JOIN THE WORKPLACE REVOLUTION

Fra risiko til motstandskraft

Hvordan nordisk eiendoms- og facility management-sektor endrer seg i en uforutsigbar tid

COOR

Facility Management utvikler seg til å bli et strategisk verktøy for virksomheters motstandskraft

Facility Management (FM) har utviklet seg betydelig fra sin tradisjonelle rolle som en usynlig støttefunksjon. Siden jeg tiltrådte som CEO i Coor Service Management, har jeg erfart hvor integrert og dynamisk dette området har blitt. I dag fungerer FM ofte som en avgjørende muliggjører på tvers av mange komplekse områder – fra arbeidsplassopplevelse til integrasjon av kunstig intelligens og teknologi.

De siste årene har vi sett et tydelig skifte der sikkerhet og motstandskraft har rykket høyere opp på agendaen. FM-profesjonelle står i økende grad overfor et bredt spekter av trusler, inkludert klimarelaterte hendelser, cyberrisikoer, infrastruktursvikt og mer. For mange organisasjoner akkumuleres risikoene, de blir stadig mer sammenvevde – og mer komplekse å håndtere.

FMs rolle vil kreve nye ferdigheter og kompetanser, men også nye allianser med funksjoner både innenfor og utenfor organisasjonen. Det handler om mer enn hendelseshåndtering – det handler om å sikre forretningskontinuitet, rask tilpasningsevne og beredskap, samtidig som man beskytter både mennesker og verdier. En integrert og strategisk tilnærming er avgjørende for å bygge miljøer der både enkeltpersoner og organisasjoner ikke bare føler seg trygge, men også kan utvikle seg – selv i usikre tider.

Med denne rapporten ønsker Coor å belyse det skiftende risikolandskapet, konsekvensene for FM og de viktigste mulighetene for å styrke virksomheters motstandskraft. Jeg håper innsiktene vil hjelpe dere å møte fremtidige utfordringer og bygge sterkere, tryggere organisasjoner.

Ola Klingenborg
CEO, Coor

Innhold

1

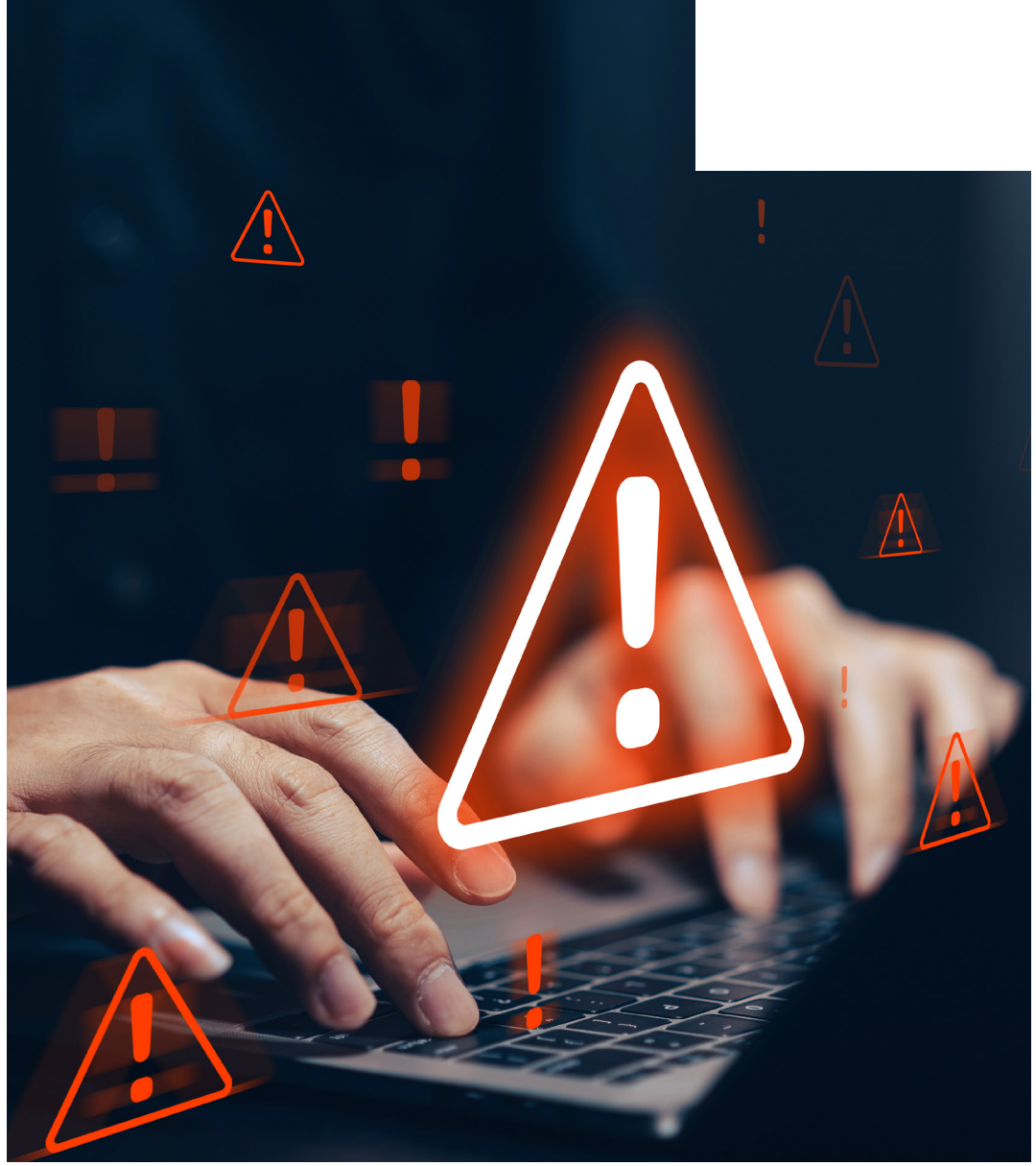
Er eiendoms-strategien din rustet for dagens trusler?

REFM (Real Estate & Facilities Management) har lenge stått i førstelinjen når det gjelder å beskytte arbeidsplassen mot ulike trusler. De siste årene har imidlertid omfanget, hastigheten og alvorlighetsgraden av disse sikkerhetstruslene vært uten sidestykke.

Med alt fra globale pandemier og geopolitisk uro til ekstremvær og digital sårbarhet – de siste fem årene har vist hvordan REFM-team må håndtere eksterne trusler fra alle kanter. Ikke bare øker truslene i hyppighet, de endrer også karakter. Ledere innen REFM blir satt på prøve på flere fronter samtidig, fra spionasje gjennom smarte bygningssystemer til politisk aktivisme og strømnettsvikt.

En global forskningsrapport fra konsulentselskapet Verdantix[1], viser at virksomheter tar større grep for å styrke bygninger mot både fysiske og digitale trusler. Mer enn 60 % av lederne oppgir at de styrker planene for fysisk sikkerhet (opp fra 46 % i 2022), mens 65 % intensiverer innsatsen innen cybersikkerhet.

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



35 %

av REFM-ledere rapporterer svakheter i kriseplanlegging

32 %

peker på uklare roller og ansvarsområder

Som svar på dette skiftende risikobildet gjennomførte Coor en omfattende undersøkelse blant 580 kontoransatte og 575 beslutningstakere innen REFM i Norden. Funnene viser et marked i høy beredskap. Motstandskraft mot eksterne risikoer og trusler rangeres nå som en av de høyeste prioriteringene for REFM-ledere i Norden – kun overgått av helse- og sikkerhetskrav.

Blant de største bekymringene finner vi cybersikkerhet, infrastruktursvikt og naturkatastrofer. Samtidig oppgir mange ledere høy tillit til egen beredskap – kanskje i overkant optimistisk. Til tross for denne selvtilliten finnes det betydelige kapasitetsmangler innen kriseplanlegging, koordinering og strategisk respons.

Ansattes perspektiv tegner imidlertid et annet bilde. Selv om cyberhendelser og helserelaterte kriser også er viktige for dem, →

varierer personlige sikkerhetsbekymringer – som bombetrusler og vandalisme – sterkt avhengig av om de jobber i urbane eller rurale kontorer. Bare 11 % av de ansatte oppga sikkerhet og adgangskontroll som en av de viktigste prioriteringene for forbedring av arbeidsplassen. Temaer som reduksjon av støynivå, tilgang til stillesoner og bedre inneklima ble vurdert som viktigere.

Denne divergensen mellom organisatorisk beredskapsplanlegging og individuelle opplevelser tydeliggjør et økende oppfatningsgap. For eiendomsledere handler oppgaven fremover ikke bare om å forsvare infrastruktur mot økende trusler, men også om å bygge tillit hos de ansatte og knytte overordnet strategi til den daglige opplevelsen av trygghet og trivsel.

Undersøkelsen viser også nasjonale forskjeller:

- Danmark: høyest bekymring, 57 % av beslutningstakere mener trusselnivået har økt de siste to årene.
- Sverige og Norge: 51 % mener trusselnivået har økt.
- Finland: lavest bekymring, 47 % melder økt trusselnivå.

Teknologibedrifter var mest opptatt av sikkerhet og etterlevelse, mens virksomheter lokalisert i mellomstore byer rapporterte størst økning i risiko.

Når nye roller innen cybersikkerhet, beredskap og tverrfaglig styring vokser frem, blir fremtidens REFM en nøkkel for å navigere i kompleksitet med trygghet, tydelighet og samarbeid. Denne rapporten utforsker hvordan nordiske organisasjoner møter utfordringene, hvor sårbarhetene fortsatt ligger, og hvordan REFM-teamene i fremtiden blir grunnleggende for virksomheters evne til å håndtere, redusere og forebygge fremtidige trusler. ■

52%

Økt trusselnivå de siste to årene

Ifølge beslutningstakere innen REFM i Norden (utvalgte områder fra en lengre liste over mulige prioriteringer)

2026: høyeste prioriteringer knyttet til selskapets eiendom og arbeidsplass

Oppfattet av REFM-beslutningstakere i Norden

2

En ny risikotid

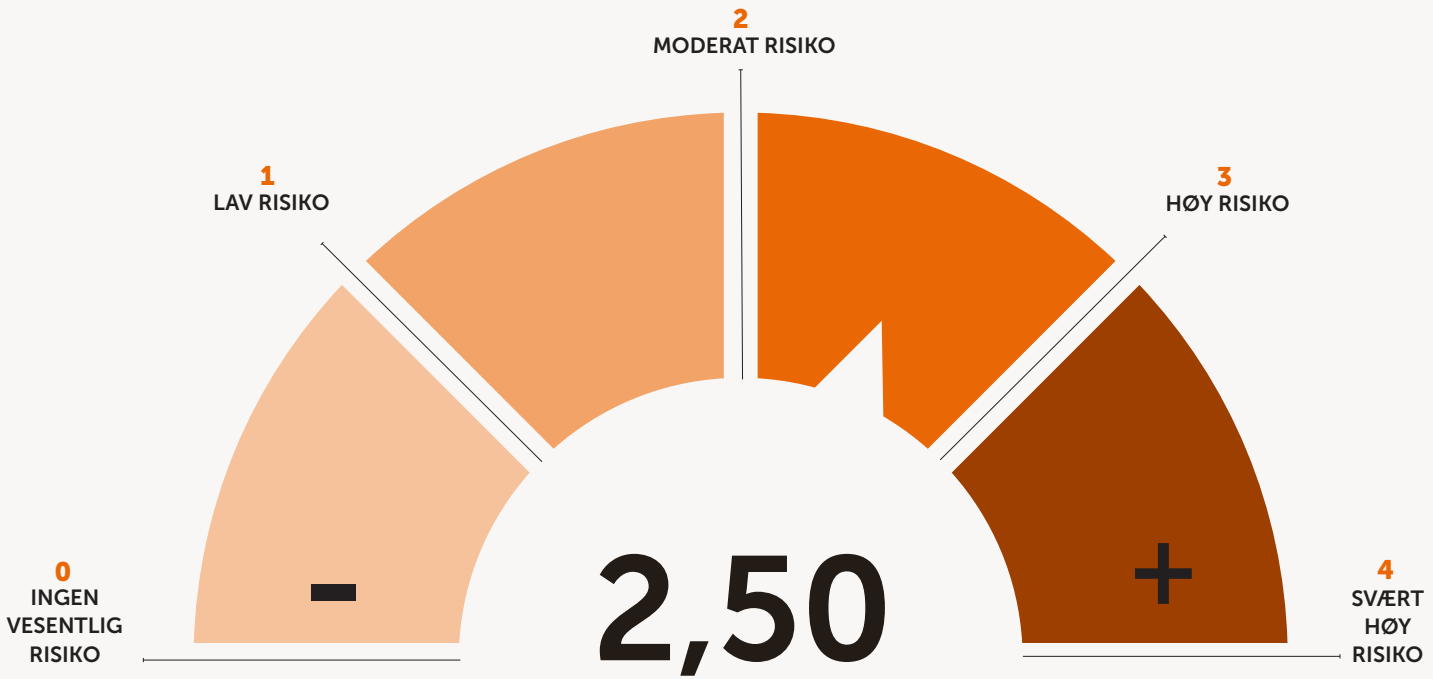
Vi har gått inn i en tid preget av økt risiko. Naturkatastrofer, cyberangrep, politisk uro og pandemier er nå en del av driftsmiljøet for enhver organisasjon. For REFM-profesjonelle innebærer dette et grunnleggende skifte i både tankesett og ansvar.

Tradisjonelle tilnærminger, bygget rundt kostnadseffektivitet og operativ drift, suppleres nå med et stadig sterkere behov for å forutse og håndtere et bredt spekter av trusler. Dette kapittelet utforsker syv sentrale kategorier av fremvoksende eksterne risikoer som sannsynligvis vil forme fremtiden til REFM:

1. **Miljø- og naturkatastrofer** – fordi ekstremvær blir mer vanlig, må organisasjoner bygge motstandskraft både i sine eiendomsporteføljer og i operativ beredskap for å ivareta sikkerheten til mennesker.
2. **Kriminalitet og vandalisme** – når bygninger blir åpnere og mer flerfunksjonelle, settes fysisk sikkerhet under økt press. Samtidig ser mange selskaper betydelig risiko knyttet til spionasje, målrettede angrep og organisert kriminalitet.
3. **Terrorisme og sivil uro** – geopolitisk ustabilitet skaper nye sårbarheter knyttet til tilgang til arbeidsplassen, sikkerhet og virksomheters omdømme.
4. **Cyber- og teknologiske trusler** – sammensmeltingen av digitale og fysiske systemer, og den økende bruken av kunstig intelligens, gjør cybersikkerhetssystemer mer utsatte.
5. **Infrastruktur- og forsyningssvikt** – etter hvert som systemene blir mer elektrifiserte, utsettes de for forstyrrelser i strømnettet. Denne risikoen løfter energimotstandskraft og beredskapsplanlegging inn i styrerommene.
6. **Risiko knyttet til regelverk og etterlevelse** – økt tilsyn, ny lovgivning og strengere krav innen sikkerhet og personvern øker risikoen for manglende etterlevelse.
7. **Helse- og biologiske trusler** – i etterkant av pandemien har helseberedskap fortsatt å være en betydelig risiko, med trusler knyttet til infeksjoner og utbrudd. →

Modell: Risikoindeks per kategori

Oppfattet risikonivå for organisasjonen
(Vektet skår fra 0–4, nordiske REFM-beslutningstakere)



Risikoprofilene for ulike organisasjoner blir stadig mer varierte, formet av sektor, geografi og driftskontekst. Spekteret av potensielle trusler er bredt, og graden av eksponering varierer betydelig mellom ulike miljøer.

For eksempel vil sårbarhetene som påvirker et tettbefolket kontorbygg i bykjernen, være annerledes enn for et produksjonsanlegg på landsbygda.

I tillegg er enkelte selskaper underlagt nasjonale sikkerhets- og beredskapsforskrifter, som for eksempel Sikkerhetsloven, for å beskytte kritisk informasjon og infrastruktur. Disse virksomhetene befinner seg ofte innenfor samfunnskritiske sektorer som finans, forsvar og offentlig forvaltning – og har gjerne kommet lengre i sine strategier og strukturer for å håndtere slike trusler. →

2,47

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

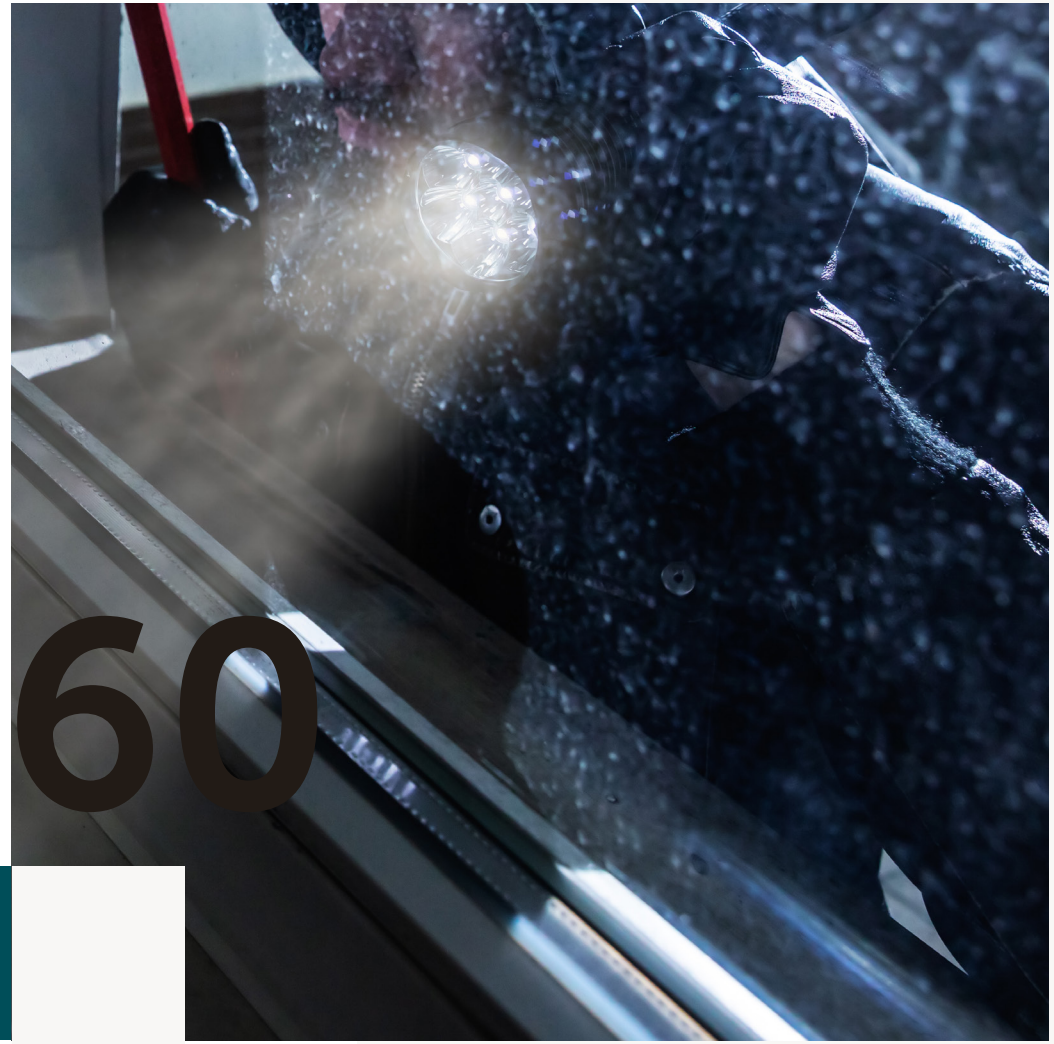
Vanlige REFM-tiltak	Områder der FM-rollen utvides
• Strukturell sikring mot flom og snø • Backup-løsninger for strøm og ventilasjon (HVAC) • Kontinuitetsløsninger (f.eks. snø- og isfjerning, hygiene, catering) • Nødskilt og evakueringsmerking	• Retningslinjer for bygningsmotstandskraft • Overvåkningssensorer og varslingssystemer • Protokoller og øvelser for ansatte på stedet • Beredskapsavtaler med leverandører • Risikovurderinger og revisjoner

Miljø- og naturkatastrofer

Ekstremvær akselererer i omfang. Verdens meteorologiorganisasjon (FN) registrerte 151 rekordartede klimahendelser i 2024, inkludert 25 i Norden[2]. Denne ustabiliteten presser FM til å bevege seg fra «just-in-time»-drift til «just-in-case»-planlegging. Ifølge vår undersøkelse ser 54 % av nordiske REFM-ledere naturkatastrofer som en alvorlig trussel.

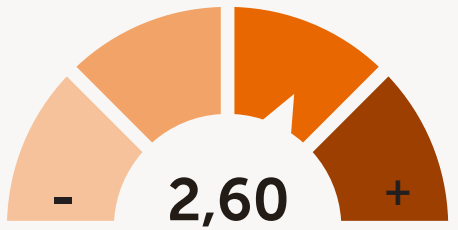
Utfordringen er global. Eiendomsselskapet JLL anslår at 37 % av all næringseiendom – tilsvarende 580 milliarder USD – ligger i de ti mest klimasårbare byene. For FM har motstandskraft for systemer og infrastruktur blitt et sentralt ansvarsområde. Det kreves investeringer både i beredskapssystemer og i mer langsiktig klimatilpasning. Kontinuitetsplanleggingen utvides også utover lokale team til å omfatte lokale beredskapstjenester og eksterne partnere.

To tredjedeler (64 %) av beslutningstakerne mener de er forberedt på naturkatastrofer, men med en økende grad av ekstremvær har motstandskraft blitt en strategisk prioritering. For FM er implikasjonen klar: sikre strukturell redundans, utvikle robuste kontinuitetsplaner og inngå partnerskap som utvider motstandskraften utenfor bygningens vegger. ■



2,60

RISIKOINDEKS



Kriminalitet og vandalisme

Arbeidsplasser blir stadig mer åpne og flerfunksjonelle – og dermed mer sårbare. Trusler spenner nå fra småtyveri til målrettet sabotasje og organisert kriminalitet, særlig ved transportknutepunkt, offentlige områder og kritisk infrastruktur. Også enkeltpersoner kan være mål, noe som krever styrket personlig beskyttelse.

Ifølge vår undersøkelse anser 57 % av REFM-ledere kriminalitet og vandalisme som en alvorlig risiko, og dette gjør kategorien til den tredje største på «Risikoindeksen». Risikoen øker til 59 % innen industri og produksjon, og til 61 % i større byer. FM-team responderer nå med tiltak utover tradisjonell sikkerhetsteknologi: grundigere leverandørkontroller, deling av kriminalitetsmønstre og opplæring av frontlinjepersonell – som resepsjonister – i sikkerhetsprotokoller.

Sikkerhet kan ikke lenger baseres kun på låser og kameraer. FM må samarbeide med politiet, sikre leverandørers integritet og styrke de ansattes kompetanse for å skape arbeidsplasser som både er trygge og tilgjengelige. ■

Vanlige REFM-tiltak	Områder der FM-rollen utvides
• Låser, alarmer og kameraovervåkning (CCTV) • Adgangspunkter og perimeterbelysning • Resepsjon og logging av besøkende • Hendelsesrapporteringsrutiner	• Integrert adgangskontroll og tverrfaglig datadeling • Koordinering av vaktrunder og digitale rapporteringsverktøy • Bakgrunnssjekk og sikkerhetsvurdering av leverandører • Samarbeid med politi og lokale sikkerhetsnettverk • Opplæring av ansatte i bevissthet og konfliktdemping

Terrorisme og sivil uro

Fra aktivisme og målrettet vold til terrorisme og sivil uro – organisasjoner blir i økende grad eksponert for de politiske og sosiale spenningene som preger verden i dag. Ifølge Allianz' Risk Barometer 2025 er politisk vold fortsatt en av de ti største forretningsrisikoene globalt. Siden 2017 har det vært over 800 betydelige anti-regjeringsprotester i mer enn 150 land, hvorav over 160 fant sted i 2024. Rundt 18 % av disse varte i mer enn tre måneder, med konsekvenser for både driftskontinuitet og forutsigbarhet[3].

I motsetning til naturkatastrofer er det vanskeligere å forutsi lokasjon, omfang og varighet av terrorhandlinger eller uro, noe som gjør pålitelige beredskapsstrategier mer komplekse å utarbeide. Konsekvensene strekker seg også utover fysisk skade: avbrudd i virksomheten, nektet adgang, sosial uro og langsiktig omdømmetap er reelle følger. Dermed er det ikke lenger nok for sikkerhets- og FM-team å sikre bygninger og ivareta ansatte – de må også beskytte virksomhetens merkevare og sikre uavbrutt drift.

I Norden ser REFM-ledere dette tydelig. Over halvparten (55 %) av beslutningstakerne oppgir at terrorisme og sivile uroligheter er en alvorlig bekymring. I intervjuer fortalte en leder ved et større produksjonsanlegg at aktivistaksjoner til tider førte til samarbeid i sanntid mellom politi, HR og sikkerhetspersonell. En leder fra en nordisk storbank beskrev hvordan nylige hendelser har ført til omlegging av rutiner for nedstenging av bygg og høyere beredskapsnivå, og bemerket:

«Vi frykter at terrorister kan bruke aktivistgrupper som påskudd for å angripe våre eiendommer.»

Mange organisasjoner beveger seg nå fra reaktiv konfrontasjon til proaktiv «kontrollert åpenhet» – en balanse mellom å beskytte ansatte og samtidig opprettholde tilgjengelighet. Etter hvert som det politiske klimaet tilspisser seg, må arbeidsplasser bygges med økt motstandskraft – ikke bare for å tåle uroligheter, men for å kunne operere trygt og forutsigbart midt i dem. ■

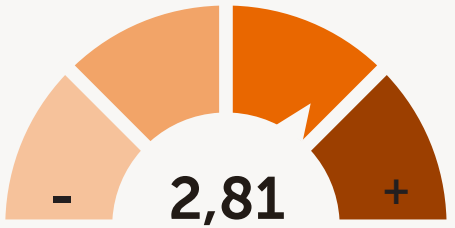
Vanlige REFM-tiltak	Områder der FM-rollen utvides
• Nedstengningsprosedyrer for bygninger • Utpekte samlingspunkter • Spesifikke adgangskontroller ved arrangementer	• Forsterket perimetersikkerhet og håndtering av folkemengder • Sikkerhetssamarbeid med offentlige myndigheter • Krisekommunikasjonsprotokoller og øvelser for ansatte • Teknologi for sanntidsvarsler om trusler i offentligheten

2,46

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

2,81

RISIKOINDEKS



Vanlige REFM-tiltak	Områder der FM-rollen utvides
• Sikre serverrom og fysisk IT-infrastruktur • Sikring av bygningsautomasjonssystemer (BAS) • Adgangskontrollsystemer	• Overvåking og trusseldeteksjon i sammenkoblede systemer • Opplæring av ansatte og leverandører i cybersikkerhet og etterlevelse • Støtte ved cyberrelaterte driftsavbrudd

Cyber- og teknologiske trusler

Etter hvert som arbeidsplasser blir mer digitalt sammenkoblet, vokser også trusselbildet knyttet til cyberangrep raskt. Cybersikkerhet er ikke lenger kun et IT-ansvar; det overlapper i stadig større grad med fysisk infrastruktur, bygningssystemer og operasjonell kontinuitet. Et brudd kan like gjerne kompromittere adgangskontroll som å lekke sensitiv informasjon.

Ifølge vår undersøkelse rangerer 66 % av REFM-ledere cyber- og teknologisk risiko som sin mest presserende bekymring – og plasserer den dermed øverst på risikoindeksen. Intervjuer med toppledere fremhevet risiko knyttet både til eksterne svindlere og interne trusler, spesielt innen høysikkerhetsbransjer som bank og produksjon. Flere organisasjoner har etablert dedikerte cybersikkerhetsenheter i IT-avdelingene, men FM blir i økende grad integrert i dette arbeidet – for eksempel ved å søke ISO-sertifiseringer som styrker sikkerheten i byggrelaterte systemer.

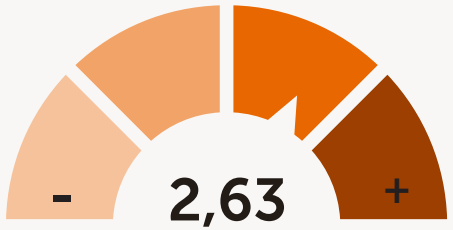
Den nyeste Nordic Threat Landscape Report 2024 fra SOCRadar illustrerer omfanget[4]: 343 omtaler av nordiske land på det mørke nettet, 105 løsepengevirusangrep (41 % i Sverige) og en bølge av phishing-angrep rettet mot Finland og Sverige. Mest utsatt er produksjons- og informasjonstjenester.

Denne utviklingen omformer FMs rolle. Allerede i dag oppgir 36 % av beslutningstakere at FM spiller en kritisk rolle i cyber-fysisk sikkerhet, mens 39 % forventer at denne rollen vil vokse. Store nordiske virksomheter leder an i samarbeidet mellom FM og IT, med felles vurdering av digital infrastruktur, simulering av angrepsscenarier og styrking av motstandskraft i smarte bygg. FM har også fått et utvidet ansvar for leverandørkontroll, opplæring av frontlinjeansatte og innarbeiding av «cyber-hygiene» i daglige rutiner der fysisk og digital drift møtes.

Cybertrusler representerer en akutt risiko for REFM. For å ligge i forkant må FM ta eierskap til grensesnittet mellom fysisk og digital sikkerhet – og sikre at systemer, leverandører og ansattes adferd samlet sett opprettholder virksomhetens motstandskraft. ■

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

RISIKOINDEKS



Vanlige REFM-tiltak	Områder der FM-rollen utvides
• Generatorer og UPS-backup • Reservekapasitet for vann- og varme-systemer • Backup-systemer for belysning	• Sanntidsovervåk-ning av forsyninger og automatiske avstengninger • Alternative energikil-der og lagringsløs-ninger • Planlegging for kontinunitet på tvers av lokasjoner

Infrastruktur- og forsyningssvikt

Etter hvert som systemene blir smartere og mer gjensidig avhengige, blir arbeidsplasser mer sårbare for infrastruktur- og forsynings-svikt. Risikoene spenner fra strømbrudd og avbrudd i vannforsyningen til bortfall av oppvarming.

I undersøkelsen fremhevet 58 % av REF-M-ledere infrastruktur- og forsyningssvikt som en kritisk risiko – den nest høyeste på risikoindeksen. Industribedrifter og produk-sjonsmiljøer rapporterer sterkest beredskap (73 %), mens virksomheter i rurale områder føler seg mindre forberedt enn urbane. Flere ledere viste til geopolitisk uro – som strøm-brudd i Spania og Ukraina – som drivere for økt oppmerksomhet.

Nordisk infrastruktur er særlig sårbar. ENT-SO-E, det europeiske samarbeidsorganet for systemoperatører, har pekt på svakheter i de nordiske strømnettene under vintertopper, når tilgangen på fornybar energi er presset[5]. Organisasjoner svarer med å investere i motstandskraft gjennom UPS-batterier, die-selgeneratorer, 3D-utskrift av reservedeler og alternative energikilder.

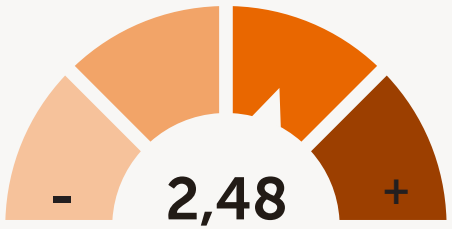
Denne utviklingen setter FM i sentrum for håndtering av infrastrukturrisiko. Hele 32 % av beslutningstakere forventer at FM vil få en stadig større rolle innen dette om-rådet. Presset øker dermed på å balansere kostnadskontroll med operasjonelt fremsyn. FM-ledere forventes å planlegge for ekstra sikkerhetsmarginer på tvers av lokasjoner, sikre kontinuitet i forsyninger og utforme løsninger som kombinerer kostnadseffektivi-tet med driftssikkerhet.

Motstandskraft i infrastrukturen er nå et tema på styrenivå. FM må forutse sys-temsvikt, diversifisere leverandørbasen og bygge inn robusthet i både bygninger og forsyningssystemer for å sikre kontinuitet. ■

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

2,63

RISIKOINDEKS



Risiko knyttet til regelverk og etterlevelse

Det regulatoriske landskapet utvides raskt, spesielt i Norden hvor regelverket blir strengere og kravene til «bevis på etterlevelse» øker. I vår undersøkelse oppga 52 % av REFM-ledere at risikoen knyttet til regelverk og etterlevelse er kritisk – i teknologisektoren og tjenesteyting økte den til 61 %.

EU-regler omformer forventningene. Nettverks- og informasjonssikkerhetsdirektivet (NIS2, 2024) og GDPR (2018) krever at FM leder risikovurderinger, planlegging for hendelseshåndtering og tredjepartstilsyn knyttet til datasikkerhet. Nasjonale rammeverk, som Sikkerhetsloven, pålegger i tillegg bakgrunnssjekker og leverandørkontroller, der FM ofte har det praktiske ansvaret. Bransjespesifikke reguleringer skaper ytterligere kompleksitet – et eksempel er Digital Operational Resilience Act (DORA), som særlig treffer finanssektoren og stiller strengere krav til digital drift og databehandling.

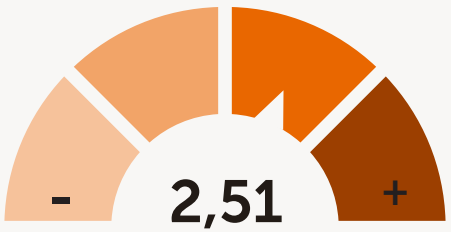
Vanlige REFM-tiltak	Områder der FM-rollen utvides
• Etterlevelse av brannforskrifter og øvelser • Tilgjengelighets-standarder • Miljøkrav for bygg • Helse- og sikker-hetsinspeksjoner	• Integrerte revisjoner og rapportering – ESG, data, sikkerhet • Utvidet opplæring i sikkerhet og etterle-velse for ansatte • Forsterket tredje-partstilsyn og revisjon av risiko på stedet

I tillegg til lovpålagt regulering må FM følge med på nye standarder og agendaer innen brannsikkerhet, arbeidsmiljø, byggeforskrifter og ESG-rapportering. Resultatet er et fragmentert og skiftende landskap, der FM fungerer som en nøkkelaktør for å sikre etterlevelse på tvers av både fysiske og digitale domener. Flere bransjeledere har etterlyst en felles «standard for total sikkerhet og motstandskraft» for å forenkle styring og kontroll.

Etterlevelse kan ikke lenger sees som en ren formalitet. FM må integrere flere overlappende rammeverk, sikre at leverandører etterlever kravene, og bygge inn robusthet i både operasjonelle og cyber-fysiske systemer. ■

2,48

RISIKOINDEKS



Helse- og biologiske trusler

Helserisikoer – fra virusutbrudd til inneklimaproblemer – er fortsatt et kjerneområde for FM etter pandemien. I vår undersøkelse vurderte 55 % av lederne helse- og biologiske trusler som en betydelig bekymring. Risikoene inkluderer ikke bare pandemier, men også mer vedvarende utfordringer som mugg, luftbårne forurensninger og skjerpede krav til ventilasjonsstandarder. Dårlig luftkvalitet alene kan knyttes til økt sykefravær og redusert kognitiv yteevne.

Pandemien førte til et skifte i hvordan FM arbeider – fra «just-in-time»-drift til «just-in-case»-beredskap. FM-team utvidet lagre, oppgraderte rutiner og samarbeidet tettere med både kliniske og operative ledere. En REFM-beslutningstaker uttrykte det slik:
«Under pandemien satte virksomhetslederne standardene, men FM sørget for å levere og koordinere gjennomføringen.»

Vanlige REFM-tiltak	Områder der FM-rollen utvides
• Rutinemessig rengjøring og hygienestandarder • Overvåkning av luftkvalitet og ventilasjon • Skilt og tilgjengelige hygienemidler	• Avanserte ventilasjons- og filtreringssystemer • Beredskapsplaner for helsekriser og lagring av verneutstyr (PPE) • Utvidet etterlevelse av helse- og sikkerhetskrav for leverandører • Krisekommunikasjon ved helsehendelser

Internasjonale rapporter underbygger viktigheten. Verdens økonomiske forum og Global Health Council identifiserte smitteutbrudd som en av de mest alvorlige helserisikoene i 2024[6]. Dette fremhever behovet for kontinuerlig overvåkning, oppgraderte miljøstandarder og raske responsmekanismer.

Helseberedskap er nå et permanent ansvar for FM. Fasilitetsledere må bygge inn pålitelig ventilasjon, hygienerutiner og fleksibel responskapasitet for å beskytte medarbeidernes helse og opprettholde kontinuitet i driften. ■

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

3

Konsekvenser for Facility Management

Etter hvert som risikoene virksomheter står overfor blir flere og mer komplekse, utvides rollen til Facility Management (FM) fra hendelseshåndtering til å være en integrert del av virksomhetens motstandskraft. FM-team forventes ikke lenger bare å drifte bygninger – de skal sikre kontinuitet, koordinere krisehåndtering og beskytte både mennesker og drift i stadig mer uforutsigbare omgivelser.

Denne utviklingen gir både muligheter og utfordringer. FM er i økende grad anerkjent som en nøkkelaktør i tverrfaglig beredskapsplanlegging, men den skiftende rollen skaper også spenninger. Forventningene øker, mens ressursene ofte forblir begrensede. Bidragene til FM blir mer strategiske, men likevel ikke alltid verdsatt. Samarbeid med IT, HR, juridisk, innkjøp og selskapsledelse er avgjørende – men ansvaret for beredskap er fortsatt uklart fordelt. Samtidig må FM balansere mellom konkurrerende prioriteringer, som å beskytte ansatte, sikre eiendeler og opprettholde en positiv arbeidsplassopplevelse.

I Norden blir særlig motstandskraft, digitale trusler og tverrfaglig beredskap strategiske imperativer. Enkelte organisasjoner har integrert FM og sikkerhet godt, mens andre fortsatt er fragmenterte og reaktive. REFM-ledere uttrykker stor tillit til egne evner, mens ansatte i større grad er opptatt av daglige arbeidsplassbehov. Å lukke gapet mellom systematisk beredskap og individuell opplevelse blir avgjørende for å bygge organisatorisk robusthet.

Fra operatør til integrator

Facility Management er i ferd med å utvikle seg fra sin tradisjonelle rolle som operatør – historisk fokusert på fysisk sikkerhet, bygningsinfrastruktur og driftsoppgaver – til å bli en proaktiv integrator og koordinator av organisatorisk beredskap. Dette reflekterer et økende behov for å bygge bro til nye domener som IT og data, HR og innkjøp, samt en dypere involvering i både taktiske og strategiske sikkerhetsspørsmål.

Tallene underbygger denne utviklingen:

- 45 % av beslutningstakere oppgir fortsatt at FMs primære rolle er å håndtere fysisk sikkerhet og infrastruktur.
- 39 % fremhever FMs involvering i IT og digitale systemer.
- Nesten halvparten (47 %) forventer tettere samarbeid mellom FM og IT.
- 35 % ser for seg sterkere integrering med krisehåndtering.

→

«FM sitter tett på ledelsen – vi vet hva som skjer både på stedet og på tvers av funksjoner. Den koordineringen er vår styrke.»

– REFM-ansvarlig ved en stor nordisk produksjonsbedrift

FM er dermed i ferd med å gå fra å være en operatør til en integrator – en funksjon som kobler sammen IT, HR, innkjøp og juridisk. Flere ledere beskriver FM som en «site commander», unikt posisjonert til å overvåke sammenkoblede systemer og koordinere respons.

Å tøye grensene for tradisjonell FM

Etter hvert som Facility Management får en mer strategisk og integrert rolle, møter funksjonen også betydelige utfordringer. Mange FM-team blir bedt om å gjøre mer – med færre ressurser. Utvidede ansvarsområder innen fysisk sikkerhet, forsyninger, etterlevelse og krisehåndtering står ofte ikke i samsvar med økte investeringer, tydeligere mandat eller større synlighet på ledernivå.

Dette gjenspeiles i hele Norden. Flere FM-ledere fortalte i intervjuer at underbemannede team forventes å håndtere stadig mer komplekse eiendommer og systemer. Som en senior beslutningstaker kommenterte:

«Vi har et lite FM-team som håndterer et område på én million kvadratmeter.»

Uten tilstrekkelige ressurser eller organisatorisk støtte risikerer FM å bli overbelastet og undervurdert – nettopp i det øyeblikket funksjonen får økt strategisk betydning.

Etter hvert som FMs innflytelse øker, oppstår spørsmål om eierskap og beslutningsmyndighet. Hvor langt skal FM strekke sitt ansvar inn i tilstøtende domener? Og hvordan kan funksjonen balansere sine grunnleggende driftsoppgaver med rollen som strategisk integrator for sikkerhet og beredskap?

Reell fremgang avhenger av et tydelig skifte i hvordan organisasjoner strukturerer og gir FM mandat. Dette innebærer ikke bare å klargjøre roller og ansvar på tvers av avdelinger, men også å plassere FM tydeligere i strategisk implementering på styrenivå. Økt tverrfaglig samarbeid, mer datadrevet styring og investering i nye ferdigheter vil være avgjørende. Med disse endringene kan FM utvikle seg fra å være en presset støttefunksjon til å bli en sentral integrator av sikkerhet, motstandskraft, bærekraft og arbeidsplasstrategi – og frigjøre sitt fulle potensial som pådriver for organisasjonens ytelse og endring.

Å bygge ny kapasitet og nye allianser

I sin nye rolle som integrator må FM gjennomføre strategiske endringer på tvers av organisasjonen. FM-funksjonen trekkes stadig mer inn i allianser med andre disipliner, men samarbeidet er ofte fragmentert og siloorientert. Dette begrenser evnen til å respondere raskt og helhetlig på avbrudd.

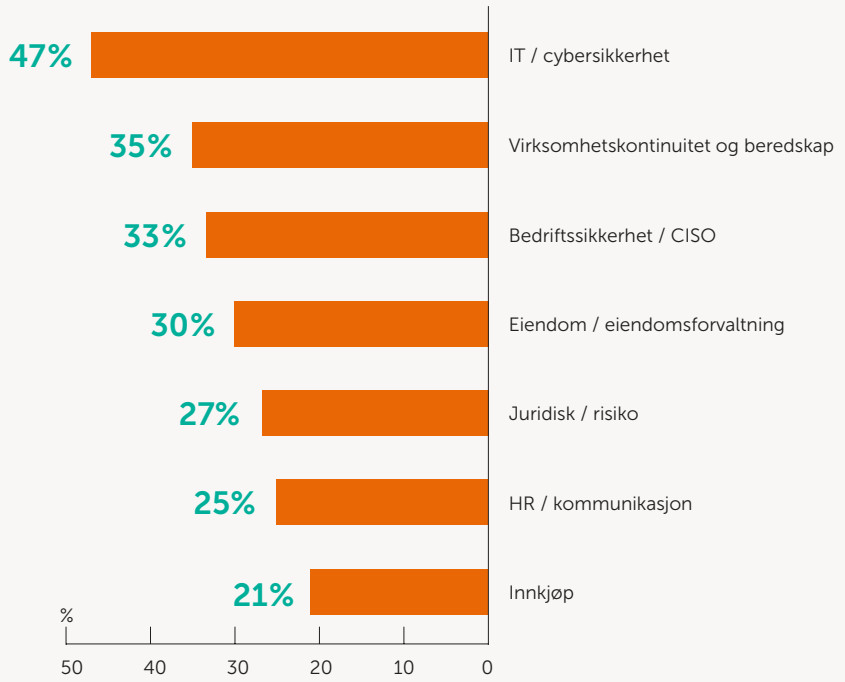
I fremtiden er samarbeid på tvers av hele organisasjonen uunngåelig. For FM er de største forventede økningene i samarbeid med:

- IT og cybersikkerhet (47 %)
- forretningskontinuitet og kriseteam (35 %)
- selskapssikkerhet (33 %)

Forskningen ga også andre eksempler på fremgang, inkludert en nordisk bank som har gitt FM ansvaret for fysisk sikkerhet, samtidig som de samarbeider med IT om cyberrobusthet. Et logistikkfirma involverer FM i å →

Organisatoriske funksjoner der samarbeid med FM forventes å øke mest

(ifølge REFM-beslutningstakere i Norden)



sette infrastruktur- og adgangsstandarder på hundrevis av steder. Og en produsent integrerer FM direkte i krisehåndtering, i samarbeid med HR, bærekraft og IT.

En FM-beslutningstaker uttrykte det slik: «Vi har ansvar for beredskap og forretningskontinuitet på tvers av organisasjonen. Det fungerer bare fordi vi er tett koblet på IT, sikkerhet og drift.»

Større integrasjoner krever imidlertid mer enn samarbeid alene – det krever også sterkere intern kapasitet i FM. To viktige endringer peker seg ut:

- **Strategisk kontinuitet:** FM forventes å utvikle planer for motstandskraft som kombinerer fysiske eiendeler, driftskontinuitet og leverandørberedskap – ikke bare utføre retningslinjer fra sikkerhet eller risikoteam. Dette plasserer FM som en aktiv pådriver for kontinuitetsplanlegging.
- **Fysisk–digitalt eierskap:** I smarte bygg fungerer FM delvis som IT. Funksjonen skal overvåke leverandørers cybersikkerhet, sikre tilkoblede bygningssystemer og øke ansattes bevissthet rundt «cyber-hygiene» i skjæringspunktet mellom fysisk og digital drift.

Begge områder krever nye ferdigheter, nye styringsstrukturer og tydelig støtte fra ledelsen. Uten klare mandater svekkes FMs evne til å handle, og beredskapen blir fragmentert.

Å balansere arbeidsplasskultur med sikkerhet

Sikkerhet og beskyttelse er nå kjerneoppgaver for FM, men de bringer med seg et nytt dilemma: hvordan beskytte mennesker og eiendeler uten å undergrave arbeidsplassens kultur.

Undersøkelsesdata viser et tydelig skille. Mens 28 % av beslutningstakerne rangerer sikkerhetsoppgraderinger som en topp prioritet, er det bare 11 % av de ansatte som sier det samme – de foretrekker tiltak knyttet til komfort, ro og bedre fasiliteter. Denne uoverensstemmelsen avdekker risikoen for å skape miljøer som oppleves som for restriktive.

Ledende organisasjoner velger derfor en annen tilnærming. I en nordisk bank holder FM-teamet mange sikkerhetstiltak «usynlige» for å unngå en følelse av permanent nedstenging. En FM-sjef uttrykte det slik:

«Du kan ikke skape en levende arbeidsplass når alt føles som en nedstenging – men truslene er reelle, og vi må håndtere dem.»

I FMs nye og utvidede rolle må ledere derfor designe arbeidsmiljøer som både er sikre og menneskelige – der sterk beskyttelse kombineres med en positiv opplevelse for de ansatte. Evnen til å håndtere oppfatninger er nå like viktig som evnen til å håndtere infrastruktur. ■

4

Et rammeverk for motstandskraft

Som svar på det økende presset og kompleksiteten Facility Management (FM) står overfor, er det et tydelig behov for en mer strukturert tilnærming. Et rammeverk som speiler FMs utvidede rolle på tvers av flere risikoområder, og som gjenspeiler den økende avhengigheten av samarbeid med andre funksjoner.

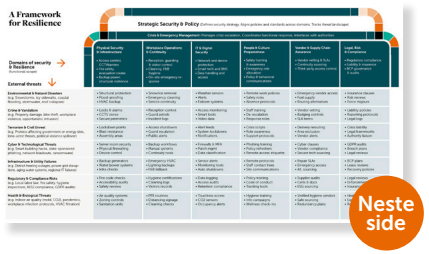
Et nytt rammeverk tar form og søker å gi veiledning i dette skiftende landskapet. Hensikten er ikke å legge alt ansvar på FM for å håndtere alle trusler alene, men å anerkjenne arbeidsplassen som et komplekst, samarbeidsbasert økosystem. Rammeverket gir veiledning i hvordan FM kan jobbe sammen med IT, HR, juridisk, innkjøp, sikkerhet og bærekraft for å etablere en mer helhetlig og koordinert tilnærming til organisatorisk motstandskraft.

Tradisjonelt har FM hatt to hovedområder:

- fysisk sikkerhet og infrastruktur
- arbeidsplassdrift og kontinuitet

Men etter hvert som trusler blir mer sammenvevde, flytter FM seg sideveis inn i tilstøtende domener som IT, HR og innkjøp, og oppover inn i mer strategiske spørsmål knyttet til sikkerhetsstyring, beredskap og krisehåndtering. I noen tilfeller får FM direkte ansvar; i andre tilfeller samarbeider funksjonen tett med spesialiserte team for å samordne responsen.

Målet er å bevege seg bort fra reaktiv tjenesteleveranse mot en modell med delt ansvar – der det blir tydelig hvem som leder, hvem som støtter og hvordan man koordinerer på tvers av siloer. Ved å tydeliggjøre ansvarsområder og samarbeidsflater gir rammeverket FM mulighet til å bli mer enn en driftsfunksjon – til å bli en strategisk muliggjører av virksomhetens motstandskraft. ■



Coor 360 – Rammeverk for sikkerhet og motstandskraft

Strategisk sikkerhet og policy (definerer sikkerhetsstrategi, tilpasser policyer og standarder på tvers av domener, følger trusselbildet)

Krise- og beredskapshåndtering (håndterer kriseeskalering, koordinerer tverrfaglig respons, fungerer som grensesnitt mot myndigheter)

Søyler / domener for sikkerhet og motstandskraft →

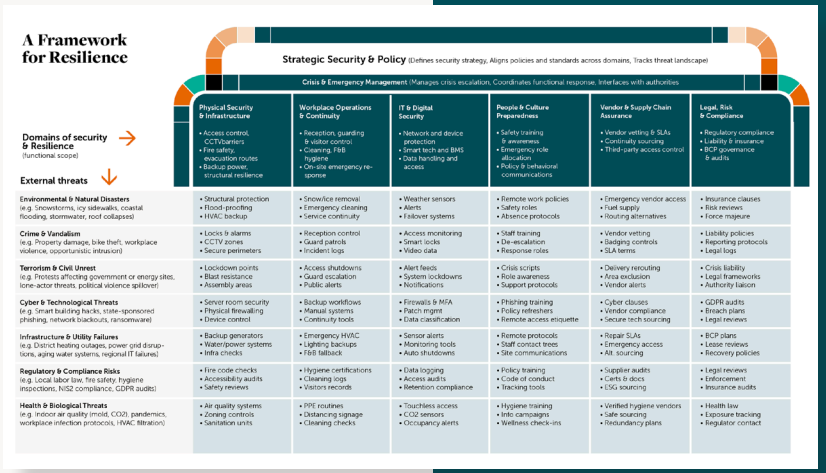
Eksterne trusler rammeverket dekker ↓

	Fysisk sikkerhet og infrastruktur • Adgangskontroll, CCTV, barrierer • Brannsikkerhet, evakueringsrutiner • Backup-strøm, strukturell robusthet	**Arbeidsplassdrift og kontinuitet** • Resepsjon, vakthold og besøkslogging • Renhold, kantine, hygiene • Beredskap på stedet	**IT og digital sikkerhet** • Nettverk og databeskyttelse • Smarte bygg og BMS • Datahåndtering og tilgangs-styring	**Mennesker og kultur** • Sikkerhetsopplæring og bevisstgjøring • Policyer og atferdsnormer • Krisetrening og responsteam	**Leverandør- og forsyningssikkerhet** • Leverandørkontroll og SLA-er • Kontinuitetsplanlegging • Tredjeparts adgangskontroll	**Juridisk, risiko og etterlevelse** • Etterlevelse av regelverk • Ansvar og forsikring • BCP-styring og -revisjoner
Miljø- og naturkatastrofer (snøstormer, flom, kysterosjon)	• Strukturell beskyttelse • Flom- og snøbeskyttelse • HVAC-backup (oppvarming, ventilasjon og kjøling)	• Beredskapsprosedyrer på stedet • Planer for tjenestekontinuitet • Operasjonell støtte ved kriser	• Sikring av serverrom og fysisk IT-infrastruktur • Sikkerhetsrutiner for byggauto-masjonssystemer (BAS) • Kontroll av digitale adgangssystemer	• Sikkerhets- og beredskapstrening for ansatte • Øvelser for krisehåndtering og evakuering • Opplæring i førstehjelp og nødrutiner	• Bakgrunnssjekk av leverandører og partnere • Sikkerhetsgodkjenning før kontraktsinngåelse • Løpende vurdering av leverandørens pålitelighet	• Risikoanalyse og trusselvurdering • Kartlegging av sårbarheter • Regelmessig oppfølging av risikobildet
Kriminalitet og vandalisme (tyveri, innbrudd, spionasje)	• Låser og alarmer • CCTV-soner (kameraovervåking) • Sikre perimeterområder	• Rapportering av hendelser • Varsling og kommunikasjons-rutiner • Samarbeid med beredskaps-enheter	• Nettverksbeskyttelse og brannmurer • Kryptering og databeskyttelse • Sikring av kritiske systemer og data	• Informasjonskampanjer for sikkerhets-bevissthet • Introduksjon og onboarding med fokus på trygghet • Synliggjøring av prosedyrer og kontaktpunkter	• Krav til beredskap og kontinuitet i kontrakter • Sikkerhetsklausuler i tjenesteavtaler (SLA) • Klare roller ved avbrudd eller hendelser	• Overholdelse av lover og forskrifter • Kontroll av interne retningslinjer og prosedyrer • Oppdatering etter nye nasjonale krav og EU-krav
Terrorisme og sivil uro (protester, politisk vold, målrettede aksjoner)	• Adgangskontroll • Resepsjon og besøksregistrering • Vaktrunder og overvåking	• Evakuering og samlings-punkter • Midlertidige arbeidsplasser • Nødrutiner for ansatte og besøkende	• Overvåking av cybertrusler og hendelser • Varslings- og responsprosedyrer • Samarbeid med IT og cybersikkerhetsteam	• Rutiner for varsling og kommunikasjon under hendelser • Roller og ansvar ved kriser • Støtte til ledere i beredskapssituasjoner	• Overvåking av kritiske leveranser • Samordning mellom FM, innkjøp og leverandører • Deling av sikkerhetsinformasjon ved risiko	• Internrevisjon og uavhengig tilsyn • Dokumentasjon av kontroller og tiltak • Rapportering til ledelse og myndigheter
Cyber- og teknologiske trusler (phishing, nettverksbrudd, løsepengevirus)	• Nødlys og skilt • Evakueringsruter og utganger • Rømningsplaner og øvelser	• Koordinering mellom funksjoner • Støtte til kriseledelse • Roller og ansvar ved beredskap	• Leverandørkontroll for IT-sikkerhet • Testing og penetrasjonsanalyser • Revisjon av digitale systemer	• Trening i konfliktforebygging og de-eskalering • Psykososial støtte ved hendelser • Trygghetsrutiner i møte med besøkende og publikum	• Revisjon av leverandørers HMS- og sikkerhetsrutiner • Oppfølging av underleverandører • Rapportering av avvik og hendelser	• Personvern (GDPR) og databeskyttelse • Informasjonssikkerhet og klassifisering • Håndtering av innsyns- og rapporteringsplikt
Infrastruktur- og forsyningssvikt (strømnett, vann, oppvarming, aldrende systemer)	• Generatorer og UPS-systemer • Backup for vann og varme • Vedlikehold av tekniske anlegg	• Tilgangsstyring under hendelser • Rutiner for bygnings-stengning og -gjenåpning • Overvåking av service- og forsyningsstatus	• Opplæring i digital sikkerhets-kultur • Veiledning i sikker bruk og passordhåndtering • Øvelser for cyberhendelser	• Samarbeid med HR og verneombud • Involvering av ansatte i sikkerhetskultur • Regelmessig evaluering av trivsel og trygghet	• Opplæring og bevisstgjøring hos eksterne aktører • Koordinering av adgang og aktiviteter på stedet • Felles øvelser med leverandørnettverk	• HMS- og arbeidsmiljøoverholdelse • Kontroll av bygningstekniske krav og brannsikkerhet • Revisjon av leverandørers etterlevelse
Risiko knyttet til regelverk og etterlevelse (GDPR, NIS2, sikkerhetslover)	• Sensorer og varslingssystemer • Overvåking av kritiske systemer • Fjernstyrt driftsovervåking	• Fjernarbeid og hybride løsninger • Støtte for digital drift og samhandling • Reserveløsninger for virk-somhetskritiske funksjoner	• Backup og gjenoppretting av data • Kontinuitetsplan for IT-tjenester • Sikker lagring og tilgangsstyring	• Kommunikasjon etter hendelser • Debrief og læring i team • Tiltak for å gjenopprette normal drift og trygghet	• Kontroll av logistikk- og transportledd • Sporbarhet i forsyningskjeden • Alternative leveranseveier ved forstyrrelser	• Forsikring, ansvar og skade-håndtering • Juridisk rådgivning ved hendelser • Samarbeid med eksterne eksperter ved gransking
Helse- og biologiske trusler (luftkvalitet, smitteutbrudd, ventilasjon)	• Risiko- og sårbarhetsvurderinger • Revisjoner av sikkerhetsrutiner • Planer for kontinuitet og gjenoppretting	• Løpende oppdatering av prosedyrer • Evaluering etter hendelser • Kontinuerlig forbedring og læring	• Risikovurdering av digitale systemer • Samordning mellom IT, FM og sikkerhet • Integrert styring av fysiske og digitale trusler	• Kultur for kontinuerlig forbedring av beredskap • Integrering av sikkerhet i organisasjons-kulturen • Langsiktig opplæring og utvikling av kompetanse	• Periodiske risikovurderinger og forbedringsplaner • Samarbeid for kontinuerlig sikkerhets-forbedring • Rapportering til ledelse og styre om status og tiltak	• Læring og forbedring etter hendelser • Oppdatering av policyer og beredskapsplaner • Periodisk gjennomgang av styringssystemet

Veiledning i bruk av rammeverket

Trinn 1

Kartlegg nøkkelfunksjoner
• Identifiser organisatoriske funksjoner knyttet til beredskapsområder (f.eks. forretningsledere, selskapssikkerhet/CISO, eiendom, HR, IT/cybersikkerhet, kommunikasjon, innkjøp, juridisk, risiko, krise-/kontinuitetsteam).



Trinn 2

Sammenlign med styringsdokumenter
• Sjekk rammeverket opp mot eksisterende retningslinjer og dokumentasjon.
• Fremhev hvor eierskap og ansvar er tydeliggjort – og hvor det finnes gap.

Trinn 3

Kjør en interessent-workshop
Samle nøkkelpersoner for å vurdere beredskap og fremtidige behov:
• Definer 5–10 kritiske trusselscenarioer (f.eks. strømbrudd på lokasjon X, svikt i adgangskontrollsystem, demonstranter ved hovedinngangen).
• Diskuter de viktigste mottiltakene, fordelt på beredskapsområder.
• Tildel roller (strategisk eier, utførende leder, støttende team).
• Vurder behovet for faste forum eller team for planlegging, koordinering og hurtig respons.

Trinn 4

Integrer i beredskapsagendaen
• Inkluder relevante deler av rammeverket i virksomhetens strategi for motstandskraft.
• Tildel klart eierskap for hvert element.
• Forplikt til regelmessig gjennomgang og kontinuerlig forbedring.

5

Konklusjon – Er organisasjonen din forberedt?

Facility Management (FM) handler ikke lenger bare om å holde lysene på. Det handler om å holde hele organisasjonen i gang gjennom avbrudd, usikkerhet og endring. Fra miljøsjokk og cyberangrep til helsekriser og sivil uro – dagens risikoer krever en ledelse som er integrert, proaktiv og dypt samarbeidende.

Når ulike disipliner samles, bør de stille seg selv noen nøkkelspørsmål for å sikre at organisasjonen er tilstrekkelig forberedt i et skiftende trusselbilde:

1. Hva er den største bekymringen deres akkurat nå, knyttet til FM, risiko og organisasjonens motstandskraft?

2. Hvilke trusler har organisasjonen definert som mest kritiske på tvers av eiendom, drift, informasjon og ansatte?

3. Hvilke tiltak og beredskapsplaner er allerede etablert for å håndtere disse truslene?

4. Hvordan er ansvar og roller fordelt mellom funksjonene, og hvilken rolle har FM når det gjelder eierskap, koordinering og direkte respons?

5. Hva er de tre viktigste utviklingsområdene dere må styrke for å gjøre organisasjonen bedre rustet mot fremtidige trusler?

Dette er ikke hypotetiske spørsmål. De utgjør forskjellen mellom motstandskraft og sårbarhet, mellom gjenoppretting og kollaps. I en verden der avbrudd er den nye normalen, er Facility Management ikke en ettertanke – det er en frontlinje i arbeidet med å styrke virksomheten for fremtiden.

Den neste krisen kan komme raskere enn forventet.

Er din arbeidsplass forberedt? ■

Metodikk

Denne rapporten kombinerer kvantitative spørreundersøkelser med kvalitative ekspertinnsikter for å gi et helhetlig bilde av det skiftende landskapet for Real Estate & Facilities Management (REFM) i Norden.

En anonym spørreundersøkelse ble gjennomført med 1 155 respondenter:

- 575 beslutningstakere innen eiendom og FM-ledelse, med lederroller og ansvar for arbeidsplass, sikkerhet og driftsstrategi.
- 580 ansatte, som ga sluttbrukerperspektivet på arbeidsplasopplevelse og organisatorisk beredskap.

Respondentene var jevnt fordelt på Sverige, Norge, Danmark og Finland, slik at resultatene representerer regionen balansert. Undersøkelsen dekket 12 ulike bransjer, inkludert bank og finans, helsevesen, produksjon, teknologi, logistikk og flere. Virksomhetene var lokalisert både i storbyer, mellomstore byer og mer rurale områder.

For å supplere funnene ble det også gjennomført dybdeintervjuer med fem senior beslutningstakere innen bank, produksjon, helse og industri. Disse intervjuene ga kontekstuelle innblikk i hvordan ledende organisasjoner responderer på nye trusler, bygger strategier for motstandskraft og redefinerer rollen til Facility Management. ■

Kilder:

• 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.

OM COOR

Coor er en av Nordens ledende leverandører av Facility Management. Vi leverer tjenesteløsninger med hjerte og hjerne – sikkert, effektivt og med omtanke for alle detaljer. Med kompetanse, engasjement og fleksibilitet skaper vi verdi for mennesker og virksomheter. De 12 000 medarbeiderne våre gjør en forskjell. Hver dag, hele året, i hele Norden.

Les mer om oss på www.coor.no

OM WORKTECH ACADEMY

WORKTECH Academy er den ledende globale forskningsplattformen og medlemsnettverket som utforsker hvordan vi kommer til å jobbe i fremtiden. Vi ser på innovasjon i arbeidslivet og på arbeidsplassen ut fra fem sentrale områder: mennesker, sted, teknologi, design og kultur. Vi samarbeider med det sterke nettverket vårt av over 14 000 individuelle abonnenter og mer enn 90 bedrifts-, design- og teknologiorganisasjoner over hele verden om å levere siste nytt innen trender, forskning og beste praksis i arbeidslivet og på arbeidsplassen.

www.worktechacademy.com

Join the Workplace Revolution er en serie nordiske undersøkelser initiert av Coor for å følge med på og forstå utviklingstrekkene i verden rundt oss.

La oss hjelpe deg videre på din FM-reise!

For ytterligere inspirasjon, besøk oss her:
https://www.coor.no/facility-services/fremtidens-arbeidsplass/

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

En rapport fra Coor,
i samarbeid med WORKTECH Academy

COOR WORKTECH ACADEMY