Guide

Din guide till att förstå riskanalys

Stratsys

Innehållsförteckning

Introduktion

Intrycket av riskhantering som ett onödigt extra som distraherar från det ’riktiga’ arbete är inte helt ogrundat. Det är inte ovanligt att riskhanteringsprocessen läggs som ett lager på existerande arbetssätt utan hänsyn till:

- Hur det påverkar nuvarande arbetssätt och bandbredd
- Vad som behövs för effektiv riskhantering

Effekten av detta blir att man lägger till fler saker att göra (rapportera, kryssa i rutor, fylla i formulär), snarare än att utvärdera och anpassa hur man arbetar.

Men att anpassa hur man gör saker är det bästa och billigaste sättet att hantera risker integrerat, även om det inte alltid är det ’enklaste’ eftersom många ser förändring som otäckt.

I den här guiden går vi igenom hur du kan identifiera, utvärdera, prioritera, och hantera era verkliga risker med mindre störning från mindre relevanta risker. Guiden är inte en utbildning i riskhantering, utan avsedd att hjälpa er att tänka igenom och kontextualisera nyckelbegrepp, så att ni kan ’äga’ dem och använda dem för att uppnå era behov på ett meningsfullt sätt.

”Jag hanterar redan risker, vi behöver ingen riskhantering”

Sant, det gör du, men du behöver riskhantering ändå. Alla hanterar risker aktivt dagligen, de flesta hanterar risk i sitt arbete, och de flesta verksamheter har någon form av risk-hantering oavsett hur lite formell struktur som finns.

Men från organisationssynpunkt är den ackumulerade effekten av improviserad riskhantering av individer i silostrukturer att man får duplicering, luckor, och ineffektiv hantering. Man tycks också ofta blanda ihop problemhantering med riskhantering (det är inte samma sak!).

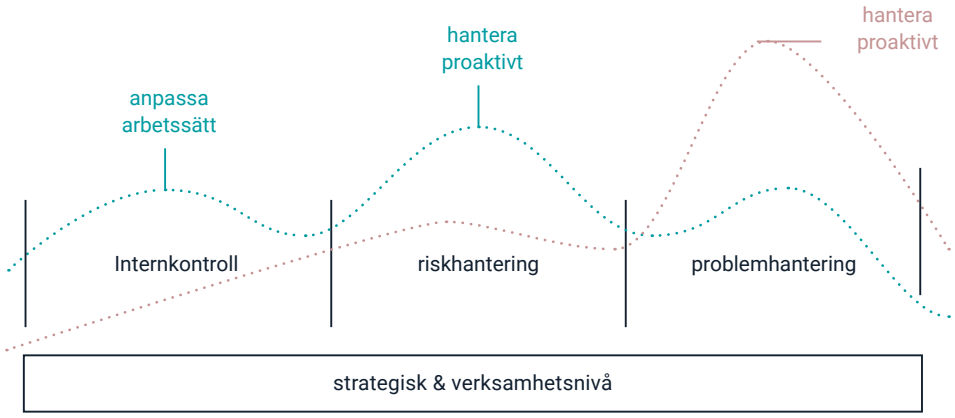
Primära ägare och ansvariga för riskhanteringen är de relevanta beslutsfattarna. Det är inte ovanligt att stöta på uttalanden som att ’det är allas jobb att hantera risk’ vilket naturligtvis ofta översätts som ’det är någon annans jobb’.

Det kan finnas riskstrateger och riskspecialister (t.ex. inom bedrägeri, säkerhet, IT-säkerhet, personal, osv) för att stödja riskhanteringsplaneringen i en organisation, men det är beslutsfattarna och budgetägarna som beslutar hurvida riskerna faktiskt hanteras. Riskhantering är inte en aktivitet separerad från verksamheten.

Det handlar om att ha en risklins i alla processer och beslutsgångar. Strukturerad riskhantering handlar om att dokumentera detta och att göra det till en arbetsplan.

Strukturerad riskhantering erbjuder en bra avkastning därför att det reducerar tid och resurser spenderade på att bekämpa ’bränder’. Fördelen med att vara strukturerad är att man blir systematisk, undviker duplicering, ökar översyn och transparens, upptäcker (och kan täcka) luckor i hanteringen. Den effekt man vill uppnå är enkelhet, integrering, och att anpassa hur vi arbetar för att göra det bättre. Produkten är en arbetsplan, men effekten är ett insitutionellt minne och ökad försäkransgrad.

Kurvor visandes arbetsbörda för proaktiv kontra reaktiv styrning.



Det börjar inte med risken, det börjar med syftet!

För att ge mening och skapa mervärde med riskplaneringen måste man börja med att identifiera organisationens syfte för riskhantering. Är det att uppnå vissa vinstmål? Kvalitetssäkra verksamheten? Produktionsvolym? Är det för måluppfyllnad? Eller kanske samtliga alternativ?

Syftet kan till exempel vara: Att maximera upstream-produktionen på ett sätt som inte underminerar kvaliteten eller uthålligheten i produktionsvolymen, och utan att utsätta personal, partners, tillgångar eller rykte för fara.Det här kopplar ihop syftet med riskhanteringen och skapar klara avgränsningar i relation till 'kostnaden för att bedriva verksamhet'. Ett tydligt uttalande sätter tonen från toppen för resten av organisationen och blir en konstant återkopplingpunkt för framtida internkommunikation.

> **Ett väldefinierat syfte hjälper er att definiera vad riskerna står i relation till, något som kommer bli viktigt när ni gräver i detaljerna kring riskerna.**

Så identifierar ni risken – information är grunden

Innan vi kommer till frågan om vilka risker vi har måste vi ha information. Om informerat beslutsfattande är naturligt bättre riskhantering (det är det!) så är informerad riskidentifikation betydligt bättre än att gissa eller komma på en massa risker bara för att få gå från riskmötet.

Det finns många sätt att analysera kontexten kring verksamhetsmål och utförande. Nedan är ett förslag på kategorisering som är till för att hjälpa till exempel en riskworkshop att fokusera på de olika riskdimensioner som omgärdar verksamheten, istället för att helt slukas av de senaste ’buzz’-orden i regelefterlevnad. Att ha en stor oroskälla eliminerar inte alla andra risker (GDPR, någon?).

Kartlägg din verksamhet – ‘Göra-pyramiden’

Den här ‘göra-pyramiden’ är ämnad som en visuell representation för att fokusera en diskussion eller riskworkshop på vilka nyckelrisker verksamheten möter. Den kan förändras beroende på verksamhetens natur och mål, men är ett sätt att förstå utmaningar som borde påverka hur vi arbetar. Ett annat sätt att närma sig detta är till exempel ’bakåt-planering’ där man börjar med målsättningen och arbetar bakåt för att kartlägga vad som behövs för att nå dit.

Pyramidens logik är enkel och kan med fördel arbetas igenom med en tvär-funktionell grupp som erbjuder olika perspektiv. Detta låter er täcka så mycket som möjligt innan prioriteringsövningarna. För att bedriva vår verksamhet på ett realistiskt och ansvarsfullt sätt måste vi veta att vi har rätt struktur (lämplig för syftet), rätt planering (kunskapsbaserad), och rätt budget (själv-förklarande).

För att fastställa detta måste vi förstå externa och interna utmaningar och krav. Ju mer kunskap som vi saknar, desto mer instabil och opålitlig blir vår verksamhet.

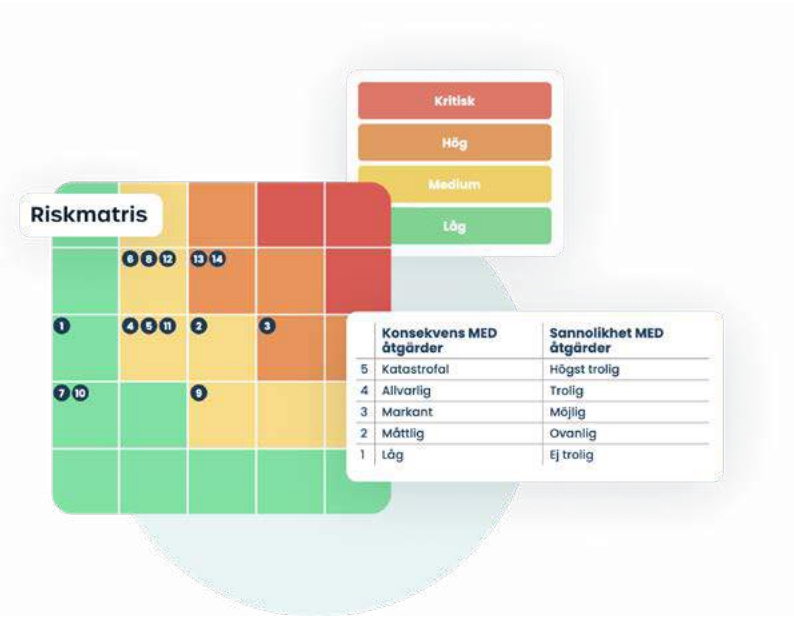
Det är också viktigt att behålla relevansen av risken i fokus, samt att ifrågasätta egna antaganden om förkunskap. Att vi ser och hör mycket om något kan få det att verka viktigare än vad det är. Till exempel, i högriskmiljöer är förar-beteenden och brist på säkerhetsbälten ofta större skadekällor än de mer omtalade säkerhetsincidenterna som involverar våld. Bältesanvändning behöver mer uppmärksamhet men får inte alltid det.

Göra-pyramiden

För att förstå och definiera våra risker ordentligt behöver vi samla in information, analysera och förstå grunderna i form av:

1. Våra interna utmaningar och hot

Vilka potentiella hinder och utmaningar måste vi övervinna? Till exempel: Finns det lagar som begränsar hur vi kan arbeta? Är miljön osäker? Är kompetenstillgången begränsad på den lokala marknaden? Är regelverken ett hinder eller en hjälp? Fungerar tull-processen eller skapas förseningar? Är infrastrukturen tillräcklig för transportbehoven? Är leveranskedjan pålitlig? Vilka beroenden finns som inte kan kontrolleras fullständigt?



2. Vår interna kapacitet och utmaningar

Hur komplicerad är verksamheten? Har vi de kompetenser som krävs tillgängliga? Har vi bandbredd att leverera resultat inom utsatt tid? Finns det utbildnings och träningsbehov? Finns det resultatrelaterade problem som skapar oro? Är personalstyrkan stabil eller har vi hög omsättning? Och så vidare.

Viktigt att beakta är att om man gör detta tidigt så kan verksamheten utveckla och anpassa hur de arbetar istället för att lägga till fler saker att göra. Resultatet är en integrerad och mindre betungande riskhantering-sprocess, men också en högre grad av förtroende och tillit för och inom organisationen.

Genom att kartlägga utmaningar och sårbarhet (gör till exempel en SWOT-analys) kan vi identifiera våra nyckel-risker för och från organisationen, för att vidare utvärdera och prioritera dem.

Organisatorisk och operativ risk

A) Organisatorisk risk (kan också kallas gemensam eller övergripande) handlar om risk som är ett uttalat orosmoment för organisationen som helhet och definierad centralt. Det kan handla om externa tryck (lagar, regler, medborgartryck, och så vidare) eller interna saker. Organisatoriska risker är bäst definierade centralt och policys, arbetsinstruktioner, och guide-dokument bör vara utformade för att bidra till riskreduktionen. Riskerna kan vara aktivt hanterade eller hanteras genom standardiserade kontrollmoment som delas ut till de relevanta delarna av organisationen som i sin tur kan lägga till fler och lokalt relevanta kontroller. De standardiserade kontrollerna blir då en typ av mini-standard för hantering av den organisatoriska risken på underenhetsnivå.

B) Operativ risk är här ett samlingsbegrepp för risker som identifierats lokalt i en organisations underenheter. Den här typen av risker står i relation till den specifika kontexten och de omständigheter en enhet är operativ i och de hanteras lokalt. Det är dock extremt viktigt att linjeorganisationen kan se dessa risker då det genererar värdefull ledningsinformation kring underenheternas utmaningar och hanteringsplan. Det skapar också underlag för mer relevant risk-baserad revisionsgranskning.

Riskaptit – vad är det & varför är det relevant?

Riskaptit är inte för alla. Det kan vara ett något förvirrande och till och med störande begrepp som kräver viss mogenhetsgrad och klarhet i organisationen för att nå sin fulla (och användbara) potential. Riskaptit kan relatera till chanstagning (‘positiv risk’) och till hur en organisation relaterar till hot. Eller både och.

Aptiten kan sättas mot specifika definierade kontextvillkor som till exempel tillåter högre risktagande. Ett tydligt exempel på sådan skillnad är när tillgångar står på spel jämfört med när liv står på spel.

En välformulerad riskaptit är en viktig del av ledningens tonsättande. Tonen, fokus, och komplexiteten av en riskaptit kommer att variera från organisation till organisation, men vi tycker det är värdefullt att betrakta det som stående guidning kring beslutsfattandets gränsdragningar och den typ av risk som en beslutsfattare på en lägre nivå får ta. Men att definiera en aptit är inte i närheten av nog – det kräver dedikerad operationalisering och kontinuerlig kommunikation från ledningen.

Om man ser riskaptit på detta sätt är den mest användbar, och mest behövd, i stora komplexa organisationer som förlitar sig på omfattande delegationsscheman för beslutsfattande tvärs över enheter och geografiska områden.

5 självklara delar i en riskaptit

1. Riskaptitsuttalandet

Riskaptitsuttalandet är en positionering som sätter tonen och rationaliseringen för risktagandet. Det definierar varför vi tar en risk eller sätter gränser för beslutsfattande i relation till en risk.

2. Standardiserad skala som indikerar förväntningar på riskkontrollerna

Till exempel, en skala som sträcker sig från ’ovillig’ (att ta någon risk) till ’djärv’ (inte så petig om hantering) är ett sätt att uttrycka detta och hjälper till att sätta aptiten i relation till andra risker. Hitta vad som passar din organisation.

3. Tydlig styrning och hjälp kring förväntningar och implikationer

Det bör finnas en förtydligande text med nyckelexempel. Det är viktigt att det finns en kommunikation om hur riskaptiten förväntas påverka beslutsfattande.

4. Specifika villkor som förändrar aptiten (kritikalitetsvillkor)

I vissa sektorer och verksamheter kan det finnas kända variationer i omständigheterna som påverkar riskaptiten på ett eller annat sätt. Till exempel i utryckningsverksamhet eller nödhjälpsoperationer har livräddande situationer högre prioritet och riskacceptans – även om det innebär fara för den egna personalens liv och hälsa.

5. Villkor för eskalering

För att vara operativt relevant och göra det lättare att koppla till beslutsprocesser ska det finnas klara villkor för när ett beslut måste eskaleras till styrelsen eller ledningsgruppen.

Det finns helt enkelt kategorier av risk där ett beslut långt ut i verksamheten kan ha omfattande negativa effekter för hela organisationen, varumärket, eller till och med medlemmar i styrelsen och ledningsgruppen personligen. När ett eskaleringsvillkor är uppfyllt krävs notifiering eller eskalering i linje med vad riskaptiten säger.

Riskbeskrivningars effekt på utvärderingar och åtgärder

Strukturen på en riskbeskrivning är extremt viktig eftersom den sätter avgränsningar för risken och därmed också gör det möjligt att planera, delegera, och spåra relevanta kontroll-åtgärder. Ett vanligt misstag är att försöka reducera antalet risker genom att baka ihop flera stycken.

Det minskar inte den faktiska riskexponeringen – och den hypotetiska administrativa vinsten av att 'förenkla' genom att baka ihop tills man inte längre har relevanta planer, äts upp av den tid och resurs man får lägga på att släcka bränder man påstod sig ha kontroll på.

För att kunna agera mot en risk måste alltså riskbeskrivningen vara så exakt som möjligt.

Att vara mer precis innebär också att man har fler individuella risker att dokumentera (alltså planera mot). Det här är också varför det är viktigt att fokusera på nyckelrisker (identifierade genom riskutvärderingen) istället för att försöka planera mot alla möjliga och omöjliga risker.

Ett sätt att tänka på riskbeskrivningen är som en formel bestående av tre distinkta delar:

orsak + händelse + effekt

Som exempel: Företag i Storbritannien som är tungt investerade och beroende av tim-försörjande leveranskedjor ser stor osäkerhet och utmaningar när Storbritannien lämnar EU, om detta innebär att man förlorar tillverkningsdelarnas fria rörlighet.

Det är inte lämpligt att sätta en enda risk och kalla den ’Brexit’ och börja planera mot det. Riskerna finns i flera olika dimensioner av verksamheten och åtgärderna behöver vara precisa. För att hanteras effektivt måste begreppet ’Brexit’ brytas ned i relevanta och hanterbara delar.

Det här är sant i relation till även (för att nämna två exempel) bedrägeri/oegentligheter (intern, extern, kvittofusk, reseersättning, anställningsprocessen, och så vidare) och säkerhet (fysisk, tillgångar, IT, data, och så vidare). Ett abstrakt koncept med många olika meningar är svårt att planera mot på ett strukturerat sätt (eller ens få alla att ha samma förståelse för dess betydelse).

“Huvudet i sanden” är inte en fungerande riskhantering

Om det finns oro kring hur omfattande en riskhanteringsplan eller ett ’riskregister’ är (inte ovanligt i starkt centraliserade hierarkier där en liten grupp försöker hantera allt) så är lösningen inte att låtsas som om risken inte finns eller att lista en massa meningslösa kontrollåtgärder.

En potentiell lösning är att den centraliserade riskhanteringsplanen bara visar aggregerade ’rubrikrisker’, men att det finns en grundlig riskhanteringsplan under dessa för varje specialistområde, projekt, eller särskild händelse som matar rubrikrisken (till exempel en särskild riskplan, en Brexit plan, och så vidare). Själva detaljhanteringen har alltså delegerats till en specialistfunktion eller team som stöttar verksamheten men också följer upp och rapporterar.

Riskutvärderingen

Riskhantering handlar om att hantera osäkerhet och är därför en ’vetenskap’ av bästa gissningar och bästa försök, inte matematisk precision (med väldigt få undantag). Poängen med en risk-utvärdering är att urskilja vad som behöver vara prioriterat och vad som inte behöver vara det.

De flesta riskutvärderingar är inte baserade på objektiva data utan till någon grad beroende av den subjektiva tolkningen och bedömningen av någon form av specialist eller expert. Det här är viktigt att förstå eftersom användandet av ’formler’ och så vidare i riskvärderingar kan ge intrycket av någon form av objektivitet.

Det finns en obegränsad variation i fråga om vilken information som behöver samlas in och vad som behöver dokumenteras i en riskutvärdering. Så länge som ni har fastställt från början varför ni gör en riskhanteringsplan överhuvudtaget och förblir trogna till det målet, så är det relativt enkelt att hitta en balans mellan behoven kopplade till beslutsfattande, översyn, och externa krav och förväntningar. Den information ni behöver är den information ni behöver för att ta ett informerat beslut om vad som är prioriterade risker och hur ni ska hantera dem.

Riskrespons

Varför ska man dokumentera om man ändå inte tänker göra något åt saken? Därför att då vet andra att man övervägt och fattat ett beslut, och att man följer risken. Även här finns det ett obegränsat antal möjliga responser som en organisation kan välja och varje organisation kan utforma sin egen lista efter behov.

1. Undvika

Till exempel stänga ner verksamhet eller upphöra med en viss typ av aktiviteter eller transaktioner.

2. Överföra

Försäkring är ett sätt att överföra risk men det kan också handla om att arbeta genom underleverantörer. Notera att överföring skapar andra typer av risker som också måste hanteras.

3. Hantera

Försöka utföra riskåtgärder och kontrollmoment som reducerar sannolikheten att något händer oss och effekten på oss om det trots allt skulle hända.

4. Acceptera

Fatta ett informerat beslut att fortsätta med nuvarande exponeringsnivå då vi antingen inte kan eller vill göra något åt risken.

Riskvärdering

Det finns tre primära steg av riskutvärdering som har olika värde i processen eller rent av inget värde beroende på hur processen ser ut. Ofta kan det vara tillräckligt att bara arbeta med nettorisk.

1. Bruttorisk

Bruttorisk är risk ’som den är’ om inga kontrollåtgärder finns på plats alls. Många organisationer använder bruttorisk eller ett liknande begrepp i sina utvärderingar, men det är värt att fundera på om det tjänar ett verkligt syfte i er specifika process. I existerande verksamhet är det osannolikt att en risk existerar i ett vakuum och att det inte finns några som helst kontrollåtgärder på plats.

Bruttorisk är mest troligt användbart när man diskuterar nya verksamhetstyper, nya marknader, eller helt ny och nyutvecklad risk som kommer kräva resurser för hantering. Det är i princip ett argument för ’vi måste hantera detta, annars…’

2. Nettorisk

Nettorisk är ’risken som den är just nu’, med existerande hantering på plats och med tillräckliga resurser. Med andra ord är det en bedömning av vår riskexponering baserat på hur vi just nu arbetar med risken. Av de tre diskuterade stegen är nettorisk det mest omedelbart matnyttiga och det steg som bör vara närvarande i förenklade modeller för riskhantering.

Det är viktigt att riskägare förstår att kontrollåtgärder listade mot en risk ska ha en konkret effekt på sannolikhet och konsekvens om risken materialiseras. Det är också viktigt att kontrollstatusen hålls uppdaterad och att riskvärdering speglar förändringar.

3. Riskmål

Riskmål är risk ’som den kunde vara’ med planerade men inte ännu implementerade kontrollåtgärder på plats. Riskmål är ett uttryck för riskhanteringspotential och är beroende av tillräckliga resurser och stöd för att få kontrollen på plats. När en kontroll har implementerats uppdateras nettorisken för att spegla detta och fler framtida kontroller planeras om möjligt in.

Kontroller och testning

Kontroller kan vara standardiserade över en verksamhet eller lokala till en underenhet. Finanskontroller är ett exempel på vanliga standardiserade kontroller. Men även många personal, IT, och andra typer av kontroller syftar till att upprätthålla en minimumstandard över hela verksamheten och alla delar. Standardkontroller ska helst vara föremål för en periodisk försäkran med eventuella undantag och åtgärdsplan för undantagen redovisade.

I fråga om att utvärdera risknivåer är det viktigt (men tydligen inte alltid så lätt) att hålla isär kontroller som är på plats och planerade kontroller. Nettorisk är alltid baserad på vad som är på plats, riskmål på vad vi förväntar oss om/när ytterligare kontroller kommit på plats. Goda avsikter och önsketänkande är inte kontrollåtgärder. Icke implementerade kontroller som saknar resurser har ingen riskreducerande effekt.

Det är också lämpligt att utveckla metoder för att testa närvaro och effektivitet hos nyckelkontroller. Det är inte bara ett bra sätt att höja den interna tillförsikten, utan också ett bra underlag för revisionsgranskningar. Centraliserade och standardiserade kontroller kan komplettera granskningar men också för att förbereda dem över längre tid så att den negativa effekten på verksamheten från en omfattande granskning minimeras och enheten fortsätter fungera optimalt.

Tonen från toppen – glöm inte att kommunicera

Riskhantering ses ofta som något ’extra’ och syftet med att lägga tid och ansträngning på strukturerad riskplanering är ofta mindre klart för många i verksamheten.

Om det är styrelsens ansvar att säkerställa att riskhanteringen är tillräcklig, så är det ledningsgruppens ansvar att se till att riskhanteringen faktiskt fungerar, efterlevs, och att risk hanteras på ett ansvarsfullt sätt. Utan ett systematiskt tillvägagångssätt blir det väldigt svårt.

För att uppnå detta måste ledningen lägga tid och resurser på att:

- Kommunicera och upprepa sina förväntningar kring värdeskapande riskhantering i verksamheten (tänk och gör, inte kryssa i rutor)
- Tydligt kommunicera roller och ansvarsfördelning i relation till riskhantering på ett sätt som gör det solklart för alla delar av organisationen
- Kontinuerligt använda och följa upp på information från riskprocessen i andra ledningsprocesser (rapporter, möten, och så vidare)
- Leda genom exempel med värdeskapande riskhantering, istället för att hålla riskmöten bara för att
- Stödja och tillföra tillräckliga resurser för att riskhanteringen och internrevisionen ska kunna lämna effektivt stöd till organisationen

Sammanfattning

Den här guiden har försökt skapa kontext och insikter i olika nyckeldelar av riskanalysen och riskhanteringsprocessen. Ett viktigt förkrav för en bra riskhanteringsprocess är det grundläggande arbetet med organisationskultur och tonen från ledningen. Det här är också vad som håller liv och relevans i processen.

Det är ett ledningsansvar att hålla syftet med processen på rätt spår. Om syftet går förlorat förlorar den all mening och blir ett tidsslöseri som kan skapa distraktioner och negativt påverka mål och resultat. Om syftet bibehålls intakt kommer det kontinuerligt att stärka hur vi arbetar och reducera den tid och de resurser som krävs för att bekämpa brinnande problem som kunnat undvikas. Och det är en vinst för alla.

Vill du veta mer om hur din organisation kan effektivisera riskarbetet?

Läs mer här

Stratsys är ett SaaS-bolag som grundades år 2000, med målet att förenkla arbetslivet för företag och organisationer. Sedan dess har bolaget utvecklat en digital plattform, med 10 branschanpassade produkter inom områden som strategisk planering, GRC och hållbarhet. Stratsys strävar efter att ge verksamheter rätt förutsättningar att nå sina mål, med verktyg för planering, genomförande och uppföljning.

För mer information besök:
stratsys.com

Stratsys