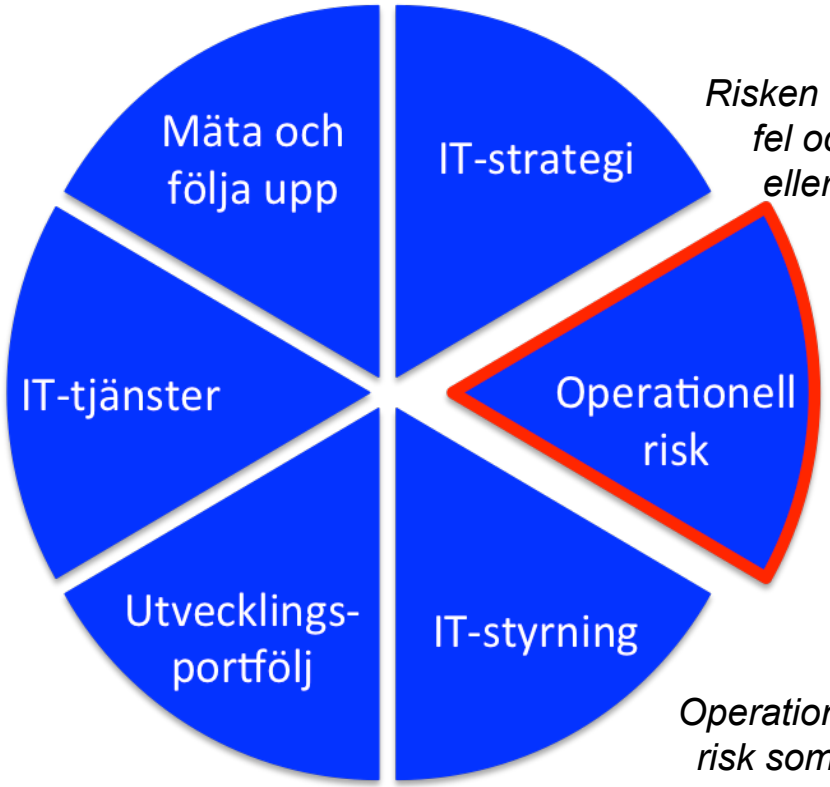
SYNLIGGÖRANDE OCH HANTERING AV OPERATIONELLA RISKER

- OPERATIONELLA RISKER
- MODELL
- BILAGOR

VI SYNLIGGÖR OCH HANTERAR OPERATIONELLA RISKER



Definition – operationell risk:
Risken att förluster uppstår på grund av fel och brister inom processer, teknik eller kompetenser eller beroende av externa faktorer (efter Basel II)

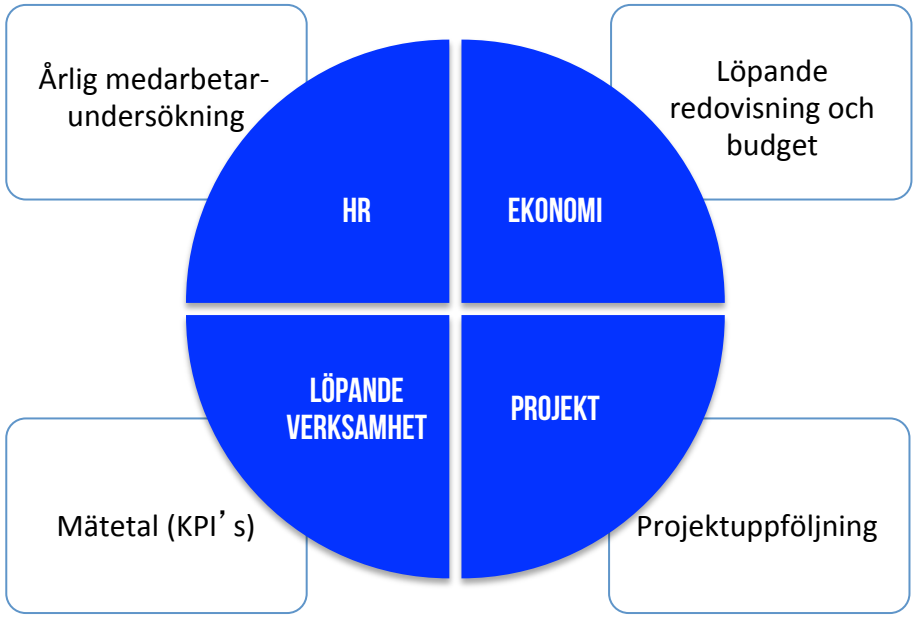
Operationell risk kan även omfatta annan risk som bedrägeri, legala risker, fysiska risker och miljörisker

OPERATIONELLA RISKER – EXEMPEL

- Flera nordiska organisationer drabbas av haverier hos en IT-partner och verksamheten avstannar helt eller delvis under ett dygn
- Ett universitetssjukhus får ställa in sina operationer pga. interna IT-störningar
- Flera myndigheter har problem då stora IT-projekt inte fallit ut som planerat
- En nordisk bank skriver av 750 MSEK pga. resursbrister och styrning
- Ett globalt läkemedelsföretag förlorar stora intäkter efter införandet av ett nytt affärssystem som inte var färdigtestat

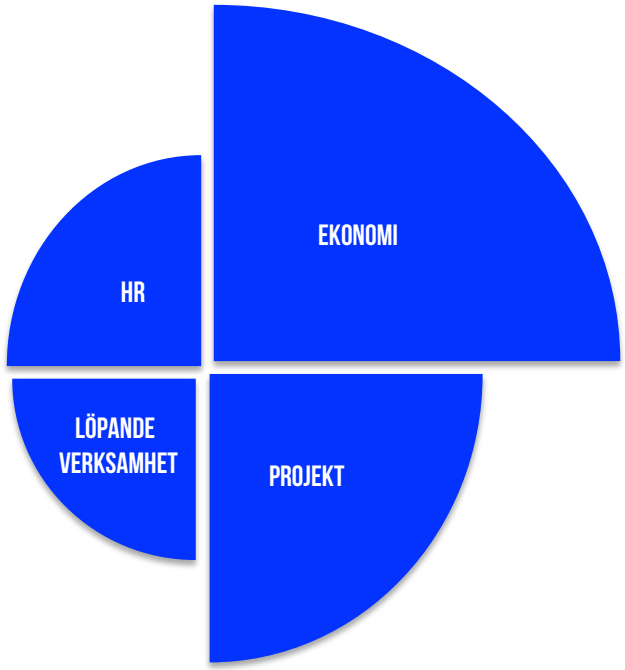
Sannolikt bara toppen av isberget (som publicerats i media under den senaste tiden)

LEDNING OCH OPERATIONELL RISKHANTERING



Generellt lägger företagsledningar och styrelser mindre vikt vid att analysera och följa operationella risker – i synnerhet avseende IT. I bästa fall finns en verksamhetsplan med balanserade och konkreta mål för IT. Fokus är på kostnader och operationella risker analyseras och följs inte specifikt.

LEDNING OCH OPERATIONELL RISKHANTERING

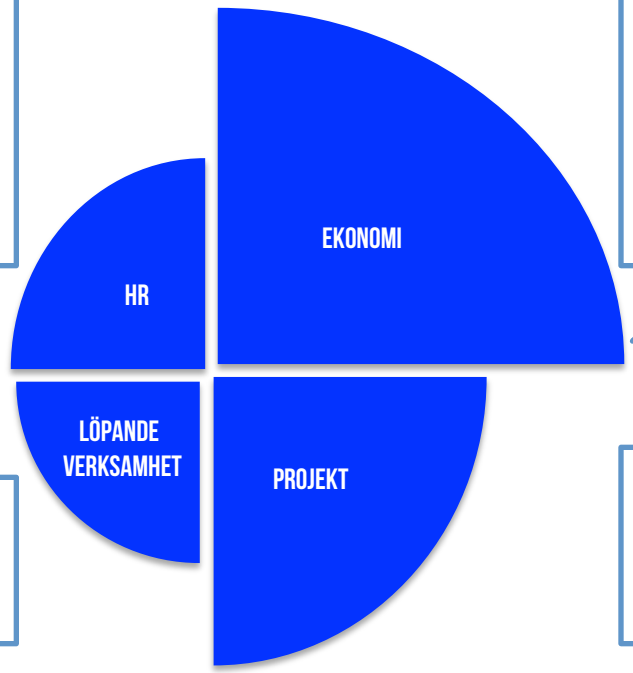


Problemet grundar sig delvis i att företagsledning och styrelse inser att IT har ett stort värde och är av strategisk natur, samtidigt som man uppfattar IT som komplext och svårt att förstå. Företräds dessutom IT av t ex CFO istället för CIO är det naturligt att fokus blir på kostnader.

LEDNING OCH OPERATIONELL RISKHANTERING

Det känns otillfredsställande att vi i styrelsen inte har kontroll på IT. Borde man inte ALLTID göra en ordentlig genomlysning av riskerna INNAN beslut om systembyten?

Jag har nog tittat på 25 möjliga företagsförvärv under min tid som VD – inte någon gång fanns en riktigt bra analys kring IT-riskerna i DD underlaget



Varför kan man bygga Öresundsbron enligt plan men aldrig lyckas med ett IT projekt?

Vilka frågor borde jag som styrelseledamot ställa till CIO för att fatta vilka risker vi de facto sitter med pga. IT

DET FINNS EN LÖSNING PÅ PROBLEMET

Vi **synliggör operationella risker** och möjliggör **snabb förbättring av riskhantering** vilket kan leda till:

- Minskade operationella risker vilket ger ekonomiska besparingar
- Ökad kvalitet vilket kan ge ytterligare kostnadsreduktioner
- Mer balanserad styrning av CIO/IT funktionen generellt
- Bättre kontroll/styrning av IT och operationella risker inom ledning och styrelse

Det finns olika tillämpningar (komplexa modeller som COSO och ICFR) drivna av myndighetskrav inom t ex den finansiella sektorn

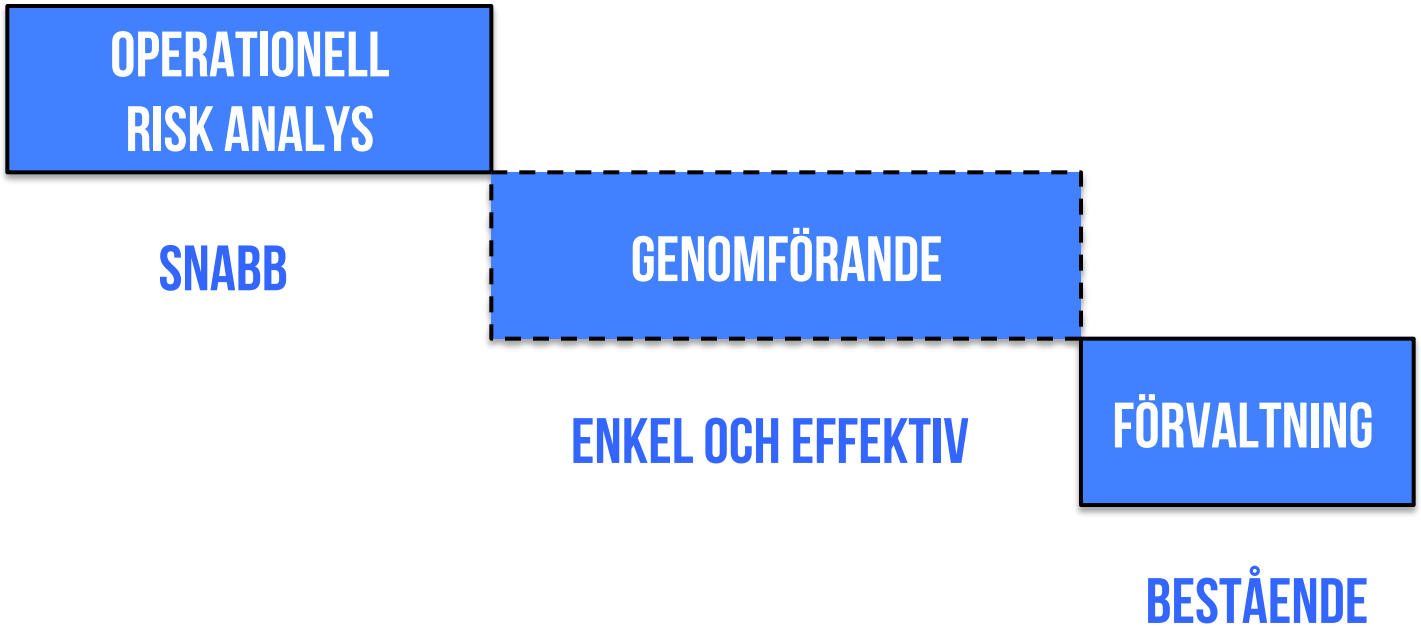
De flesta företag och myndigheter kommer dock långt med en **enklare och mer pragmatisk modell**

NÄR ÖVERVÄGA ATT GÖRA EN OPERATIONELL RISKANALYS?

- Inför strategiskiften
- Som del i due diligence processen i samband med företagsaffärer (köp eller försäljning av företag/verksamheter)
- Innan man fattar beslut att starta större utvecklingsprojekt eller vid systembyten
- Innan man fattar beslut att lägga ut delar av sin verksamhet
- Som nytillträdd SO eller CEO/CFO/CIO
- Om styrelsen eller ledningen inte känner att man har god kontroll på vilka de operationella riskerna faktiskt är

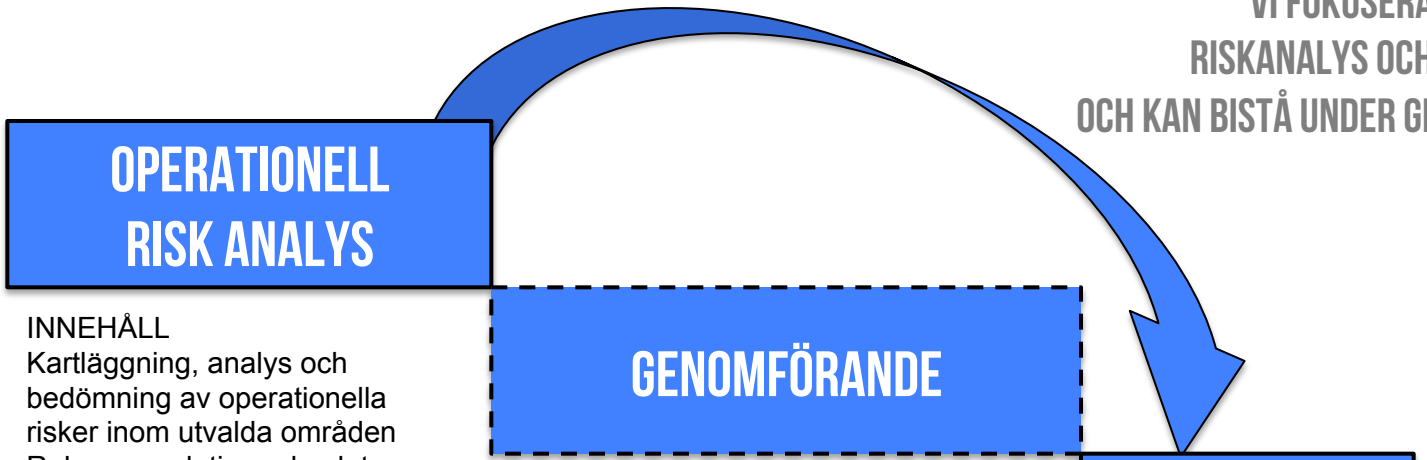
Verksamheter med **OPERATIONELL RISK** som en återkommande punkt på styrelsens dagordning, med ett uttalat ledningsansvar avseende operationell riskhantering och med riskindex som del i management rapporteringen ligger sannolikt långt framme

VÅR MODELL



VÅR MODELL

VI FOKUSERAR PÅ FASERNA
RISKANALYS OCH FÖRVALTNING
OCH KAN BISTÅ UNDER GENOMFÖRANDE



INNEHÅLL
Kartläggning, analys och bedömning av operationella risker inom utvalda områden
Rekommendationer beslut och åtgärdsplan

LEVERANS
Riskanalys i form av skriftlig rapport och lednings-presentation
Beslutad/rekommenderad åtgärdsplan i stort
Komplett dokumentation inkl. riskhanteringsmallar

TIDSOMFATTNING
4 veckor
(6-8 kalender veckor)

INNEHÅLL
Projektledning
Upphandlingsstöd
Genomförande (vissa specifika projekt)

LEVERANS
Enligt överenskommelse

TIDSOMFATTNING
2-3 månader/iteration

INNEHÅLL
Komplett styrmodell och ramverk for riskarbete
Löpande stöd till CIO, CFO och riskledning
Utbildning/dokumentation
Dokumenthantering

LEVERANS
Anpassas till kundbehov

TIDSOMFATTNING
Anpassas till kundbehov

OPERATIONELL RISKANALYS

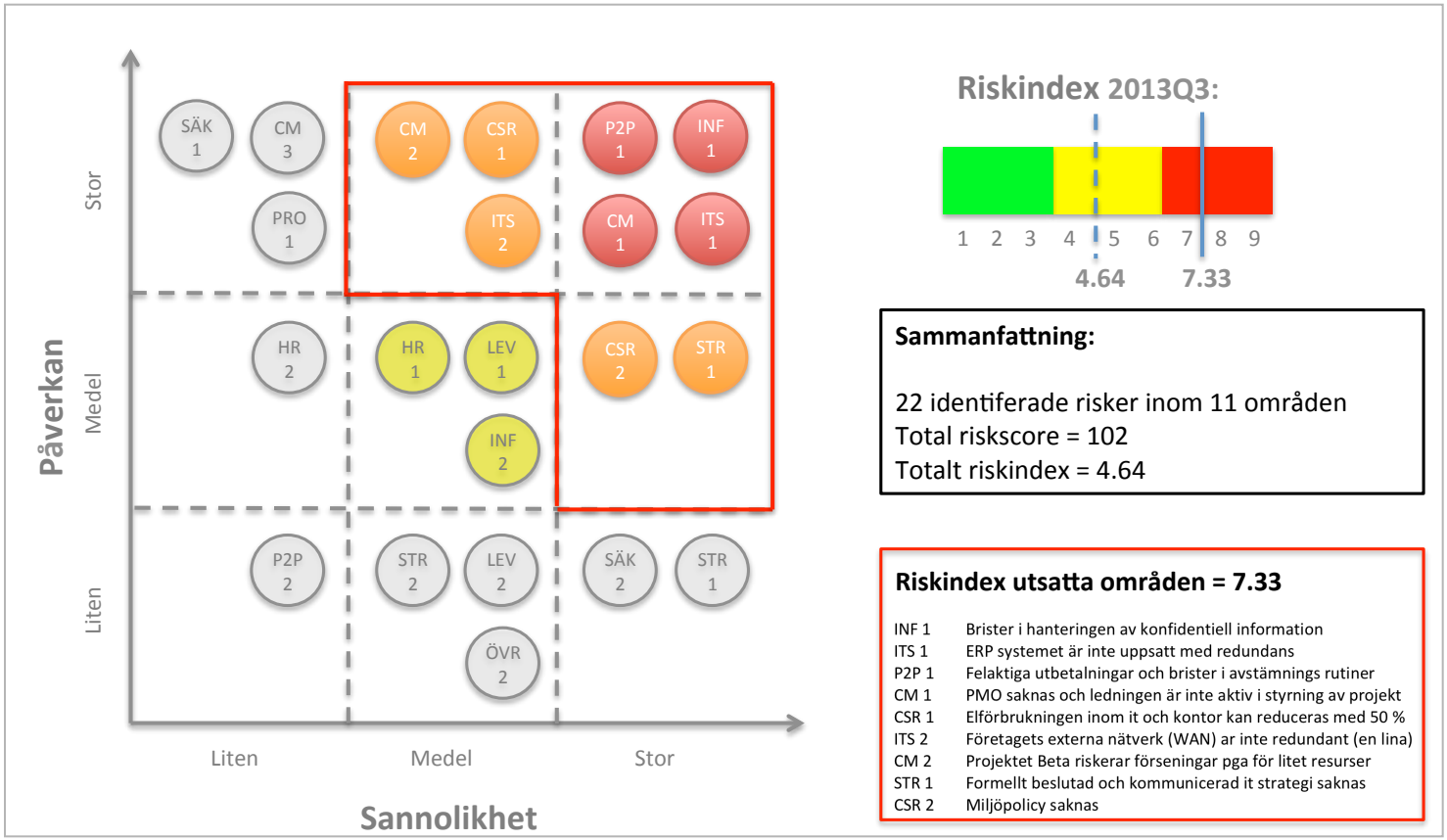
Under fasen **OPERATIONELL RISKANLYS** kartläggs, analyseras och bedöms risker avseende processer, system, kompetenser samt externa faktorer inom ett antal, tillsammans med kunden, utvalda områden som t ex;

Riskområde	Exempel analys och frågeställningar
CM – Change management	Förmåga/mognad att driva projekt, projektstyrningsmodell. Finns PMO. Levereras projekten enligt plan.
CSR – Miljö/CSR	Finns processer som minimerar energiförbrukning inom it och lokaler. Finns miljöpolicy. CSR. Pappersförbrukning.
HR – Human Resources	Personalomsättning. Kompetenskartlaggning, befattnings och rollbeskrivningar inom it. It organisation.
INF – Informationssäkerhet	Finns informations säkerhetspolicy. PUL. ''Tyst period''. Utskrifter och dokumenthantering. BYOD och dataintegritet.
LEV – Leverantörer	Leverantörer av it tjänster (drift, systemutveckling, moln), licenshantering, styrning och SLA, HW/asset management.
P2P – Procure to pay	Transaktionsintensitet, automatisk avstämning, har felaktiga eller sena betalningar skett, betalningsanmärkningar. Andra finansprocesser som record to report, order to cash, BI/DW, management rapportering med fler kan genomlysas
PRO – Processer inom it	Best practise. ISO. Förekommer brister inom it processer. Finns ITIL eller motsvarande. Förvaltningsorganisation, help desk och support samt beställarorganisationen.
STR – Strategi och styrning	Ledningens styrning av it. Finns en it strategi, målbild och vision. It planer och genomförande. Lokal it styrning och ledning. Dokumentation, beslutsprocess, rapportering, KPI.
SÄK – Säkerhet	Incidenthistorik och driftstörningar. Redundans och fall-back rutiner HW, SW, WAN/LAN, telefoni. Katastrofplanering. Externa granskningar. Back-up rutiner, behörigheter och lösenord. Säkerhetspolicy it. Skalskydd och inpassering.
ÖVR – Övrigt	Andra risker som identifierats.

Detta sker huvudsakligen genom intervjuer, workshops samt genom att analysera dokumentation/information och andra insamlade fakta

OPERATIONELL RISKANALYS

Slutrapporten innefattar bland annat ett styrkort med identifierade risker och riskindex vilket ger styrelse, ledning och CIO en god uppfattning om risksituationen



OPERATIONELL RISKANALYS

Slutrapporten innefattar också en konkret åtgärdsplan i stort med rekommendationer hur prioriterade operationella risker kan hanteras

Riskmitigering av prioriterade IT-säkerhetsrisker				
Identifierade risker att åtärda	Riskmitigering	Deadline	Ansvarig	Status
ITS 1 – ERP systemet är inte redundant vilket innebär att verksamheten är helt beroende av att befintlig IT-miljö fungerar	Omförhandla befintligt avtal med sourcing partner A. Lägg en gemensam plan for beställning och installation av dubbla driftsmiljöer	Q2 2014	CIO	
ITS 2 – Företagets externa leverantör av nätverkstjänster (WAN) är inte redundant (man har bara en data lina) vilket gör hela verksamheten sårbar	Förhandla möjligheten att komplettera med ett andra reserv nätverk genom leverantör A, alternativt upphandla redundans av leverantör B eller annan	Q2 2014	CIO	
ITS 1 ITS 2	Testa och utbilda extern och intern IT personal i restore procedures	Q2 2014	CIO	

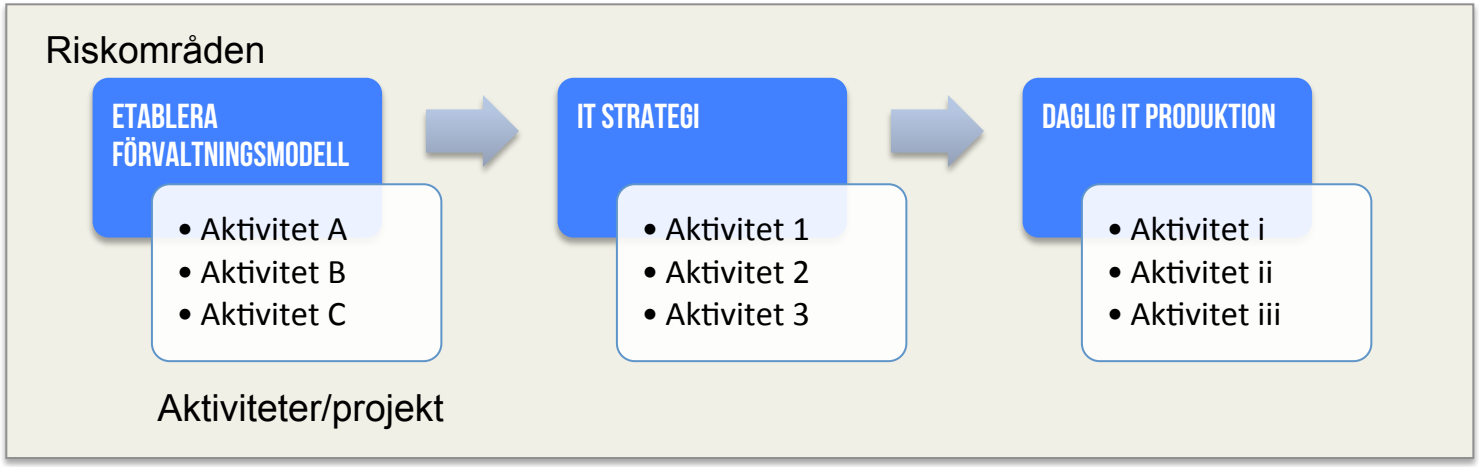
Figur: Utdrag från åtgärdsplan i stort

GENOMFÖRANDE

OPERATIONELL RISKANALYS avslutas med att resultatet, rekommendationer och en åtgärdsplan i stort presenteras för ledningen och beslut om riskhantering tas

Efter beslut och inför eller under **GENOMFÖRANDE** kan vi erbjuda:

- Övergripande projektledning och planering
- Stöd och rekommendationer vid val av underleverantörer
- Genomförande av vissa aktiviteter/projekt



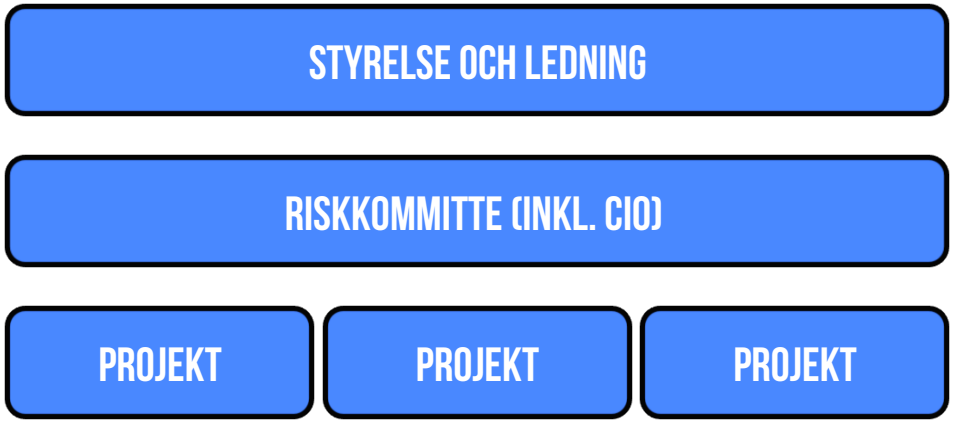
Figur: Konceptuellt exempel

FÖRVALTNING

I samband med **GENOMFÖRANDE** rekommenderar vi att man inför enkla men formella processer för fortsatt styrning och uppföljning av operationella risker

Avseende **FÖRVALTNING** kan vi bistå med tjänster som säkrar kontinuitet i riskarbetet;

- Etablerande av förvaltningsmodell
- Punktvis eller regelbundet stöd och utbildning
- Dokumentationshantering och löpande rapportering
- Årlig uppföljning med ledning/styrelse



EXEMPEL

#1 OPERATIONELL RISKHANTERING

Bakgrund

Ledningen i ett medelstort företag hade under en tre årsperiod lyckats halvera it kostnaderna genom att lägga ut drift, konsolidera flera IT-avdelningar och standardisera.

Genomförande

Styrelsen insåg att man som resultat också satt med stora operationella risker och valde att analysera läget. Det visade sig att affärssystemet och nätverket inte var redundant uppsatta hos it-partnern. Vid en störning skulle verksamheten drabbas (vilket skett). Det saknades viktiga processer och kompetenser inom IT samt stora brister i informations-säkerheten (t ex PUL, informationshantering och inpasseringsrutiner). En åtgärdsplan initierades och en särskild riskkommitté inom ledningsgruppen bildades.

Resultat

Idag har företaget god kunskap om sina risker och man har kunnat reducera några av de mest påtagliga. Arbetet med fortsatt riskmitigering pågar och ledningen följer regelbundet risk index. Operationella risker finns på styrelsens agenda.

EXEMPEL

#2 OPERATIONELL RISKHANTERING – UTLAGD IT DRIFT

Bakgrund

Ett tjänsteföretag hade lagt ut produktion och förvaltning av sina IT system for att sänka sina kostnader. Samtidigt förlorade man kontrollen och den egna IT organisationen hade bristande erfarenhet att arbeta mot en extern leverantör. Styrningen baserades på ’’relation’’ snarare än formella strukturer, processer, avtal och affärsrelation.

Genomförande

Leverantören saknade ett antal processer och kompetenser vilket resulterade i att samma misstag drabbade kunden vid upprepade tillfallen med stora produktionsbortfall – incidenter som aldrig sammanställts. Ett enkelt ramverk for KPI rapportering och uppföljning av underliggande orsaker togs fram. Den interna IT organisationen utbildades i ITIL och satte upp en intern system förvaltning som kravställare mot leverantören.

Resultat

Radikalt förbättrad kvalitet i IT leveransen samt sänkta kostnader och möjlighet att omförhandla avtal alternativt byta leverantör.

FORMAL RISK FRAMEWORKS

The Basel II/III Directives for Banks and Solvency II Directive (≈ Basel accord for Insurance industry) includes ‘’Sound Practices for the Management and Supervision of Operational Risk’’ and ‘’Operational Risk - Supervisory Guidelines for the Advanced Measurement Approaches’’. Basically Basel II requires all banking institutions to set aside capital for operational risk.

COSO (Committee of Sponsoring Organizations of the Treadway Commission) issued Internal Control – Integrated Framework to help businesses and other entities assess and enhance their internal control systems. That framework has since been incorporated into policy, rule, and regulation, and used by thousands of enterprises to better control their activities in moving toward achievement of their established objectives.

ICFR (Internal Control for Financial Reporting) – According to AICPA, effective controls reduce the risk of asset loss and help ensure that plan information is complete and accurate, financial statements are reliable, and that the plan complies with laws and regulations.

BASEL II – EVENT TYPE RISK CATEGORIES

The following lists the official Basel II defined event types with some examples for each category:

1. Internal Fraud - misappropriation of assets, tax evasion, intentional mismarking of positions, bribery
2. External Fraud - theft of information, hacking damage, third-party theft and forgery
3. Employment Practices and Workplace Safety - discrimination, workers compensation, employee health and safety
4. Clients, Products, & Business Practice- market manipulation, antitrust, improper trade, product defects, fiduciary breaches, account churning
5. Damage to Physical Assets - natural disasters, terrorism, vandalism
6. Business Disruption & Systems Failures - utility disruptions, software failures, hardware failures
7. Execution, Delivery, & Process Management - data entry errors, accounting errors, failed mandatory reporting, negligent loss of client assets

VI ÄR SPECIALISERADE PÅ ATT STÖTTA CIO/IT-FUNKTIONER SOM INTE FUNGERAR OPTIMALT

- INTERIM CIO AND CHANGE MANAGEMENT
- OPERATIONELL RISK
- TURN-AROUND

FOR MORE INFORMATION

WWW.SENIORITEXECUTIVE.COM
BJÖRN OVAR JOHANSSON
OVAR@TELIA.COM
+46708259495