Riskkultur – fundamentet för en god riskhantering

KRISTIAN KALLENBERG

Kapitel 13, utdrag ur Risker och riskhantering i näringsliv och samhälle
Richard Wahlund (red.) 2016

ISBN: 978-91-86797-22-5

STOCKHOLM SCHOOL OF ECONOMICS
SSE INSTITUTE FOR RESEARCH

Riskkultur – fundamentet för en god riskhantering

KRISTIAN KALLENBERG

Inledning

Under de senaste årtiondena, framför allt de senaste tio åren, har det skett tydliga framsteg i utvecklingen av normativa ramverk och standarder för hur företag och organisationer bör arbeta med risker. Det är tydligt att många organisationer har anammat dessa och i högre grad än tidigare arbetar strukturerat med sin riskhantering. Ändå fylldes affärspress och svenska media mellan 2013 och 2015 av rapportering om ett stort antal företagskriser som visade på brister i riskanalys och riskhantering, efterlevnad av lagar och regler samt intern styrning och kontroll. Oavsett om det begåtts några brott eller ej är marknadens och allmänhetens syn på dessa händelser att detta är oetiskt, har skadat förtroendet för företagen och i vissa fall även fått finansiella konsekvenser.

Många frågar sig säkert hur dessa företagsskandaler och brister i riskhantering kunnat inträffa. Har företagen inte tydliga policyer som definierar och styr vad man som anställd och chef får och inte får göra? Regleras detta inte tydligt i styrande bolagskoder, etiska policyer och i hållbarhetsarbetet? Granskas bolagen inte av internrevision och externa revisorer som borde ha hittat dessa uppenbara fel och brister i hur företagen använder sina medel, representeras av de anställda och genomför upphandlingar och sourcingaktiviteter?

Uppenbarligen finns det inom vissa organisationer en diskrepans mellan hur man säger sig hantera dessa områden och hur man konkret arbetar med frågorna. Trots ökat tryck på transparens och ökade krav på *governance*, riskhantering och intern styrning och kontroll kommer olika missförhållanden gång på gång till ägarnas och allmänhetens kännedom. Det finns som jag ser det två huvudsakliga förklaringar: Antingen är det interna kontrollramverket felkonstruerat eller också efterlevs det av olika anledningar inte. Båda dessa förklaringar relaterar till organisationens riskkultur.

Detta kapitel behandlar begreppet riskkultur och syftar till att redogöra för hur man skapar förståelse kring en organisations riskkultur, hur denna riskkultur kan etableras och påverkas samt hur den ger förutsättningar för att lyckas med den formella riskhanteringen och därigenom möjliggör sänkta riskexponeringar. För att förstå en organisations riskkultur måste ett antal integrerande faktorer analyseras. I kapitlet diskuteras kontextens, organisationskulturens och individens roll för att förklara riskkulturen.

Riskkultur

En formaliserad riskhantering kan bara lyckas om den understöds av en värdemässig grund och en tro bland medarbetare och chefer på att den skapar värde för organisationen. Min erfarenhet som konsult och delaktig i olika kurser och utbildningar om riskhantering, intern styrning och kontroll visar att sådana värdegrunder ofta saknas eller åtminstone inte tillämpas.

Många riskchefer lyfter just ledningens bristande stöd och engagemang kring riskhanteringen som ett viktigt skäl till att man inte lyckas etablera en fullgod riskhantering inom sina bolag, vilket även understöds av studier på området (FSB, 2014). Många organisationer upplever snarast den formella riskhanteringen som administrativt tung, framdriven av krav från externa intressenter (t ex olika regleringar) och som ytterligare ett område för rapportering som inte skapar värde för organisationen.

Begreppet riskkultur

Begreppet riskkultur är inte entydigt definierat, utan ett flertal definitioner förekommer (IIF, 2009). En ofta förekommande definition är att riskkultur är ett system av värderingar och beteenden som formar beslut kring risk och riskhantering i interaktion med varandra. Riskkulturen påverkar beslut och aktiviteter i hela organisationen, bland chefer och medarbetare, informellt och formellt. Begreppet ställs ofta i relation till organisations- och företagskultur och är kanske den viktigaste faktorn för att etablera en god riskhantering och en god intern styrning och kontroll.

En formell riskhantering är verkningslös om organisationen inte dessutom lyckas etablera en god riskkultur. Uppenbarligen kan regler och styrande dokument missförstås eller misstolkas, med eller utan avsikt. Utan ett strukturerat arbete för att etablera en god riskkultur blir andra satsningar på formaliserad riskhantering mindre givande. Varje organisation kan sägas ha en riskkultur, men den fråga varje företagsledning bör ställa sig är huruvida denna är god och rätt utformad samt om den stödjer eller stjälper organisationens långsiktiga mål.

Motiv för riskhantering

Förespråkare för en mer informell approach till riskhantering menar ofta att kritiska risker i verksamheten bör hanteras i linjen vart eftersom de uppkommer, utan stöd av någon riskfunktion eller enhetlig metod för riskhantering. Under de senaste tio åren har dock olika styrande ramverk och metoder för en mer övergripande och enhetlig riskhantering vunnit ökad acceptans i många organisationer.

Den riskkultur som finns inom en organisation ger förutsättningarna för etableringen av en formell riskhantering. En god riskkultur med god förståelse för organisationens riskexponering underlättar det formella riskhanteringsarbetet och gör strategiska beslut som rör riskhanteringsaktiviteter mer accepterade. På motsvarande sätt ger organisationer som brister i riskkultur, medvetet eller omedvetet, utrymme för risktagande som helt eller delvis går utanför vad som kan anses som acceptabla risker.

Riskhantering utifrån krav och behov

Under de senaste årtiondena har nya risker som har att göra med t ex globalisering, digitalisering, IT, terrorism, outsourcing, massmedial bevakning, en ständig förändring och ökad komplexitet i affärslivet ställt nya krav på dagens organisationer. Delvis till följd av denna utveckling har nya legala och regulativa krav som rör riskhanteringen ställts på organisationer inom många branscher. Det är viktigt att poängtera att företag och organisationer har olika drivkrafter att utveckla sin riskhantering. Förenklat kan man säga att utvecklingen sker i ett samspel mellan externa och interna intressenters krav och behov å ena sidan och organisationens riskkultur å andra.

Ur ett behovsperspektiv kan riskhantering ses som ett verktyg för att förbättra den operativa verksamheten, effektivisering, ökad produktivitet och förhöjd kvalitet. Området gränsar till kontinuitetshanteringsarbete, begränsning av avbrott. Mål kring lägre risker i produktion och leveranser, säkerhet och kontinuitet har i ökande grad blivit viktiga skäl till att organisationer etablerar och formaliserar riskhanteringen. Också externa intressenter som ställer krav på organisationen värderar god kontroll över sina risker och ett etablerat ramverk för riskhanteringen högre än tidigare.

På kravsidan finns både frivilliga åtaganden och lagstadgade krav. Ofta ställer styrelse och ägare krav, men även många andra är uttalade kravställare när det gäller riskhanteringen. Redovisningsregler, kapitaltäckningskrav för bank-, finans- och försäkringsbolag, hållbarhetsredovisningar och ökade krav på certifieringar och olika standarder (t ex ISO 31000) gör det formella riskhanteringsarbetet viktigare idag än tidigare. Flera ramverk för riskhantering är tydligt normativa och ställer krav på vad organisationer bör arbeta med för att uppnå en god riskhantering, och delvis hur.

På vilket sätt är riskkultur viktigt?

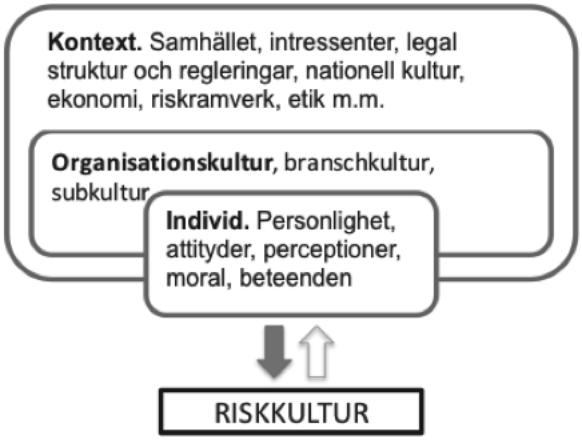
Brister i riskkulturen ger enskilda individer eller grupper inom en organisation utrymme att överträda lagstadgade krav eller interna krav som beslutats och konkretiserats genom policyer och riktlinjer. Dessa brister kan visa sig genom den omgivande organisationens underlåtenhet att agera mot beslut

och aktiviteter som är felaktiga, eller åtminstone tveksamma ur etiskt perspektiv. Riskkultur, eller snarare brist på sådan, har sagts vara en viktig förklaring till den finansiella kris som drabbade världsekonomin under 2008 och 2009 (FSB, 2014). I efterhand har det blivit tydligt att dessa brister och överträdelser både förekom inom den formella riskhanteringen, med brister i styrning, kontroller och risklimiter, t ex rörande krediter och säkerheter - men även att dessa överträdelser skedde i en risksökande kultur som tillät det, inte så sällan med ledningars och styrelsers goda minne.

Den tongivande Walkerrapporten drog slutsatsen att [t]*he principal emphasis is in many areas on behaviour and culture*, och understryker vikten av strukturerat och medvetet arbete för att förbättra riskkulturen och förändra beteendet för att undvika liknande kriser i framtiden (ICAEW, 2009). Finanskrisen ledde till stor obalans i de finansiella systemen internationellt. Som resultat ser den regulativa miljön helt annorlunda ut i dag i efterspelet av krisen, med tydliga krav på kapitalreserver och krav på kontinuerlig och strukturerad analys och rapportering av risker. Dessa krav understryker vikten av riskkulturens betydelse för att lyckas med den formella riskhanteringen och har lett till ökat fokus på detta.

Riskkulturens byggstenar

Som tidigare poängterats så skapas riskkulturen i interaktion mellan olika aktörer och intressenter och tydliggörs genom olika beteenden och beslut. Dessa beteenden och utfallet av olika beslut sker i ett sammanhang och i en organisation, och har även sin grund i individers (eller grupper av individers) värderingar och attityder till risk och risktagande. Utöver konkreta beslut, som kan vara direkt eller indirekt kopplade till risker, och observerade beteenden bland individer eller grupperingar inom en organisation, finns det ett antal områden som kan analyseras för att få en bättre förståelse av organisationens riskkultur. För den fortsatta diskussionen konkretiseras detta i figur 1 på nästa sida.



Figur 1. Riskkulturens byggstenar.

Kontexten

Kontexten påverkar organisationens förutsättningar och därmed även olika beslut som rör riskkulturen. För att lyckas såväl med att etablera en god riskkultur som med den formella riskhanteringen har det visat sig viktigt att förstå och beakta både kontexten och olika intressenter (Hodges, 2000; Ward, 2001). Kontexten påverkar både organisationskulturen – direkt och indirekt – och individers attityder och beteenden, samt i förlängningen även beslut kring risker och hantering av dessa.

Vissa kontextuella faktorer är således direkt styrande och påverkar organisationen (t ex genom reglering och lagstiftning, generellt eller rörande specifika riskområden), medan andra påverkar hur olika individer påverkas av kontexten och uppfattar och agerar på risker och riskrelaterad information, vilket i sin tur påverkar organisationen. Individens roll som medskapare av riskkulturen behandlas senare, men det är viktigt att nämna att olika nationella, kulturella, sociala, ekonomiska och konkurrensrelaterade kontextuella aspekter kan förklara både individuella och kollektiva reaktioner och beslutsfattande och beteenden kring risk.

Dessa kontextuella aspekter formas ofta av olika intressenter, som kan sägas ha fått större betydelse och inflytande på organisationer de senaste

decennierna (Borglund, 2006). Ur ett riskhanteringsperspektiv har det visat sig vara av stor vikt att inkludera olika intressenter, både för den riskhantering som rör samhällsrisker och den som bedrivs i organisationer och företag (Löfstedt & Vogel, 2001; Slovic, 2000). Det ligger inte inom ramen för detta kapitel att göra någon mer omfattande analys av de kontextuella faktorer som påverkar riskkulturen, men det finns ett antal intressenter som formulerat krav på styrande lagar och regleringar kring riskhantering, och andra som utvecklat riskramverk som fått stor betydelse för dagens riskhantering.

Svensk kod för bolagsstyrning (SOU, 2003) och Årsredovisningslagen (ÅRL,1995) ger råd och ställer lagkrav kring riskhantering. De understryker att det är ledningens och styrelsens ansvar att risker hanteras, att aktiviteter och processer är effektiva och ändamålsenliga, och att riskhanteringen kopplas ihop med den övergripande styrningen och den interna kontrollen av en organisation.

COSO-ramverket växte fram efter krav på förbättrad genomlysning och hantering av risker i efterdyningarna av ett antal redovisningsskandaler, bland annat Enron. COSO, Committee of Sponsoring Organizations of the Treadway Commission, utvecklades för att hantera finansiell rapportering, men den holistiska standard man nu tillämpar omfattar intern styrning och kontroll (inklusive intern finansiell kontroll), internrevision och *enterprise risk management* (COSO, 1992, 2004).

För finansbranschen ökade kraven på strukturerad riskhantering efter finanskrisen, och EU har genom direktiv och råd, bland annat Basel- och Solvencedirektiven, utvecklat ramar och regler kring kapitalreserver och hantering av olika typer av risker för banker och finansiella institut samt för försäkringsbranschen. Ur ett nationellt svenskt perspektiv operationaliseras de krav som definierats av EU bland annat genom Finansinspektionens föreskrifter och allmänna råd om styrning, riskhantering och kontroll (FFFS 2014:1).

Finansinspektionen (FI) poängterar vikten av begreppet riskkultur och understryker att de organisationer och institut som är tillståndspliktiga gentemot inspektionen bör sträva efter en integrerad riskkultur som omfattar hela organisationen, där alla medarbetare är fullt medvetna om sitt eget ansvar för riskhanteringen. FI understryker att riskhanteringen inte enbart bör

överlåtas till riskspecialister eller kontrollfunktioner, utan att organisationen bör sträva efter ett gemensamt synsätt på målbilden för att skapa en effektiv riskkultur.

ISO 31000 är en internationell standard, men ingen certifiering. Den utgör ett ramverk kring styrning och processer för riskhantering, och den rekommenderar att organisationer utformar, implementerar och fortlöpande utvecklar ramverket för att integrera riskhanteringsprocessen i organisationens övergripande styrning, strategi och planering, ledning, rapporteringsprocesser, policyer, normer och kultur. Kulturbegreppet är inte specifikt kopplat till riskkultur utan snarare till organisationens formella och informella organisationskultur (ISO, 2009).

Förordning om intern styrning och kontroll (FISK, 2007) tydliggör de krav som åligger myndigheter. Även statliga bolag, kommuner och landsting tillämpar varianter av dessa krav. En viktig del i den interna styrningen är att organisationen regelbundet ska genomföra en riskanalys, där risker identifieras, analyseras och hanteras. Utgångspunkten är de mål som avkrävs och sätts upp av organisationen, och en del riktas även mot otillbörlig påverkan och bedrägerier.

Organisationskultur

Liksom riskkultur visar sig organisationskultur genom återkommande beteenden som delvis har sin grund i olika värderingar och individers attityder. Dessa faktorer är till viss del föränderliga. Kulturen är inte konstant utan relaterar – som det latinska ordet *cultura* anger – till odling, bearbetning och bildning, och den utvecklas i ett samspel, i en ständigt återkommande interaktion med de som är delaktiga i och formas av den. Kulturen är således föränderlig och något mer än statiska värderingar.

Riskkultur kan ses som en delmängd av det mer övergripande begreppet organisationskultur. Riskkulturen tydliggör organisationens kollektiva inställning till risk och dess riskaptit samt tar sig uttryck i förmågan hos organisationen (eller en del av den) att hantera risk. I diskussionen av de kriser som flera stora företag upplevt de senaste åren, t ex SCA, Stora Enso och Telia, liksom flera finansinstitut under finanskrisen, såsom Carnegie, HQ bank och Swedbank, har brister i organisationskulturen med avseende

på risktagande nämnts som en viktig förklaring till dessa och andra krisers uppkomst (Holton, 1998; Kallenberg, 2007).

Man kan se mönster kring risktagande inom vissa branscher. Ambitionsnivån och mognaden rörande riskhanteringen kan påverkas av branschtillhörighet eller nationell lagstiftning som påverkar specifika riskområden (McCrae & Balthazor, 2000; Ward, 2001). Skillnader i riskkultur och mognad beträffande riskhantering kan även förklaras av riskuppfattningen hos de personer som söker sig till branschen, de specifika arbetsuppgifterna, arbetets karaktär och belöningsmodeller, men även organisationskulturen (ICAEW, 2009).

Att organisationer, industrier och branscher skiljer sig i sin syn på risk och hur de värderar och arbetar med den är både tydligt och rätt naturligt, och har sin grund i verksamhetens karaktär samt historiska faktorer. Tyngre industri, kärnkraftsindustri, petrokemi m fl har arbetat mer formaliserat med riskhantering under lång tid på grund av karaktären på sin verksamhet. Detta har drivits fram av lagkrav, regleringar och ett ökat ansvarstagande för verksamhetens påverkan, vilket i sin tur drivits på av det omgivande samhället och närsamhället och granskat av allmänheten och media.

Ledarskapets betydelse

Riskhantering handlar om styrning mot definierade mål. COSO-ramverket lyfter vikten av ett tydligt mandat från ledningen och styrelsen genom en tydligt definierad, uttalad och kommunicerad *tone at the top*. ISO 31000 understryker att etableringen av en god riskkultur och fungerande riskhantering kommer att misslyckas om den inte har styrelsen och ledningens stöd.

Ett första steg är således att förankra ledningen i arbetet med riskhanteringen och få dem att förstå varför arbetet är viktigt och på vilket sätt det skapar värde. Genom att peka på ett antal olika huvudriskområden inom organisationen bör man bilda sig en uppfattning om ledningens och styrelsens attityder till riskerna samt av vilken förståelse som finns för i steg ett hur de kan slå mot uppsatta mål och i steg två hur de bör hanteras. Ledarskapet för en förändring av riskkulturen bör definieras med en plan och formaliseras genom styrande dokument samt en definition av vilka risker organisationen vill och kan ta, och detta bör sedan förankras bland mellanchefer och medar-

betare i organisationen genom utbildning, kommunikation och uppföljning.

Utgångspunkten för att etablera en god riskkultur är således både en formalisering av arbetet och en etablering av bärande och väl kommunicerade normer i linje med etiska policyer och värdegrunder. Det är ofrånkomligen så, att för att skapa en förtroendeskapande riskhantering behövs det ett tydligt mandat och en tydlig agenda som stöds och förmedlas av ledningen.

Individen

Riskperceptioner – individers uppfattningar om risk – har studerats inom många discipliner såsom psykologi, sociologi, statsvetenskap, ekonomi m fl. Utifrån riskkulturbegreppet och de kritiska faktorer som påverkar skapandet av en god riskkultur begränsas diskussionen här till att det finns skillnader i riskuppfattningar. Dessa påverkar attityder och värderingar kring risker och riskrelaterad information, och i förlängningen även beteenden och beslut, både individuellt och organisatoriskt.

Forskningen om risk och riskperceptioner fick ökat fokus under 1970-talet, som konsekvens av en ökad oro för kärnkraft, miljögifter och olika tekniska risker (Löfstedt, 2005). Utgångspunkten var från början samhällsorienterad och fick betydelse för en rad olika områden, så väl inom beslutsfattande på samhällsnivå som i organisationer och företag (Sjöberg, 2003; Slovic, 2000). Forskningen har det gemensamt att den grundar sig i olika psykologiska och personlighetsrelaterade aspekter, som påverkar och påverkas av sociala, politiska, kulturella, ekonomiska och institutionella faktorer.

Kontroverser som rör risker och riskhantering har ofta sin grund i individers olika riskperceptioner och vad som ibland anses vara irrationella reaktioner kring risk. Den psykometriska modellen utvecklad av bland annat Fischoff et al. (1978), Douglas och Wildavskys kulturteori (1982) och Tverskys och Kahnemans arbeten (t ex 1974, 1981) med subjektiva sannolikheter har också haft mycket inflytande på förståelsen för beslutsfattande omkring risk och riskhantering (Kallenberg, 2008).

Antropologerna Douglas & Wildavskys kulturteori (1982) är särskilt intressant att lyfta fram för att belysa riskkulturbegreppet som det behandlas i detta kapitel. Teorin visar att individers riskuppfattningar, och därmed deras reaktioner på riskrelaterad information, skapas och påverkas av olika kul-

turella och sociala faktorer samt att det finns likheter och olikheter i riskuppfattning mellan grupper av individer. Det är rimligt att anta att detta är en god förklaringsmodell även när det gäller branschspecifika och subkulturella uppfattningar om risk (McCrae & Balthazor, 2000).

I arbetet med att skapa en god riskkultur är det viktigt att förstå att olikheter kring riskperceptioner finns och att kunskapen om dessa olikheter bör ligga till grund för utformningen av den styrning som avser att förflytta riskkulturen i önskad riktning.

Utöver riskperceptionerna är det viktigt att inte bara förstå och ta hänsyn till individernas värderingar ur etiskt perspektiv, utan också analysera dessa för att bilda sig en uppfattning av hur väl de stämmer överens med den värdegrund som organisationen vill stå för och arbetar med. Genom att skapa förståelse för individernas etiska värderingar och moraliska ställningstaganden, särskilt när det gäller risktagande men även mer generellt, kan organisationen identifiera potentiella riskområden, rikta utbildningsinsatser och arbeta strukturerat med att förändra synsätt och arbetssätt. Denna analys bör även ligga till grund för organisationens utformning av sitt interna kontrollramverk och sitt riskhanteringsarbete.

Mot en god riskkultur

Vad utmärker en god, eller kanske ännu hellre effektiv riskkultur? Enkelt uttryckt är den en kollektiv uppfattning om hur risker och riskhantering bör hanteras som ligger i linje med organisationens uppsatta mål. En god riskkultur gör det möjligt för en organisation att fatta korrekta och informerade beslut om risker. En god riskkultur är således normativ, eftersom den definierar vad som är rätt och fel och ställer handlingar, kommunikation och beslut i relation till denna norm. En god riskkultur är tydlig och transparent, och medarbetare på olika nivåer vet vad som förväntas av dem när det gäller hantering av risker och vad som är ett acceptabelt risktagande. För att lyckas med detta måste värderingar och etiska principer som gäller risker till viss del formaliseras genom styrande dokument och direktiv.

I ett ännu mer formaliserat perspektiv kan riskerna och acceptansen för

dem tydliggöras genom en definierad riskaptit (vilka och hur stora risker man är *villig* att ta) som relateras till organisationens riskkapacitet (hur stora risker organisationen *kan* ta). En definierad riskaptit fungerar som ett stöd för att nå uppsatta mål och utgör ett underlag för definition av risklimiter för särskilt kritiska risker. Den kan också vara en viktig del i styrningen och prioriteringen av riskhanteringsaktiviteter utifrån riskexponering inom olika riskområden och målbilder (FFFS, 2014). Riskaptiten är inte konstant utan ändras i takt med omgivningen, kontexten, affärsmiljön, behov inom och krav på verksamheten samt organisationens målsättning. Riskaptiten och besläktade risklimiter för specifika risker bör i möjligaste mån relatera till andra prestationsmål inom verksamheten såsom KPI:er och andra kvantifierade mått.

För att lyckas skapa en formaliserad riskkultur som ger avtryck i organisationen måste relevanta beslutsfattare stå bakom denna, och det måste vara tydligt var ansvaret för att hantera riskerna ligger. Risker bör ha en utpekad riskägare som tar ansvar för att riskerna hanteras i linje med den riskhanteringsstrategi ledningen beslutat om eller styrelsen ställt krav på (t ex att acceptera eller mitigera en risk). Ur ett styrningsperspektiv bör riskansvaret även kopplas till individers, enheters och ledningsgruppers mål, t ex genom målkort.

En hantering i linje med de processer man etablerat och de gränsvärden man satt upp bör premieras, och på samma sätt bör icke-hantering av riskerna eller underlåtenhet kring att hantera dem få någon form av sanktion eller konsekvens. Genom att koppla riskhanteringen till styrning och övriga krav påverkar man verksamheten i riktning mot den målbild man har, både vad gäller specifika risker och kring organisationens övergripande riskexponering. Ur styrningsperspektiv bör man även etablera individuella incitament som kan leda till ett mer engagerat riskhanteringsarbete (FSB, 2014).

Värdegrund och strategi

Analysen av en organisations risker och utformningen av ett ramverk för riskhantering bör alltid ställas i perspektiv till organisationens strategi, målbild och definierade värdegrund. Värdegrunden kompletterar organisationens strategi och bör även vara styrande för uppförandekod, policyer,

instruktioner och riktlinjer. För att lyckas etablera en god riskkultur är det viktigt att värdegrund, strategi, målbild och taktiska och operativa aktiviteter hänger ihop. Med taktiska och operativa aktiviteter menas här även aktiviteter, kontroller och åtgärder som syftar till att hantera risker i linje med en definierad riskaptit.

Definierad riskhantering

Med definierad riskhantering avses ett för organisationen anpassat riskramverk. Detta kan grundas i något av de styrande ramverk som diskuterats tidigare, och bör i huvudsak konkretisera en styrningsmodell, där roller och ansvar för riskhanteringen (inklusive styrande principer, policyer och riktlinjer) definieras i enlighet med organisationens befintliga besluts-, arbets- och delegationsordning. Riskramverket ska även innehålla en enhetlig process för riskhanteringen, som tydliggör hur organisationen ska genomföra riskanalyser, med en för organisationen anpassad process för att identifiera, värdera, hantera och rapportera risker till olika intressenter.

Etablering av riskkulturen

För att nå den uppsatta målbilden med riskkulturen bör organisationen genomföra en analys där nuläget analyseras med den definierade målbilden i åtanke. Denna analys bör inriktas mot både riskkulturen och det befintliga ramverket. Det finns många verktyg för att genomföra en sådan analys, som kan inriktas mot individer, grupper av individer och organisationen som helhet. Den kan också utgå från riskramverkets utformning och funktionalitet genom att analysera t ex överträdelser, brott, kontinuitet i produktionen, kvalitetsbrister, skador på personalen, motivation eller medarbetarnas syn på sin arbetssituation och sina chefer.

Genom självskattningar eller andra undersökningsmetoder kan medarbetares inställningar till olika områden, riskperceptioner och etiska och moraliska ställningstaganden, ge en bild av i vilken grad medarbetarna delar den värdegrund och den riskkultur som definierats för organisationen. Detta skapar förståelse för var avvikelser mot uppsatta mål sannolikt kommer att

uppstå och hur insatser bör riktas. Här skulle t ex den i kapitlet om anseenderisker och dataskydd presenterade metoden kunna användas.

Insatser kan t ex vara att förtydliga det styrande ramverket med justeringar i policyer och instruktioner, en mer konkretiserad och bättre förmedlad riskaptit, utveckling av *key risk indicators* och uppdaterade kontroller och uppföljningar av särskilt kritiska riskområden. För att lyckas med insatser och för att etablera och förändra riskkulturen är det viktigt med uppföljning och kommunikation. Kommunikation angående risker kan vara en särskild utmaning och kräver god förståelse för kontextuella, organisatoriska, individuella och riskspecifika faktorer.

Den ofta citerade professor Peter Drucker (2001) menar att *culture eats strategy for breakfast* och detta tror jag stämmer i hög grad när det gäller att säkerställa en god riskhantering. Utan förståelse för och aktivt förändringsarbete kring riskkulturen är det svårt – så gott som omöjligt – att etablera en riskhantering som skapar värde.

En effektiv riskhanteringsprocess måste förankras i organisationen genom ledningens och styrelsens stöd och uttalade och kommunicerade prioritering av området. Riskhanteringsprocessen kan endast skapa värde om den också på ett strukturerat sätt kopplas ihop med övrig styrning av organisationens kultur genom strategiarbete, affärsplanering, målsättning och budgetering, i samspel med organisationens kontext och med förståelse för och i förankring hos de individer som utgör organisationen

Referenser

Borglund, T. (2006). *Aktieägarvärden i Fokus*. Stockholm: Stockholm School of Economics.

COSO (1992). *Internal Control Integrated Framework*. New York: The Committee of Sponsoring Organizations.

COSO (2004). *Enterprise Risk Management – Integrated Framework*. New York: The Committee of Sponsoring Organizations.

Douglas, M. & Wildavsky, A. (1982). *Risk and Culture: An Essay on the Selection of Technological and Environmental Dangers*. Berkeley: University of California Press.

Drucker, P. (2001) *The Essential Drucker.* New York: Harper Business.

FFFS (2014:1). *Finansinspektionens föreskrifter och allmänna råd om styrning, riskhantering och kontroll i kreditinstitut*. Stockholm: Finansinspektionen.

FSB (2009). *Guidance on Supervisory Interaction with Financial Institutions on Risk Culture*. Financial Stability Board.

FISK (2007). *Förordning (2007:03) om intern styrning och kontroll*. Stockholm: Sveriges Riksdag.

Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S. & Combs, B. (1978). How safe is safe enough? A Psychometric study of attitudes towards technological risks and benefits. *Policy Sciences*, 9(2), 127-152.

Hodges, A. (2000). Emergency risk management. *Risk Management: An International Journal*, 2(3), 7-18.

Holton, G. Y. (1998). The new climate of risk. *Treasury Management International*, 69, 24-28.

ICAEW (2009). *A Review of corporate governance in UK banks and other financial entities*. London: Institute of Chartered Accountants in England and Wales.

IIF (2009). *Reform in the Financial Services Industry: Strengthening Practices for a More Stable System*. International Institute of Finance.

ISO (2009). *Risk Management – Guidelines on principles and implementation of risk management*. Geneva: ISO 31000.

Kallenberg, K. (2007). The role of risk in corporate value: A case study of the ABB asbestos litigation. *Journal of Risk Research*, 10, 1007-1025

Kallenberg, K. (2008). *Business at Risk, Four Studies on Operational Risk Management*. Stockholm: Stockholm School of Economics.

Löfstedt, R. E. (2005). *Risk Management in Post-Trust Societies*. New York: Palgrave Macmillian.

Löfstedt, R. E. & Vogel, D. (2001). The changing character of regulation: A comparison of Europe and the United States. *Risk Analysis* 21, 399-406.

McCrae, M. & Balthazor, L. (2000). Integrating risk management into corporate governance: The Turnbull Guidance. *Risk Management: An International Journal*, 2(3), 35-45.

Sjöberg, L. (2003). The different dynamics of personal and general risk. *Risk Management: An International Journal*, 5, 19-34.

Slovic, P. (2000) (Red.). *The Perception of Risk*. London: Earthscan.

Tversky, A. & Kahneman, D. (1974). Judgement under uncertainty: heuristics and biases. *Science*, 185, 1124-1131.

Tversky, A. & Kahneman, D. (1981). The Framing of decisions and the psychology of choice. *Science*, 211, 453-458.

SOU (2004: 130). *Svensk Kod för Bolagsstyrning*. Stockholm: SOU.

Ward, S. (2001). Exploring the role of the corporate risk manager. *Risk Management: An International Journal*, 3(1), 7-25.

ÅRL (1995). *Årsredovisningslagen (1995:1554:6).* Stockholm: Sveriges Riksdag.