores the scale of the challenge.[4] The report recorded 343 dark web mentions of Nordic countries, 105 ransomware attacks (41% in Sweden), and a surge in phishing incidents targeting Finland and Sweden. Manufacturing and information services were the most exposed sectors.

This environment is reshaping FM's role. Already, 36% of decision-makers say FM plays a critical part in cyber-physical security, with 39% expecting that role to grow. Large Nordic firms are leading the way, collaborating with IT to vet digital infrastructure, simulate attack scenarios, and strengthen smart building resilience. FM is also extending its remit beyond systems to people by overseeing vendor compliance, training frontline staff, and embedding cyber hygiene into daily operations at the physical–digital edge.

Cyber threats are an urgent risk for REFM. To stay ahead, FM must own the physcal–digital interface – ensuring systems, vendors, and staff behaviours collectively uphold resilience. ■

REFM Commonplace	Areas expanding FM role
• Secure server rooms / physical IT infrastructure • Building automation system (BAS) security • Access control system management	• Monitoring and cyber–physical threat detection in connected systems • Staff and vendor cyber etiquette and compliance training • Incident support for cyber-related facility disruptions

[4] SoRadar, 2024. Nordic Threat Landscape Report 2024.

REFM Commonplace	Areas expanding FM role
• Generator and UPS backup • Water and heating system redundancy • Lighting backup systems	• Real-time utility monitoring and automated shutoffs • Alternative energy sourcing and storage • Cross-site contingency planning for service continuity

Infrastructure and Utility Failures

As systems grow smarter and more interdependent, workplaces are increasingly vulnerable to infrastructure and utility failures. Risks range from power grid disruptions to water supply interruptions and heating outages.

In the survey, 58% of REFM leaders cited infrastructure and utility failures as a critical risk, making it the second highest on the Threat Index. Industrial and manufacturing firms report the strongest preparedness (73%), while rural facilities feel less confident than their urban counterparts. Leaders pointed to geopolitical shocks – such as power outages in Spain and Ukraine – as drivers of heightened awareness.

Nordic infrastructure is particularly fragile. ENTSO-E, the European network of transmission system operators, has flagged vulnerabilities in Nordic power grids during winter peaks when renewable inputs are stretched[5]. Organisations are responding by investing in utility resilience through uninterruptible power supply (UPS) batteries, diesel generators, spare-part 3D printing, and alternative energy sources.

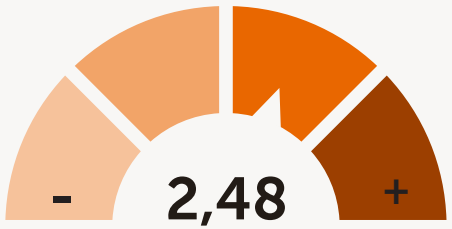
This shift places FM at the centre of infrastructure risk management. With 32% of decision-makers predicting a growing role for FM in infrastructure risk management, the pressure is on to balance cost control with operational foresight. Beyond reactive fixes, FM leaders are expected to plan for redundancy across sites, secure continuity of utilities, and balance cost with operational foresight.

Infrastructure resilience is a board-level concern. FMs must anticipate systemic failures, diversify suppliers, and design redundancy into both facilities and utilities to safeguard continuity. ■

[5] Entsoe, 2025. Summer Outlook Report 2025.

2,63

RISK INDEX



REFM Commonplace	Areas expanding FM role
• Fire code compliance and drills • Accessibility standards adherence • Environmental compliance for facilities • Health & safety inspections	• Site-level risk audits and third-party oversight • Staff safety & compliance training • Compliance reviews and integrated reporting – ESG, data, security, etc.

Regulatory and Compliance Risks

The regulatory environment is expanding, particularly in the Nordics where regulation is becoming stricter and there is new pressure from 'proof of compliance' requirements. In our survey, 52% of REFM leaders cited compliance risks as critical, rising to 61% in technology and services sectors.

EU-level directives are reshaping expectations. The Network and Information Security Directive 2 (NIS2, 2024) and GDPR (2018) require FM to lead risk assessments, incident response planning, and third-party oversight for data security. National frameworks such as the Security Protective Act further mandate background checks and security vetting, with FM often responsible for implementation. Sector-specific regulations add complexity. The Digital Operational Resilience Act (DORA), primarily targeting the financial sector, has significantly raised requirements around digital and data handling.

Beyond binding regulation, FM must also track new standards and evolving agendas on fire safety, work environment, building codes, and ESG reporting. The result is a fragmented and shifting landscape, where FM acts as a key enforcer of compliance across physical and digital systems. Industry leaders have even called for a unified 'total security and resilience standard' to simplify governance.

Compliance is not a box ticking exercise. FMs must integrate multiple overlapping frameworks, enforce vendor compliance, and ensure resilience across both operational and cyber-physical domains. ■

2,48

2,51

REFM Commonplace	Areas expanding FM role
• Routine cleaning and hygiene standards • Air quality monitor-ingring and ventila-tion • Hygiene signage and supplies	• Broader health risk protocols, readiness plans and PPE stockpiling • Advanced air filtration and sensor systems • Health & safety compliance for vendors • Crisis communi-cation on health incidents

Health and Biological threats

Health risks – from viral outbreaks to indoor air quality – remain central to FM since COVID-19. In our survey, 55% of leaders rated health and biological threats as a significant concern. Risks include pandemics, but also persistent issues such as mould, airborne contaminants, and rising scrutiny of ventilation standards. Poor air quality alone is linked to absenteeism and reduced cognitive performance.

The pandemic shifted FM from 'just-in-time' to 'just-in-case' operations. Facilities teams expanded storage, upgraded protocols, and coordinated more closely with clinical and operational leaders. As one FM decision maker noted, 'During the pandemic the business owners in the organisation set up the standards, but FM provided and coordinated the roll out.'

Global reports reinforce the importance. The World Economic Forum and Global Health Council flagged infectious disease outbreaks as one of the most severe public health risks in 2024[6]. This underlines the need for continued surveillance, upgraded environments, and rapid response systems.

Health resilience is now a permanent FM responsibility. Facilities leaders must embed robust ventilation, hygiene protocols, and agile response capabilities to protect workforce wellbeing and maintain continuity. ■

[6] World Economic Forum, 2024. The Global Risks Report 2024.

3

The Impact on Facilities Management

As organisational risks multiply, FM's role is expanding from incident response to integrated resilience. Facilities teams are now expected to do more than manage buildings – they must enable continuity, coordinate crisis response, and safeguard people and operations in increasingly complex environments.

This transition brings both opportunity and challenge. FM is recognised as a connector in cross-functional resilience planning, yet its changing identity creates tensions. Expectations are rising while resources remain constrained. FM's contributions are increasingly strategic, yet often underappreciated. Collaboration with IT, HR, legal, procurement, and corporate strategy is critical, but accountability for resilience frequently remains unclear. At the same time, FM must balance competing priorities including protecting employees, securing assets, and preserving a positive workplace experience.

In the Nordic market, resilience, digital threat management, and cross-functional preparedness are becoming strategic imperatives. Some organisations have well-integrated FM and security functions; others remain fragmented and reactive. While REFM leaders express confidence in their capabilities, employees remain focused on day-to-day workplace needs. Closing this gap between systemic readiness and individual experience will be critical to building organisational resilience.

From operator to integrator

Facilities Management is evolving from its traditional role as an operator – historically focused on physical security, building infrastructure, and workplace operations – into a proactive integrator and coordinator of organisational resilience. This shift reflects a growing need to traverse new domains, including IT and data, HR, and procurement, while becoming more involved in tactical and strategic security matters and teams.

This shift is reflected in the data. While 45% of decision-makers still identify FM's primary role as managing physical security and →

"FM sits close to leadership - we know what's happening across the site and across functions. That coordination is our strength."

– REFM responsible for a large Nordic manufacturing company.

infrastructure, 39% now highlight FM's involvement in IT and digital systems. Nearly half (47%) expect closer FM–IT collaboration, and 35% anticipate deeper integration with crisis management.

FM is evolving from operator to integrator – connecting domains such as IT, HR, procurement, and legal. Leaders describe FM as the 'site commander,' uniquely positioned to oversee interconnected systems and coordinate responses.

Stretching the limits of traditional FM

As Facilities Management takes on a more strategic and integrated role, the path forward is not without obstacles. Many FM teams are being asked to do more, but with less. Expanding responsibilities across physical security, utilities, compliance, and crisis coordination are often not matched by increased investment, clearer mandates, or greater visibility within senior leadership.

This challenge is echoed across the Nordic region. In interviews, multiple FM leaders explained that under-resourced teams are expected to manage increasingly complex sites and systems. As one senior FM decision maker commented, 'We have a small FM team managing a 1-million-square-metre site.' Without adequate resourcing or organisational support, FM risks being overstretched and undervalued – just as its strategic importance reaches a new level.

As FM's influence expands, questions of ownership and decision-making persist. How far should FM's remit extend into adjacent domains, and how can it balance its foundational operational responsibilities with its growing role as a strategic integrator of security and resilience?

Real progress will depend on a step change in how organisations structure and empower FM. This means not only clarifying roles and responsibilities across departments, but also embedding FM more firmly in strategic implementation at board level. Advances in cross-functional collaboration, data-driven management, and investment in new skills will be essential. If these shifts take place, FM can evolve from being a stretched support function into a central integrator of resilience, sustainability, and workplace strategy – unlocking its full potential as a driver of organisational performance and change.

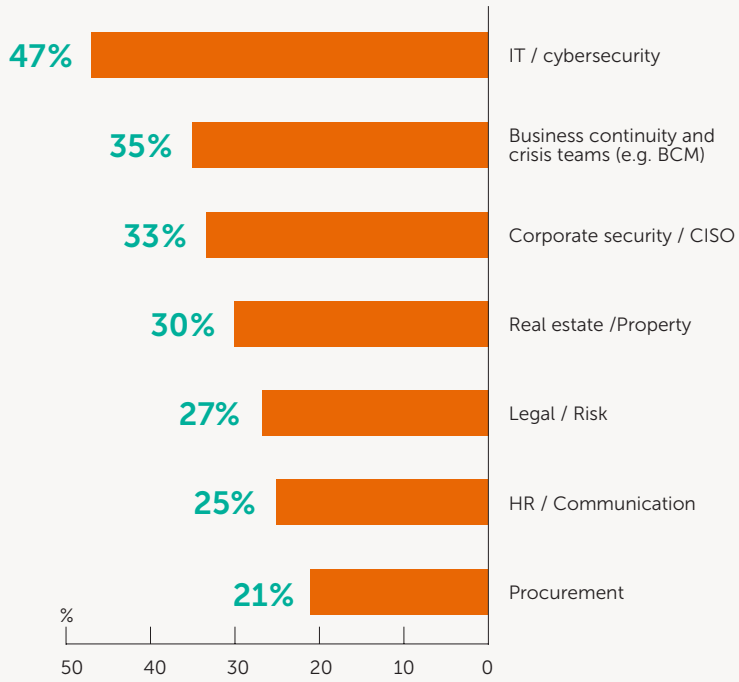
Forming new capabilities and alliances

In FM's new role as an integrator, strategic changes need to occur across the organisation. The FM function is being drawn into new alliances across different disciplines. Yet collaboration often remains inconsistent and siloed, limiting FM's ability to respond swiftly and holistically to disruption.

In the future, collaboration across the entire organisation is inevitable. For Facilities Management, the biggest increases in collaboration are expected with IT and cybersecurity (47%), business continuity and crisis teams (35%), and corporate security (33%). →

Organizational functions where FM collaboration is foreseen to increase the most

(according to REFM decision makers in the Nordic)



Some organisations are already breaking down silos to achieve this. While there is no universal blueprint for FM to follow, and collaboration varies by business, examples are emerging. As one FM decision-maker puts it: 'We oversee preparedness and business continuity across organisational functions. It only works because we're plugged into IT, security, and operations.'

Other examples of progress emerged from the research including a Nordic bank which has FM leading physical security while partnering with IT on cyber resilience. And a logistics firm which involves FM in setting infrastructure and access standards across hundreds of locations. And a manufacturer embeds FM directly in crisis management, coordinating with HR, sustainability, and IT.

However, greater integration requires more than collaboration alone – it also demands stronger in-house capabilities within FM. While there are many changes that are pushing traditional FM capabilities forward, the two most imminent shifts are:

- **Strategic continuity:** FM is expected to develop resilience plans that integrate physical assets, operational continuity, and vendor readiness – not merely execute directions from corporate security or risk teams. This positions FM as an active driver of continuity planning.
- **Physical–digital ownership:** In smart buildings, FM operates partly as IT. The function must oversee vendor cyber compliance, secure connected building systems, and drive staff awareness of cyber hygiene at the physical–digital interface.

Both areas demand new skills, governance structures, and leadership backing. Without mandate clarity, FM's ability to act will be undermined, leaving resilience fragmented.

Balancing workplace culture with security

Security and protection are now core FM priorities, but they bring a new dilemma of how to safeguard people and assets without undermining workplace culture.

Survey data shows the divide. While 28% of decision-makers list security upgrades as a top workplace priority, only 11% of employees agree, favouring comfort, quiet, and better amenities. This disconnect exposes the risk of creating environments that feel overly restrictive.

Leading organisations are reframing their approach. At a Nordic bank, FM deliberately keeps many security measures 'invisible' to avoid a sense of lockdown. As one facilities head put it: 'You can't build a vibrant workplace when everything feels like lockdown – but the threats are real and we have to manage that.'

In the new and expanded role of FM, leaders must design secure but human environments – blending robust protection with positive employee experience. The ability to manage perception is now as critical as the ability to manage infrastructure. ■

4

A Framework for Resilience

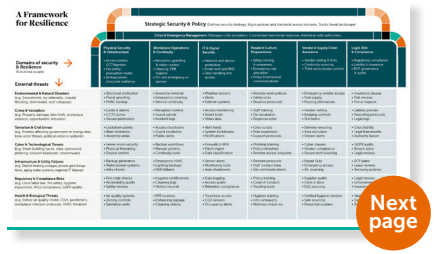
In response to the growing pressures and complexities facing Facility Management, there is an urgent need for a more structured approach that reflects FM's expanded role across multiple risk domains and its growing interdependence with other departments.

An emerging framework seeks to provide guidance for this evolving landscape. Rather than proposing that FM assume full ownership of every threat response, the framework recognises the workplace as a complex, collaborative ecosystem. It offers guidance for how FM can work alongside IT, HR, legal, procurement, security, and sustainability teams to create a more holistic and integrated roadmap for organisational threat resilience.

Looking into the framework, FM most commonly sits within two traditional responsibilities: physical security and infrastructure and workplace operations and continuity. However, as threats become more interconnected, FM's role is shifting sideways into adjacent domains such as IT, HR, and procurement and upwards into more strategic involvement in security governance, overall preparedness and crisis management.

In some cases, FM is assuming direct responsibility for these areas; in others, it is collaborating closely with specialist functions to coordinate an integrated response.

The goal is to move beyond reactive service delivery toward a model of shared responsibility and clarify where FM should lead, where it should support, and how it can facilitate coordination across siloes. By outlining key responsibilities and points of collaboration, this framework aims to empower FM to become not just a maintainer of buildings and workplaces, but a strategic enabler of company resilience.



A Framework for Resilience

Domains of security & Resilience (functional scope) →

External threats ↓

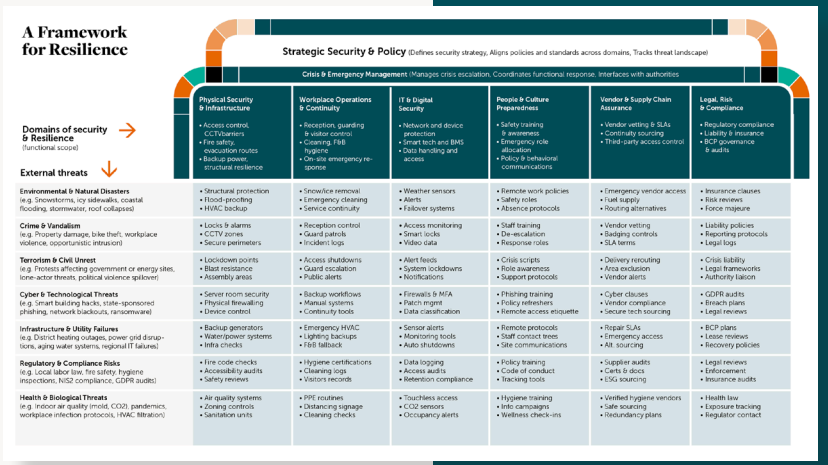
	Physical Security & Infrastructure • Access control, CCTVbarriers • Fire safety, evacuation routes • Backup power, structural resilience	Workplace Operations & Continuity • Reception, guarding & visitor control • Cleaning, F&B hygiene • On-site emergency response	IT & Digital Security • Network and device protection • Smart tech and BMS • Data handling and access	People & Culture Preparedness • Safety training & awareness • Emergency role allocation • Policy & behavioral communications	Vendor & Supply Chain Assurance • Vendor vetting & SLAs • Continuity sourcing • Third-party access control	Legal, Risk & Compliance • Regulatory compliance • Liability & insurance • BCP governance & audits
Environmental & Natural Disasters (e.g. Snowstorms, icy sidewalks, coastal flooding, stormwater, roof collapses)	• Structural protection • Flood-proofing • HVAC backup	• Snow/ice removal • Emergency cleaning • Service continuity	• Weather sensors • Alerts • Failover systems	• Remote work policies • Safety roles • Absence protocols	• Emergency vendor access • Fuel supply • Routing alternatives	• Insurance clauses • Risk reviews • Force majeure
Crime & Vandalism (e.g. Property damage, bike theft, workplace violence, opportunistic intrusion)	• Locks & alarms • CCTV zones • Secure perimeters	• Reception control • Guard patrols • Incident logs	• Access monitoring • Smart locks • Video data	• Staff training • De-escalation • Response roles	• Vendor vetting • Badging controls • SLA terms	• Liability policies • Reporting protocols • Legal logs
Terrorism & Civil Unrest (e.g. Protests affecting government or energy sites, lone-actor threats, political violence spillover)	• Lockdown points • Blast resistance • Assembly areas	• Access shutdowns • Guard escalation • Public alerts	• Alert feeds • System lockdowns • Notifications	• Crisis scripts • Role awareness • Support protocols	• Delivery rerouting • Area exclusion • Vendor alerts	• Crisis liability • Legal frameworks • Authority liaison
Cyber & Technological Threats (e.g. Smart building hacks, state-sponsored phishing, network blackouts, ransomware)	• Server room security • Physical firewalling • Device control	• Backup workflows • Manual systems • Continuity tools	• Firewalls & MFA • Patch mgmt • Data classification	• Phishing training • Policy refreshers • Remote access etiquette	• Cyber clauses • Vendor compliance • Secure tech sourcing	• GDPR audits • Breach plans • Legal reviews
Infrastructure & Utility Failures (e.g. District heating outages, power grid disruptions, aging water systems, regional IT failures)	• Backup generators • Water/power systems • Infra checks	• Emergency HVAC • Lighting backups • F&B fallback	• Sensor alerts • Monitoring tools • Auto shutdowns	• Remote protocols • Staff contact trees • Site communications	• Repair SLAs • Emergency access • Alt. sourcing	• BCP plans • Lease reviews • Recovery policies
Regulatory & Compliance Risks (e.g. Local labor law, fire safety, hygiene inspections, NIS2 compliance, GDPR audits)	• Fire code checks • Accessibility audits • Safety reviews	• Hygiene certifications • Cleaning logs • Visitors records	• Data logging • Access audits • Retention compliance	• Policy training • Code of conduct • Tracking tools	• Supplier audits • Certs & docs • ESG sourcing	• Legal reviews • Enforcement • Insurance audits
Health & Biological Threats (e.g. Indoor air quality (mold, CO2), pandemics, workplace infection protocols, HVAC filtration)	• Air quality systems • Zoning controls • Sanitation units	• PPE routines • Distancing signage • Cleaning checks	• Touchless access • CO2 sensors • Occupancy alerts	• Hygiene training • Info campaigns • Wellness check-ins	• Verified hygiene vendors • Safe sourcing • Redundancy plans	• Health law • Exposure tracking • Regulator contact

Guide to using this framework

Step 1

Map Key Functions

• Identify the organisational functions linked to resilience domains (e.g. Business Owners, Corporate Security/ CISO, Real Estate, HR, IT/ Cybersecurity, Communications, Procurement, Legal, Risk, Crisis/Continuity teams).



Step 2

Benchmark Against Governance

• Compare the framework with existing governing documents.

• Highlight where ownership and responsibilities are formalised – and where gaps remain.

Step 3

Run a Stakeholder Workshop

Bring key functional stakeholders together to assess readiness and shape future needs:

• Define 5–10 critical threat scenarios (e.g. grid blackout at site X, access control system failure, protestors at main entrance).

• Explore the most important countermeasures, aligned to resilience domains.

• Assign collaboration roles (strategic owners, lead executors, supporting teams).

• Review the structural need for forums or teams to ensure readiness (planning reviews, coordinated implementation, rapid response teams).

Step 4

Integrate into the Resilience Agenda

• Embed relevant parts of the framework into your organisational resilience strategy.

• Assign clear ownership for each element.

• Commit to regular reviews and continuous improvement over time.

5

Is Your Organisation Prepared?

Facility Management is no longer just about keeping the lights on. It's about keeping the organisation moving through disruption, uncertainty and change. From environmental shocks and cyberattacks to health crises and civil unrest, today's risks demand leadership that is integrated, proactive, and deeply collaborative.

As different disciples come together, they should be asking themselves key questions to ensure organizational readiness in an evolving threat landscape:

1. What is your current biggest concern related to FM, risk and company resilience?

2. Which threats has your organisation deemed to be most critical across company facilities, operations, information and people?

3. What mitigating measures and response plans have been put in place to manage these?

4. How are responsibilities distributed across your organisational functions and what role is FM carrying in terms of ownership, coordination, direct response, etc.

5. Which are your three most important development areas to strengthen company readiness for future threats?

These are not hypothetical questions. They are the difference between resilience and vulnerability, recovery and collapse. In a world where disruption is the new constant, Facility Management is not an afterthought, it's a frontline force in future-proofing your businesses.

The next crisis may not wait. Will your workplace be ready? ■

Methodology

This report combines quantitative survey data with qualitative expert insights to provide a comprehensive view of the evolving real estate and facilities management (REFM) landscape across the Nordic region.

An anonymous survey was conducted with 1,155 respondents, comprised of 575 real estate and facilities management decision-makers, representing leadership roles with responsibility for workplace, security, and operational strategies, and 580 employees, providing a perspective on workplace experience and organisational preparedness from the end-user standpoint.

Respondents were evenly distributed across Sweden, Norway, Denmark, and Finland, ensuring a balanced regional representation. The survey captured a cross-section of 12 industries, including banking and financial services, healthcare, manufacturing, production, technology, logistics, and more. Organisations spanned across large metropolitan areas, midsized cities, and rural locations.

To complement the survey findings, in-depth interviews were conducted with 5 senior decision-makers across the banking, production, healthcare, and manufacturing sectors. These interviews provided contextual insights into how leading organisations are responding to evolving workplace threats, building resilience strategies, and redefining the role of Facility Management. ■

Sources:
• Allianz Commercial, 2025. Political violence and civil unrest trends 2025. • Entsoe, 2025. Summer Outlook Report 2025.
• JLL, 2024. From Climate Risk to Climate Resilience. • SoRadar, 2024. Nordic Threat Landscape Report 2024.
• Verdantix, 2025. Global Corporate Survey: Real Estate Technology Budgets, Priorities & Preferences For 2025
• World Economic Forum, 2024. The Global Risks Report 2024. • World Meteorological Organisation, 2024. Extreme Weather Events 2024.

ABOUT COOR

Coor is one of the Nordic region's leading providers of Facility Management.
We deliver service solutions with heart and mind – safely, efficiently, and with care in every detail. With competence, commitment, and flexibility, we create value for people and businesses. Our 12,000 employees make a difference. Every day, all year round, across the Nordics.

Learn more about us www.coor.com

ABOUT WORKTECH ACADEMY

WORKTECH Academy is the leading global research platform and member network exploring how we'll work tomorrow. We look at innovation in the world of work and workplace through five key streams: people, place, technology, design and culture. We engage with our powerful network of over 14,000 individual subscribers and more than 90 corporate, design and technology organisations around the world to deliver content on the latest trends, research and best practice in work and workplace.

www.worktechacademy.com

Join the Workplace Revolution is a series of Nordic surveys initiated by Coor to monitor and understand trends in the world around us.

We can support you on your FM-journey!

For more inspiration, please visit
coor.com/our-services/workplace/JTWR-2025-from-risk-to-resilience/

Christer Olsson
Commercial
Coor Sweden
christer.olsson@coor.com

Trine Hagfors
Commercial
Coor Norway
trine.hagfors@coor.com

Jesper Oelert-Pedersen
Commercial
Coor Denmark
jesper.oelert-pedersen@coor.com

Matias Bäckström
Commercial
Coor Finland
matias.backstrom@coor.com

Oscar Stjernborg
Report editor
Coor Group
oscar.stjernborg@coor.com

A report by Coor
in partnership with WORKTECH Academy

COOR WORKTECH ACADEMY