SIMPT
Svenska institutet mot penningtvätt
Swedish Anti-Money Laundering Institute

Grundläggande vägledning inom allmän riskbedömning

Beslutad av Simpts styrgrupp i november 2017

Innehållsförteckning

1 Inledning

Syftet med Svenska institutet mot penningtvätt, Simpt, är att ta fram vägledning för de finansiella företagens tillämpning och tolkning av penningtvättsregelverket. Följande vägledning tar sikte på företagens riskbedömning av verksamheten, den allmänna riskbedömningen.

Vägledningen omfattar dels *grundläggande vägledning*, dels *verksamhetsspecifik vägledning* (bilagd). Den verksamhetsspecifika vägledningen har tagits fram av medlemsföretagen i Simpt och beskriver hur regelverket tillämpas i praktiken. Företrädare för medlemsföretagen (referensgruppen) har också varit delaktiga i arbetet med den grundläggande vägledningen.

Denna grundläggande vägledning inom ämnet allmän riskbedömning är generell och omfattar till stora delar en beskrivning av vad som krävs enligt penningtvättsregelverket. Vägledningen utgår från lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism samt Finansinspektionens föreskrifter (FFFS 2017:11) om åtgärder mot penningtvätt och finansiering av terrorism. Vägledningen innehåller i denna del också en beskrivning på ett övergripande plan av hur verksamhetsutövare ser på och hanterar kravet på att göra allmän riskbedömning samt en metod för att göra riskbedömning av verksamheten.

Den verksamhetsspecifika vägledningen innehåller i huvudsak en beskrivning av olika hotaktiviteter och sårbarheter relaterade till vissa beskrivna produkter och tjänster, men även i viss mån en beskrivning av andra faktorer som kan påverka hur de produkter och tjänster som tillhandahålls i verksamheten kan utnyttjas för penningtvätt eller finansiering av terrorism. Den enskilda verksamhetsutövaren kan – utifrån de specifika förhållandena i den egna verksamheten – finna stöd i vägledningen för att bedöma hur de produkter och tjänster som tillhandahålls kan utnyttjas för penningtvätt eller finansiering av terrorism och hur stor risken är för att detta sker.

Denna första version av vägledning är inte avsedd att vara heltäckande. Det kan finnas anledning att utveckla och fördjupa vägledningen inom allmän riskbedömning framöver.

Utkasten till vägledning har varit föremål för öppen konsultation. Synpunkter har inkommit från myndigheter och privata aktörer. Avsikten har varit att i största möjliga utsträckning beakta synpunkterna i arbetet med vägledningen. Vissa synpunkter är sådana att de kan komma att hanteras i det fortsatta arbetet med vägledningen. Exempelvis är Datainspektionens synpunkt om att Simpt bör lämna praktiska råd om hur bestämmelserna om behandling av personuppgifter bör tolkas, i linje med det avsedda fortsatta arbetet. Information har också inhämtats från Säkerhetspolisen (hösten 2017).

2 Riskbaserat förhållningssätt

2.1 Allmänt om det riskbaserade förhållningssättet

Det svenska penningtvättsregelverket utgår från internationella åtaganden och bygger på EU:s fjärde penningtvättsdirektiv (Europaparlamentets och rådets direktiv (EU) 2015/849 av den 20 maj 2015 om åtgärder för att förhindra att det finansiella systemet används för penningtvätt eller finansiering av terrorism, om ändring av Europaparlamentets och rådets förordning (EU) nr 648/2012 och om upphävande av Europaparlamentets och rådets direktiv 2005/60/EG och kommissionens direktiv 2006/70/EG), som i sin tur bygger på de rekommendationer som den mellanstatliga organisationen Financial Action Task Force, Fatf, har tagit fram. Fatf är internationell standardsättare på området för bekämpning av penningtvätt och finansiering av terrorism. År 2012 reviderade Fatf sina rekommendationer. Det riskbaserade förhållningssättet lyfts där fram som en viktig grund för en effektiv

fördelning av resurser (rekommendation 1). Det fjärde penningtvättsdirektivet genomsyras i än högre grad än tidigare direktiv av principen om ett riskbaserat förhållningssätt.

Utmärkande för Fatfs rekommendationer och för penningtvättsdirektivet är det ansvar som tilldelas verksamhetsutövarna. Det förebyggande arbetet med att förhindra penningtvätt och finansiering av terrorism utgår väsentligen från dessa aktörer och kraven på de enskilda aktörerna är höga (prop. 2016/17:173 s. 178).

Syftet med lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism (penningtvättslagen) är att förhindra att finansiell verksamhet och annan näringsverksamhet utnyttjas för penningtvätt eller finansiering av terrorism (1 kap. 1 § penningtvättslagen). I linje med vad som följer av de internationella regelverken, ska verksamhetsutövarnas åtgärder för att uppnå detta syfte utgå från ett riskbaserat förhållningssätt.

Det riskbaserade förhållningssättet innebär att åtgärder ska vidtas utifrån en riskbedömning. För verksamhetsutövarens del innebär det riskbaserade förhållningssättet att sådant som omfattningen av åtgärder, förfaranden och kontroller ska utformas och fortlöpande anpassas efter riskerna för penningtvätt och finansiering av terrorism i den specifika verksamheten. Flest och mest omfattande åtgärder ska sättas in där riskerna är som störst. Där riskerna är mindre räcker det med färre och mindre omfattande åtgärder. Följaktligen är det riskbaserade förhållningssättet ett sätt att styra resurserna i verksamheten till de viktigaste områdena när det gäller arbetet mot penningtvätt och finansiering av terrorism (prop. 2016/17:173 s. 178).

Det riskbaserade synsättet bör medföra att verksamhetsutövare kan motverka att deras verksamhet utnyttjas för penningtvätt och finansiering av terrorism till en lägre kostnad och med högre effektivitet än vid ett i detalj reglerat system (prop. 2016/17:173 s. 178). De förebyggande åtgärderna bör utformas så att kostnaderna för regelefterlevnaden inte blir oproportionerliga (jfr fjärde penningtvättsdirektivets beaktandesats 2).

2.2 Riskbaserat förhållningssätt i praktiken

Det riskbaserade förhållningssättet innebär att åtgärder ska vidtas utifrån en riskbedömning. Det finns inte någon gemensamt överenskommen definition av begreppet risk. Bedömningen av risk kan dock ta sin utgångspunkt i tre frågor som sammantaget beskriver karaktären på riskerna (Totalförsvarets Forskningsinstituts, FOI, modell för risk- och sårbarhetsanalys, Forsa-modellen).

Utifrån de tre frågor som följer av Forsa-modellen kan följande utgångspunkter tas för riskbedömning enligt penningtvättsregelverket.

1. Går produkten/tjänsten att använda för penningtvätt eller finansiering av terrorism, vad kan inträffa (oönskade händelser eller scenarier)?

2. Hur sannolikt är det att detta inträffar (t.ex. antalet kunder som använder produkten/tjänsten)?

3. Om det inträffar, vad blir konsekvenserna (t.ex. stora belopp)?

Konsekvenserna av genomförd penningtvätt eller finansiering av terrorism kan sättas i relation till såväl det enskilda företaget som till samhället i stort. Lyckade försök kan leda till att kriminella attraheras till företaget, men också till sådant som ett skadat förtroende för det finansiella systemet om dess institutioner förknippas med illegala tillgångar och penningtvätt, vilket i sin tur hotar den finansiella stabiliteten (jfr regeringens skrivelse 2013/14:245 En nationell strategi för en effektiv regim för bekämpning av penningtvätt och av finansiering av terrorism s. 3)

Syftet med penningtvättsregelverket – att förhindra att verksamheten utnyttjas för penningtvätt eller finansiering av terrorism – innebär ytterst att verksamhetsutövarna bidrar till arbetet med att förebygga och upptäcka brottslig verksamhet. Utgångspunkten för det riskbaserade förhållningssättet bör vara att rimliga åtgärder vidtas i det enskilda fallet. För att hamna på en nivå som är rimlig utifrån syftet att förhindra att verksamheten utnyttjas för penningtvätt och finansiering av terrorism, krävs ett systematiskt arbete utifrån riskerna i verksamheten.

Det riskbaserade förhållningssättet innebär att det är nödvändigt att göra mer i vissa fall och mindre i andra. Den verksamhetsutövare som vidtar alla åtgärder i alla situationer agerar inte riskbaserat och därmed inte heller effektivt. Den som agerar utan urskiljning riskerar att inte fokusera på de faktiskt riskfyllda situationerna. Den som gör ”lite till” i fråga om sina kontroller för att vara på den säkra sidan, riskerar också att onödigtvis försvåra eller förhindra genomförandet av olika affärsverksamheter.

Det riskbaserade förhållningssättet handlar inte om att arbeta utifrån en ”nollvision”. Det är inte realistiskt att utgå från att ett företag kan säkerställa att verksamheten aldrig utnyttjas för penningtvätt eller finansiering av terrorism. Det kan finnas situationer när företaget har vidtagit alla rimliga åtgärder för att identifiera och minska sina risker för penningtvätt och finansiering av terrorism, men ändå utnyttjas för dessa syften (jfr Fatf Guidance for a Risk-Based Approach the Banking Sector s. 6).

Det riskbaserade förhållningssättet är inte avsett att hindra ett företag från att ha produkter, tjänster eller kunder som innebär hög risk för penningtvätt eller finansiering av terrorism i verksamheten. Avgörande är att företaget kan och faktiskt vidtar åtgärder för att hantera riskerna i verksamheten.

3 Allmän riskbedömning

3.1 Inledning

Avsnittet om allmän riskbedömning är uppdelat i tre delar. Avsnitt 3.2 innehåller i huvudsak en beskrivning av vad som krävs enligt penningtvättsregelverket och en sammanfattning av vad som framgår av prop. 2016/17:173 Ytterligare åtgärder mot penningtvätt och finansiering av terrorism. Avsnitt 3.3 innehåller en beskrivning på ett övergripande plan av hur verksamhetsutövare ser på och hanterar den allmänna riskbedömningen i praktiken. Avsnitt 3.4, slutligen, omfattar en beskrivning av en metod som kan vara ett stöd för företag att göra den allmänna riskbedömningen. Metoden kan komma att utvecklas och fördjupas framöver inom ramen för det fortsatta arbetet med vägledningen. Upplägget med att beskriva allmän riskbedömning i tre avsnitt innebär en viss upprepning i olika avseenden. Dispositionen är något som kan komma att ses över i det fortsatta arbetet med vägledningen.

3.2 Allmänt om den allmänna riskbedömningen

Detta avsnitt innehåller i huvudsak en beskrivning vad som krävs enligt penningtvättsregelverket som det beskrivs i prop. 2016/17:173 s. 206–209, 510 och 511 Ytterligare åtgärder mot penningtvätt och finansiering av terrorism, om inte annan källa anges.

Verksamhetsutövare ska göra en allmän riskbedömning. Den allmänna riskbedömningen innebär en bedömning av hur de produkter och tjänster som tillhandahålls i verksamheten kan utnyttjas för penningtvätt eller finansiering av terrorism och hur stor risken är för att detta sker.

Vid den allmänna riskbedömningen ska det särskilt beaktas vilka slags produkter och tjänster som tillhandahålls, vilka kunder och distributionskanaler som finns och vilka geografiska riskfaktorer som föreligger. Hänsyn ska också tas till uppgifter som kommer fram vid verksamhetsutövarens

rapportering av misstänka aktiviteter och transaktioner samt till information om tillvägagångssätt för penningtvätt och finansiering av terrorism och andra relevanta uppgifter som myndigheter lämnar (2 kap. 1 § penningtvättslagen).

Definitionen av penningtvätt och finansiering av terrorism (1 kap. 6 och 7 §§ penningtvättslagen)

Penningtvätt

Med penningtvätt avses, enligt 1 kap. 6 § penningtvättslagen, åtgärder med avseende på pengar eller annan egendom som härrör från brott eller brottslig verksamhet som
1. kan dölja egendomens samband med brott eller brottslig verksamhet,
2. kan främja möjligheterna för någon att tillgodogöra sig egendomen eller dess värde,
3. kan främja möjligheterna för någon att undandra sig rättsliga påföljder, eller
4. innebär att någon förvärvar, innehar, hävdar rätt till eller brukar egendomen.

Åtgärderna ska vara av sådan art att de typiskt sett kan medföra att t.ex. egendomens samband med brott döljs. Det krävs inte att sambandet faktiskt har dolts för att penningtvätt ska anses föreligga.

Med penningtvätt enligt penningtvättslagen jämställs åtgärder med egendom som typiskt sett är ägnade att dölja att någon avser att berika sig eller någon annan genom en framtida brottslig handling. Syftet är att verksamhetsutövarna ska förebygga och i övrigt reagera på typiska penningtvättsåtgärder, även om det inte är klarlagt att egendom som hanteras varit föremål för brott, vilket krävs för att penningtvätt ska föreligga. Tillämpningen begränsas genom att förfarandet typiskt sett ska vara ägnat att dölja att någon avser att berika sig eller någon annan genom en framtida brottslig handling. Så är exempelvis fallet med delmoment i välkända upplägg för att kunna avlöna svart arbetskraft, där penningtvättsbrottet oftast anses vara begånget först efter det att transaktionerna vidtagits. Även avvikande överföringar till jurisdiktioner som kan betraktas som skatteparadis och andra liknande förfaranden avses, även då verksamhetsutövaren inte är klar över att egendomen ännu varit föremål för brott (prop. 2016/17:173, s. 508).

Finansiering av terrorism

Med finansiering av terrorism avses enligt 1 kap. 7 § penningtvättslagen insamling, tillhandahållande eller mottagande av pengar eller annan egendom i syfte att egendomen ska användas eller med vetskap om att den är avsedd att användas
1. för att begå sådan brottslighet som avses i 2 § lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall,
2. av en person eller en sammanslutning av personer som begår sådan brottslighet som avses i 2 § lagen om straff för finansiering av särskilt allvarlig brottslighet i vissa fall, eller gör sig skyldig till försök, förberedelse, stämpling eller medverkan till sådan brottslighet, eller
3. för en sådan resa som avses i 5 b § lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet.

Verksamhetsutövarens riskbedömning ska besvara frågan om och hur dess produkter eller tjänster kan användas för att exempelvis dölja brottsligt åtkommen egendoms samband med brott eller brottslig verksamhet (prop. 2016/17:173 s. 510).

Riskbegreppet innebär i första hand en bedömning av hur sårbar verksamhetsutövaren är för att utnyttjas för penningtvätt eller finansiering av terrorism. Det kan förekomma att produkter eller

tjänster inte bedöms som sårbara i sig utan att bristen (sårbarheten) ligger i andra delar av ”systemet”, t.ex. i distributionskanalerna. Det kan också förekomma att sårbarheter beror på andra omständigheter, såsom verksamhetsutövarens storlek, organisatorisk komplexitet och andra verksamhetsspecifika, men inte produkt- eller tjänstrelaterade, omständigheter (prop. 2016/17:173 s. 207).

Vid den allmänna riskbedömningen ska det särskilt beaktas vilka slags produkter och tjänster som tillhandahålls, vilka kunder och distributionskanaler som finns och vilka geografiska riskfaktorer som föreligger men även andra omständigheter och faktorer ska beaktas när det är relevant (prop. 2016/17:173 s. 510).

Med kundriskfaktorer avses bl.a. sådana omständigheter som ska beaktas vid riskklassificeringen av kunden (enligt 2 kap. 4 och 5 §§) (prop. 2016/17:173 s. 510).

Geografiska faktorer är sådana som är relaterade till förhållandena i de länder där produkter eller tjänster erbjuds eller där verksamhetsutövarens kunder är baserade (prop. 2016/17:173 s. 510). För att bedöma om exempelvis förekomsten av många transaktioner till ett visst land innebär en ökad sannolikhet för att en tjänst som möjliggör gränsöverskridande penningtransaktioner utnyttjas för penningtvätt eller finansiering av terrorism, är kännedom om riskerna som kan förknippas med landet i fråga av avgörande betydelse (prop. 2016/17:173 s. 208).

Riskfaktorer avseende distributionskanaler kan exempelvis vara om verksamhetsutövaren har kontroll över produkter eller tjänster när de erbjuds kunden eller om distribution sker via en tredje part (prop. 2016/17:173 s. 510).

För att vara relevant och tillförlitlig ska en riskbedömning så långt möjligt vara baserad på verkliga sårbarheter och risker. Kvantitativ data som visar att penningtvätt eller finansiering av terrorism genom ett visst förfarande eller med en viss typ av tjänst eller produkt är vanligt förekommande, är av vikt för att riskanalysen ska vara verklighetsanpassad (prop. 2016/17:173 s. 208 och 510).

Kunskap som erhållits vid rapportering av misstänkta transaktioner och aktiviteter ska beaktas av verksamhetsutövaren. En verksamhetsutövare kan genom egna analyser och åtgärder för övervakning och rapportering av misstänkta aktiviteter och transaktioner bilda sig en uppfattning om riskerna i verksamheten. Genom dessa åtgärder kan verksamhetsutövaren få en översiktlig bild av olika externa riskfaktorer som påverkar risken för penningtvätt eller finansiering av terrorism i verksamheten (prop. 2016/17:173 s. 208.

Verksamhetsutövare är skyldiga att i riskbedömningen beakta information som tillhandahålls av tillsynsmyndigheter, brottsbekämpande myndigheter och andra myndigheter (2 kap. 1 § andra stycket penningtvättslagen och jfr prop. 2016/17:173 s. 510).

Den allmänna riskbedömningen omfattar en proportionalitetsbedömning. Riskbedömningen ska vara så omfattande som motiveras av förhållandena i det enskilda fallet. Omfattningen av den allmänna riskbedömningen ska bestämmas med hänsyn till verksamhetsutövarens storlek och art och de risker för penningtvätt och finansiering av terrorism som kan antas föreligga (2 kap. 2 § penningtvättslagen, jfr också prop. 2016/17:173 s. 209).

En riskbedömning för en verksamhet med ett fåtal okomplicerade produkter och tjänster får vara mindre omfattande än för ett företag med komplicerade eller med ett större utbud av produkter och tjänster (Finansinspektionens beslutspromemoria FI Dnr 16–2467 s. 10).

Med verksamhetens art avses i första hand vilken verksamhet som bedrivs, inbegripet vilka varor eller tjänster som tillhandahålls, hur komplexa dessa varor och tjänster är och andra liknande omständigheter. Med verksamhetens storlek avses t.ex. omsättning, antal anställda, antal verksamhetsställen och liknande förhållanden (prop. 2016/17:173 s. 209).

Riskbedömningen ska utformas så att den kan ligga till grund för verksamhetsutövarens rutiner, riktlinjer och övriga åtgärder mot penningtvätt och finansiering av terrorism (2 kap. 2 § penningtvättslagen).

Riskbedömningen är av stor vikt för flertalet åtgärder i penningtvättslagen. För det första ska rutiner och riktlinjer vara utformade i syfte att motverka de identifierade riskerna. Den allmänna riskbedömningen spelar också en viktig roll vid riskbedömningen av kunderna, vilken i sin tur styr omfattningen av åtgärderna för kundkännedom. Riskbedömningen ska också beaktas när verksamhetsutövaren bestämmer omfattning och inriktning på övervakningen av aktiviteter och transaktioner. Riskbedömningen ska vara utformad på ett sådant sätt att den kan användas för dessa syften (prop. 2016/17:173 s. 511).

3.3 Allmän riskbedömning i praktiken

Allmän riskbedömning handlar om att bedöma risken för att verksamheten ska utnyttjas för penningtvätt och finansiering av terrorism. Det är inte fråga om den riskbedömning som görs inom ramen för kundkännedomen. Däremot är den riskbedömning som görs av verksamheten av direkt betydelse för kundkännedomen, eftersom riskbedömningen av kunden ska bestämmas med utgångspunkt i den allmänna riskbedömningen. Risken för att bli föremål för sådant som sanktioner (den regulatoriska risken eller ”compliancerisken”) eller rykten är också sådant som faller utanför den bedömning som ska göras av risken för att de produkter och tjänster som tillhandahålls i verksamheten kan utnyttjas för penningtvätt och finansiering av terrorism.

Allmän riskbedömning är inte något som utförs vid ett tillfälle och dokumenteras som en utförd åtgärd, utan en ständigt pågående process. Riskbedömningen ska visserligen dokumenteras, men framför allt ska den genomsyra tillämpningen av penningtvättsregelverket. Den allmänna riskbedömningen är ytterst ett stöd för verksamhetsutövare att kunna tillämpa regelverket på ett ändamålsenligt sätt. Exempelvis har företaget, vid riskklassificeringen av enskilda kundrelationer, möjlighet att tillgodoräkna sig en relevant och tillförlitlig allmän riskbedömning som visar att risken som kan förknippas med en viss produkt eller tjänst är låg (jfr prop. 2016/17:173 s. 260).

I riskbedömningen måste beaktas alla faktorer i verksamheten. Verksamhetens produkter och tjänster måste beaktas, men även andra faktorer i verksamheten och inte minst hur de olika faktorerna påverkar varandra. Alla typer av produkter och tjänster kan i princip förvärvas eller tas i anspråk med begagnande av pengar eller annan egendom som antingen har ett brottsligt ursprung eller är avsedda att användas för finansiering av terrorism. Möjligheterna att dölja sambandet mellan egendomen och brottet behöver inte ha något att göra med de särskilda egenskaper som är inbyggda i produkten eller tjänsten (t.ex. att innehav av produkten inte kan kopplas till viss person). I stället kan sättet att genomföra betalningen av produkten eller utnyttjandet av en tjänst, t.ex. i form av att tillhandahålla ett konto, innebära en risk, t.ex. genom att överföringen av medel inte är – tillräckligt – spårbara.

Centralt vid riskbedömningen är förståelsen för vad som påverkar risken och att värdera risken. En faktor kan innebära en viss risknivå sedd för sig själv, men i kombination med andra faktorer en helt annan nivå. Ett företag som marknadsför sig mot en ny kundkrets bör fråga sig om och i så fall hur den nya kundkretsen kan komma att påverka risken som är förknippad med produkten. Riskbedömning bygger i stor utsträckning på hypoteser, dvs. på att föreställa sig olika tillvägagångssätt. Den ska dock så långt möjligt vara baserad på konkreta och realistiska sårbarheter och risker.

Vid analysen av hur verksamheten kan utnyttjas för penningtvätt eller finansiering av terrorism, är det givetvis inte alldeles enkelt att förutse och föreställa sig klara tillvägagångssätt. Den erfarenhet man kan ha skaffat sig genom tidigare misstankar ger sällan facit på om det faktiskt var fråga om penningtvätt eller finansiering av terrorism. Men även en visserligen inte verifierad men tänkbar, realistisk möjlighet att exempelvis en viss produkt skulle kunna utnyttjas för penningtvätt eller finansiering av terrorism, kan vara grund för att vidta åtgärder. Det är inte bara den kunskap som har erhållits vid rapportering utan även den som erhålls i samband med närmare överväganden om rapportering ska ske av misstänkta transaktioner och aktiviteter som bör beaktas av verksamhetsutövaren. Det är viktigt att dra slutsatser av den information som finns i verksamheten och att använda informationen.

I syfte att underlätta förståelsen för hur exempelvis en viss produkt skulle kunna utnyttjas för penningtvätt eller finansiering av terrorism, kan det ofta vara värdefullt att den eller de som ska göra den allmänna riskbedömningen har en dialog, t.ex. i form av en workshop, med personer i verksamheten som har djupare kunskap om de produkter som omfattas av bedömningen.

Den allmänna riskbedömningen ska fokusera både på riskerna för penningtvätt och på riskerna för finansiering av terrorism. Den gemensamma nämnaren är utnyttjandet av det finansiella systemet för illegala ändamål. Den principiella skillnaden är dock att penningtvätt syftar till att dölja en vinstgenererande brottslig handling, något som inte behöver vara fallet vid finansiering av terrorism, eftersom terrorism kan finansieras med legalt intjänade medel (prop. 2016/17:173 s. 170). Denna grundläggande skillnad gör att det ofta är viktigt att hålla isär penningtvätt från finansiering av terrorism (Jfr ESAs Final Guidelines The Risk Factors Guidelines JC 2017 37 26/06/2017 s. 6).

Det kan många gånger vara betydligt svårare att föreställa sig konkreta scenarier när det gäller finansiering av terrorism än penningtvätt. Finansiering av terrorism kan avse små transaktioner som dessutom innebär små avvikelser i förhållande till vad det kan finnas anledning att förvänta sig om kunden. Det kan alltså se ut som helt vanliga transaktioner och det kan vara svårt att hitta mönster. Det kräver ofta mycket analysarbete för att t.ex. identifiera hur verksamhetens produkter och tjänster kan utnyttjas för penningtvätt och finansiering av terrorism, varför insamling av extern information, t.ex. från Säkerhetspolisen många gånger blir viktig.

Finansiering av terrorism kan ske på många fler sätt än den traditionella finansieringen av resenär. Nedan följer några exempel på former av terrorismfinansiering i västvärlden inklusive Sverige:

1. Resenär finansierar sig själv genom exempelvis sparande – vanligaste metoden
2. Resenär som finansieras genom lån eller bedrägerier
3. Pengar skickas från Sverige till stridande individer (normalt från individ till individ)
4. Finansiering av rekrytering, facilitering och utbildning i Sverige eller utomlands
5. Finansiering för genomförande av attentat
6. Pengar samlas in och skickas till terroristorganisationer
7. Utländska terroristorganisationer investerar pengar i Sverige eller andra delar av västvärlden

Den allmänna riskbedömningen ska drivas så långt och utformas så pass tydligt att den omedelbart ska kunna utgöra underlag för en bedömning av vilka konkreta åtgärder som ska vidtas för att minska riskerna. Detta ska göras i tillräcklig grad för att kunna avgöra om en produkt eller tjänst ska kunna tillhandahållas en kund. Varje företag avgör inom ramen för sin riskbegränsande infrastruktur vilka åtgärder som ska vidtas för att effektivt hantera riskerna. Det kan t.ex. göras genom olika typer av produktbegränsningar, åtgärder inom ramen för monitoreringssystemet eller genom utbildning av personalen.

Exempel på källor till information att ta del av och beakta vid allmän riskbedömning

Källor som företaget måste ta del av:

- Lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism
- Förordning (2009:92) om åtgärder mot penningtvätt och finansiering av terrorism
- Finansinspektionens föreskrifter (2017:11) om åtgärder mot penningtvätt och finansiering av terrorism

Källor att ta del av och beakta när relevant:

- EU:s fjärde penningtvättsdirektiv (Europaparlamentets och rådets direktiv (EU) 2015/849 av den 20 maj 2015 om åtgärder för att förhindra att det finansiella systemet används för penningtvätt eller finansiering av terrorism, om ändring av Europaparlamentets och rådets förordning (EU) nr 648/2012 och om upphävande av Europaparlamentets och rådets direktiv 2005/60/EG och kommissionens direktiv 2006/70/EG).
- Prop. 2016/17:173 Ytterligare åtgärder mot penningtvätt och finansiering av terrorism
- Penningtvätt, En nationell riskbedömning (2013)
- Finansiering av terrorism, En nationell riskbedömning (2014)
- Finansiella aktiviteter kopplade till personer från Sverige och Danmark som anslutit sig till terrorgrupper i Syrien och Irak mellan 2013 – 2016 (Centrum för asymmetriska hot- och terrorismstudier, Cats, vid Försvarshögskolan, rapport på uppdrag av Finansinspektionen, 2017)
- Finanspolisens (Finanspolissektionen inom Polismyndigheten) årsrapporter
- Penningtvätt och annan penninghantering, Kriminella, svarta och grumliga pengar i legal ekonomi (Brå rapport 2015:22)
- Penningtvätt upplägg med osanna fakturor (Finansinspektionen och Ekobrottsmyndigheten, 2016)
- Understanding Terrorist Finance, Modus Operandi and National CTF-regimes (Centrum för asymmetriska hot- och terrorismstudier, Cats, vid Försvarshögskolan, 2015)
- Rapport från kommissionen till Europaparlamentet och rådet om bedömningen av de risker för penningtvätt och finansiering av terrorism som påverkar den inre marknaden och berör gränsöverskridande verksamhet, COM(2017) 340 final
- Basel AML Index Report 2016

Information kan hämtas på följande ställen:

- www.bis.org
- www.fatf-gafi.org
- www.fi.se/penningtvatt
- www.jmlsg.org.uk
- www.oecd.org
- www.wolfsberg-principles.com

En sammanställning över bl.a. vägledningar från Fatf finns på regeringens hemsida, www.regeringen.se/amlcft

De europeiska tillsynsmyndigheterna (ESA) Europeiska bankmyndigheten (EBA), Europeiska försäkrings- och tjänstepensionsmyndigheten (Eiopa) och Europeiska värdepappers- och marknads-myndigheten (Esma) har tagit fram gemensamma riktlinjer som utgör allmänna råd och därmed

vägledning kring riskfaktorer för företagen att beakta. Vägledningen omfattar åtgärder för förenklad och skärpt kundkännedom. De allmänna råden tar främst sikte på faktorer att beakta vid riskbedömningen av den enskilda affärsförbindelsen eller transaktionen. Företaget kan dock även använda de allmänna råden i sin allmänna riskbedömning (Final Guidelines The Risk Factors Guidelines JC 2017 37 26/06/2017 se bl.a. s. 9, se också Finansinspektionens beslutspromemoria FI Dnr 16-2467 s. 9).

3.4 Metod för att göra allmän riskbedömning

3.4.1 Relevanta begrepp

Hot
Med hot eller hotaktiviteter avses alla handlingar som främjar eller leder till penningtvätt eller finansiering av terrorism. Individer eller organisationer som utför dessa handlingar betecknas som hotaktörer (jfr Finansiering av terrorism, En nationell riskbedömning s. 21).

Inneboende risk
Den inneboende risken avser risken för penningtvätt eller finansiering av terrorism innan mitigierade åtgärder har vidtagits.

Konsekvens
Begreppet konsekvens hänför sig till den skada som penningtvätt eller finansiering av terrorism kan orsaka och omfattar bl.a. de effekter som den underliggande aktiviteten har på bl.a. institutioner. Konsekvenserna kan vara både kortsiktiga och långsiktiga (jfr FATF Guidance National Money Laundering and Terrorist Financing Risk Assessment February 2013 s. 7).

Residualrisk
Residualrisk är den risk som företaget exponeras för efter det att mitigerande åtgärder har vidtagits (jfr ESAs Final Guidelines, The Risk Factor Guidelines, JC 2017 37, 26/06/2017 s. 10).

Sårbarhet
Sårbarhet är en systemdel som saknas eller vars funktion bedöms utgöra ett problem för möjligheten att uppnå systemets mål. En sårbarhet relaterar normalt sett till någon specifik form av hot, tänkt eller faktiskt föreliggande. Andra kan vara av mer generell karaktär och relevanta för en bred uppsättning hot (jfr Penningtvätt, En nationell riskbedömning s. 29).

3.4.2 Övergripande metodbeskrivning

I det följande beskrivs en metod som kan vara ett stöd när ett företag ska göra den allmänna riskbedömningen (se illustration). Metoden är särskilt relevant inför att nya produkter och tjänster introduceras, men också för de i verksamheten befintliga produkterna och tjänsterna. Metoden kan komma att utvecklas och fördjupas framöver inom ramen för det fortsatta arbetet med vägledningen.

Metoden för att göra allmän riskbedömning omfattar flera steg och är ett löpande arbete. Genomförandet av steg 1 och steg 2 ska resultera i den allmänna riskbedömningen. I det följande steget (steg 3) ska åtgärder vidtas för att minska de risker som har identifierats i de två första stegen. I det fjärde steget ska verksamhetsutövaren bedöma vilka effekter som har uppnåtts genom åtgärderna i steg 3.

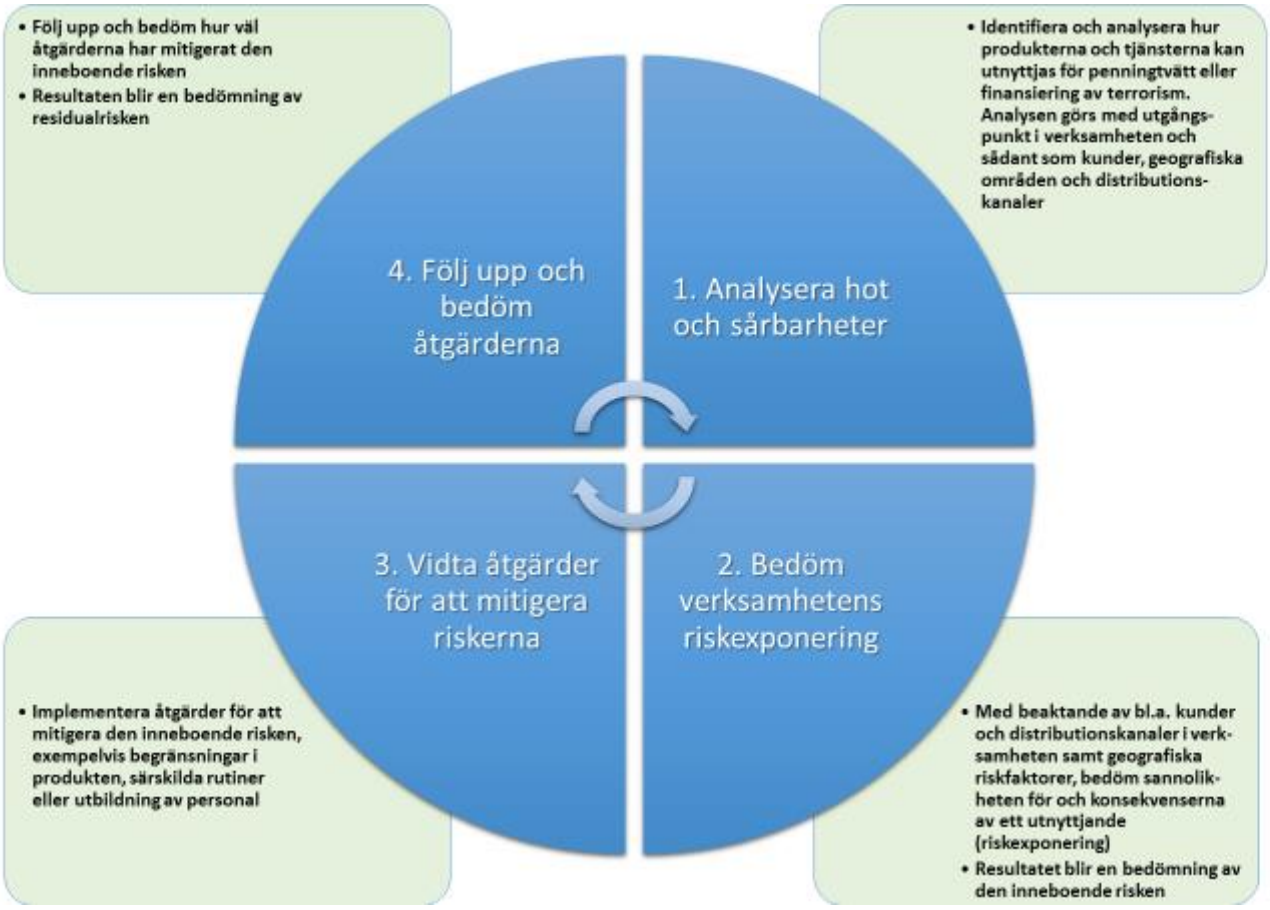
I ett första steg (steg 1) identifieras och analyseras hot och sårbarheter. Det handlar om att identifiera och analysera om, och i så fall på vilka sätt, produkterna och tjänsterna i verksamheten kan utnyttjas för penningtvätt eller finansiering av terrorism. Företaget bör ställa sig frågan hur ett utnyttjande skulle kunna gå till och vad om faktiskt skulle kunna inträffa. Analysen utgår från den typ av verksamhet som bedrivs och för att kunna göra analysen krävs att företaget beaktar faktorer som påverkar risken, såsom verksamhetens kunder, t.ex. vilken som är målgruppen för en viss produkt, distributionskanaler, t.ex. hur en viss produkt är avsedd att distribueras samt geografiska riskfaktorer, t.ex. om kunderna typiskt sett har hemvist i ett högriskland.

I nästa steg (steg 2) görs en bedömning av sannolikheten för och konsekvenserna av att verksamheten utnyttjas för penningtvätt och finansiering av terrorism. Det innebär att en bedömning görs av hur stor risken är för att verksamheten utnyttjas, dvs. en bedömning av verksamhetens riskexponering. Vid bedömningen av sannolikheten för att utnyttjas bör företaget, liksom vid analysen av hot och sårbarheter, särskilt beakta sådant som vilka slags kunder och distributionskanaler som finns i verksamheten samt geografiska riskfaktorer.

Hot- och sårbarhetsanalysen samt bedömningen av riskexponeringen leder sammantaget till en bedömning av den inneboende risken, d.v.s. risken för att företagets produkter och tjänster kan komma att utnyttjas för penningtvätt eller finansiering av terrorism. Med utgångspunkt i bedömningen av den inneboende risken ska företaget vidta åtgärder för att mitigera riskerna. Mitigerande åtgärder kan vara utformade på många olika sätt, det viktiga är att de lindrar eller mildrar identifierade risker på ett sätt som gör att riskerna effektivt hanteras (steg 3).

För att säkerställa att åtgärderna mitigerar identifierade risker och att företaget därmed har kontroll över riskerna, behöver företaget löpande följa upp och bedöma deras effekt. Det innebär såväl en uppföljning av att åtgärder vidtas som en bedömning av att de fungerar. Bedömningen av de mitigerande åtgärdernas effekt ger en bild av företagets residualrisk, dvs. den risk företaget exponeras för efter det att åtgärder har vidtagits (steg 4).

Illustration av en metod för att göra allmän riskbedömning



3.4.3 Den inneboende risken (steg 1 och 2)

3.4.3.1 Inledning

Den samlade bedömningen av hot och sårbarheter samt sannolikhet och konsekvens (risk-exponeringen) ger en bild av den inneboende risken för penningtvätt och finansiering av terrorism i företagets produkter och tjänster (steg 1 och 2). Den inneboende risken utgör utgångspunkten för företagets viktiga arbete med att vidta åtgärder för att hantera riskerna (steg 3 och 4).

En grundförutsättning för riskbedömningen är en förståelse både för de verkliga och de möjliga hot som kan föreligga, antingen nu eller i framtiden. Sårbarheterna relaterar till hoten i den meningen att om det inte finns ett hot, är det inte relevant att bedöma om företaget är sårbart inför det (jfr Penningtvätt En nationell riskbedömning 2013 s. 21). Däremot kan det finnas sårbarheter som är av mer generell karaktär och som därmed är relevanta för en bred uppsättning hotaktiviteter.

Hot och sårbarheter kan se olika ut och de olika produkterna och tjänsterna behöver därför bedömas separat. Detta innebär – i ett senare led – att ett företag kan anpassa sina mitigerande åtgärder och sina resurser till de produkter och tjänster som det faktiskt erbjuder och därmed riskbaserat bemöta sina penningtvätts- och terrorismfinansieringsrisker.

3.4.3.2 Analysera hot och sårbarheter (steg 1)

Hotaktiviteter

En hotaktivitet är en aktivitet som kan leda till penningtvätt eller finansiering av terrorism. Den eller de personer som genomför aktiviteten är hotaktör.

De flesta penningtvätts- och terrorismfinansieringsupplägg kan beskrivas med hjälp av följande hotaktiviteter.

- *Värdeomvandlande aktiviteter,* exempelvis köp av tillgångar av olika slag eller växling.
- *Värdeöverförande* och *värdeförflyttande aktiviteter,* exempelvis penningöverföring.
- *Värdebevarande aktiviteter,* exempelvis lagring av brottsvinster eller registrering av innehav av olika slag.

För terrorismfinansiering tillkommer följande hotaktiviteter.

- *Värdegenererande aktiviteter*, exempelvis insamling av pengar på olika sätt, såsom upptagande av lån eller olika former av brott.

Ett penningtvätts- eller terrorismfinansieringsupplägg består vanligtvis av en sekvens av de olika hotaktiviteterna.

De olika hotaktiviteterna kan utgöra utgångspunkten för att besvara frågan hur produkten eller tjänsten skulle kunna utnyttjas för att tvätta pengar eller finansiera terrorism.

Sårbarheter

En sårbarhet är en systemdel, t.ex. en automatiserad eller digitaliserad process eller en rutin, som saknas eller vars funktion bedöms utgöra ett problem för möjligheten att förhindra penningtvätts- eller terrorismfinansieringsaktiviteter. En sårbarhet relaterar normalt sett till någon specifik form av hotaktiviteter, tänkt eller faktiskt föreliggande. Det finns också sådana som är av mer generell karaktär och därmed relevanta för en bred uppsättning hotaktiviteter, exempelvis möjligheten att få tillgång till stora mängder kontanter.

För att bedöma den inneboende risken måste företaget identifiera förhållanden som gör det svårare att upptäcka penningtvätt eller finansiering av terrorism, alternativt gör en produkt eller tjänst attraktiv att använda för dessa ändamål. Exempelvis innebär de olika produkternas och tjänsternas egenskaper, såsom olika typer av beloppsbegränsningar eller skatteeffekter, att produkterna och tjänsterna kan vara mer eller mindre attraktiva att använda för penningtvätt eller finansiering av terrorism. Detsamma gäller sättet som produkten eller tjänsten distribueras på.

Bedömning av riskfaktorer

Det första steget i den allmänna riskbedömningen består i att identifiera och analysera/bedöma hot och sårbarheter. Det innebär en analys/bedömning av de förhållanden/faktorer som kan medföra att verksamheten utnyttjas för penningtvätt eller finansiering av terrorism. Riskfaktorer omfattar för verksamheten relevanta kunder, länder, geografiska områden, produkter, tjänster, transaktioner och distributionskanaler.

Varje riskfaktor måste inledningsvis analyseras/bedömas för sig själv med avseende på möjliga risker. En faktor, t.ex. en produkt som företaget tillhandahåller eller avser att tillhandahålla, ska bedömas med utgångspunkt i allt som ingår i själva produkten. Bedömningen omfattar således inte i detta skede andra faktorer som kan påverka risken, t.ex. vilken sorts kunder som ska ha möjlighet att förvärva

produkten eller på vilka sätt den ska betalas. Analysen ska genomföras så att företaget kan förstå hur faktorn kan utnyttjas. Den individuella bedömningen ska således utmynna i en bedömning av vilka brottsliga aktiviteter som är tänkbara.

Produkten eller tjänsten ska också sättas in i sitt affärsmässiga sammanhang. Det innebär att en bedömning ska göras av hur en faktor påverkas av andra faktorer, dvs. en bedömning av helheten. Risken som finns med en viss produkt påverkas av sådant som kundsegment; finns kunderna typiskt sett i högriskländer, är kunderna personer i politiskt utsatt ställning (PEP) eller är kunderna verksamma i kontantintensiva branscher? Det kan också vara faktorer som inte i sig själva innebär en risk men som tillsammans med andra faktorer innebär risker.

Nedan anges några faktorer som kan ha betydelse för företagets allmänna riskbedömning. Se ESAs Final Guidelines The Risk Factor Guidelines JC 2017 37 26/06/2017 för ytterligare vägledning.

Kunder

Kundriskfaktorer kan vara relaterade både till kundens natur och till kundens beteende. Faktorer relaterade till kundens natur kan t.ex. vara koppling till högriskland, verksamhet i högriskbransch och PEP. Faktorer relaterade till kundens beteende kan vara relevanta både vid etablerandet av en affärsförbindelse och löpande i relationen.

- Vilka typer av kunder använder produkten eller tjänsten? Vilken är målgruppen för produkten eller tjänsten? Är det exempelvis en produkt som normalt används av stora/komplexa företag eller av konsumenter?
- Har verksamheten utländska kunder och särskilt kunder som har sin verksamhet i högriskländer eller förekommer transaktioner till eller från sådana länder?
- Har verksamheten många personer i politiskt utsatt ställning (PEP) som kunder eller företagskunder med PEP som verklig huvudman, kan det finnas skäl att betrakta dessa kunder som en särskild kundtyp i den allmänna riskbedömningen.
- Har verksamheten kunder som bedriver kontantintensiv verksamhet eller kunder som har många konton i olika finansiella företag och stor rörlighet när det gäller konton och medel?
- Har verksamheten distanskunder?

Den bedömning av verksamhetens kunder som görs inom ramen för den allmänna riskbedömningen bör omfatta förhållanden som kan vara relevanta för större grupper av kunder, sådant som vilka kunder som typiskt sett använder produkten och hur de typiskt sett använder den.

Exempel (förenklat): Relationen mellan allmän riskbedömning och bedömning av kundens riskprofil

En försäkringsprodukt har en viss målgrupp och utgångspunkten är att kunderna använder produkten på ett visst sätt. Detta beaktas inom ramen för den allmänna riskbedömningen där produkten anses vara förenad med låg risk.

I bedömningen av en viss kunds riskprofil beaktas om kunden tillhör produktens vanliga kundkrets och avser att använda produkten på ett annat sätt än hur kunder vanligtvis använder produkten. Om kunden avviker i något av dessa avseenden kan det få till följd att kundrelationen anses vara förknippad med en högre risk än vad som följer av den allmänna riskbedömningen.

Distributionskanaler

- Hur distribueras produkten eller tjänsten?
- Har verksamhetsutövaren kontroll över produkter och tjänster när de erbjuds kunden eller sker distribution via en tredje part eller underleverantör?
- Erbjuds produkten eller tjänsten utan personlig kontakt, dvs. på distans?

Geografiska områden

- Involverar transaktionen något annat land?
- Hur kan produkten eller tjänsten användas geografiskt?
- Finns det möjlighet att föra värden över gränser eller att flytta dem tillhögrisländer, t.ex. ”skatteparadis” eller finns det annan anknytning till högrisländer, t.ex. länder med betydande korruption eller där narkotikahandel är vanligt förekommande? Om företaget har filialer eller samarbetspartners i andra länder, kan det vara relevant att detta tas med i bedömningen eftersom produktens eller tjänstens spridning kan bli annorlunda beroende på var den erbjuds.
- Företaget kan utifrån tillgänglig information besluta om en landlista där varje land ges en risknivå med en mer utförlig analys beträffande de geografiska områden som företaget har kopplingar till.

3.4.3.3 Bedöm verksamhetens riskexponering (steg 2)

Riskexponeringen är ett mått på hur stor risken bedöms vara för att verksamhetens produkter och tjänster utnyttjas för penningtvätt och finansiering av terrorism. Bedömningen av riskexponeringen utgör grunden för att bedöma vilka åtgärder som är lämpliga att vidta för att hantera risken. Det är därför viktigt att förstå *varför* något är eller inte är en risk och inte endast *att* det är en risk. Denna bedömning görs särskilt utifrån de produkter och tjänster som faktiskt tillhandahålls i verksamheten, dess kunder, distributionskanaler och geografiska riskfaktorer.

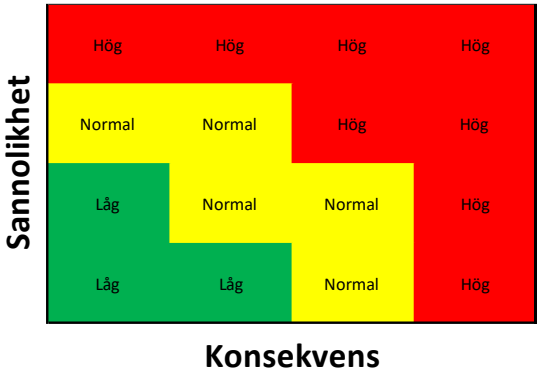
Riskexponeringen bestäms utifrån en bedömning av hur troligt eller sannolikt det är att produkterna och tjänsterna utnyttjas för penningtvätt och finansiering av terrorism och hur allvarliga effekterna eller konsekvenserna bedöms bli vid ett utnyttjande.

Om riskexponeringen är begränsad till ett fåtal kunder, kan vissa åtgärder vara både mer lämpliga och resurseffektiva än om riskexponeringen relaterar till tusentals kunder. Bedömningarna ger en bild av de områden där företaget behöver satsa mer resurser men även var företaget kan satsa mindre resurser.

Vid bedömningen av konsekvenserna är det viktigt att beakta de skillnader som finns i fråga om penningtvätt och finansiering av terrorism. Skulle en händelse kunna få allvarliga konsekvenser, exempelvis lyckad penningtvätt av stora belopp, behöver sannolikheten inte bedömas vara särskilt hög för att det ska bedömas som en förhöjd risk (se figur).

I *figuren* illustreras risknivåerna låg, normal och hög risk som ett resultat av förhållandet mellan de två dimensionerna sannolikhet och konsekvens. Det är inget som hindrar ytterligare nivåer, t.ex. olika nivåer inom normal risk eller ytterligare nivåer av hög risk. En sådan indelning kan ytterligare underlätta för företaget att bestämma åtgärder för att hantera riskerna. Risknivåerna bör inte utgå från någon värdering innebärande att en viss nivå är godtagbar eller inte utan detta sker i ett efterföljande skede när möjligheten till mitigerande åtgärder och förväntade utfall av sådana kan bedömas.

Figuren illustrerar – förenklat – sambandet mellan sannolikhet och konsekvens. Illustrationen kan överföras till exempelvis ett scoringsystem där varje produkt tilldelas en riskklass som används i riskbedömningar på kundnivå.



3.4.4 Vidta åtgärder för att mitigera riskerna (steg 3)

Den allmänna riskbedömningen ska läggas till grund för att bestämma de åtgärder, t.ex. rutiner och kundbemötande, som ska vidtas för att mitigera riskerna. Åtgärderna kan vara utformade på många olika sätt, det viktiga är att de lindrar eller minskar riskerna så att de effektivt kan hanteras. Åtgärderna kan omfatta sådant som att införa begränsningar i hur produkter och tjänster kan användas, införa särskilda rutiner för kundkännedom eller att utbilda personal.

Åtgärder som redan är vidtagna när den allmänna riskbedömningen genomförs och är sådana att utfallet av åtgärderna inte behöver avvaktas för att en bedömning av riskerna i samband med kommande kundrelationer eller transaktioner ska kunna göras, omfattas av det underlag som ska beaktas i det tidigare steget (steg 2). Det kan röra sig om sådant som så att säga är inbyggt i produkten såsom beloppsbegränsningar eller att den är avsedd för en begränsad marknad såväl geografiskt som med avseende på kundkategori.

Faktiska erfarenheter och bedömningar av de åtgärder som vidtas (steg 4) används sedan för att bedöma sannolikhet och konsekvenser när den allmänna riskbedömningen successivt uppdateras med tillämpning av steg 1 och steg 2.

3.4.5 Följ upp och bedöm åtgärderna (steg 4)

3.4.5.1 Inledning

För att säkerställa att företaget har kontroll över de risker som företaget är exponerat för, behöver företaget löpande följa upp och bedöma kontrollåtgärderna, dvs. de mitigerande åtgärdernas effekt. Företaget behöver inte endast följa upp att åtgärder vidtas, utan även av att de fungerar och fyller sitt syfte. Det är därför av betydelse att veta *varför* något är en risk, inte endast *att* det är en risk.

Bedömningen av hur väl åtgärderna har mitigerat riskerna ger en bild av företagets residualrisk, dvs. den risk som företaget exponeras för efter det att mitigerande åtgärder har vidtagits.

Om bedömningen visar att åtgärderna inte ger önskad effekt och att företaget då har en oönskad residualrisk, behöver företaget agera. Det är då viktigt att internt rapportera till behöriga beslutsfattare.

3.4.5.2 Residualrisk

De inneboende riskerna ska sättas i relation till hur effektiva åtgärder som finns för att möta riskexponeringen, resultatet blir verksamhetens residualrisk. En hög inneboende risk kan sänkas med effektiva mitigerande åtgärder, men inte försvinna helt. Det är viktigt att ha en förståelse för både den inneboende risken och residualrisken för att kunna göra en korrekt utvärdering och vidta relevanta åtgärder.

Residualrisken visar om den riskexponering som exempelvis en viss produkt innebär för verksamheten hanteras på ett tillräckligt effektivt sätt. För att minska den inneboende risken behöver antingen effektivare mitigerande åtgärder vidtas eller den inneboende risken minskas genom att företaget exempelvis inte erbjuder en viss typ av produkt.

3.4.5.3 Följa upp och bedöma kontrollåtgärderna

Ett företag bör ta ställning till vilken del av verksamheten som ska ha ansvar för att följa upp arbetet och bedöma arbetet mot penningtvätt och finansiering av terrorism. Det finns klara fördelar med att ansvaret placeras hos en enhet som inte har deltagit i det underliggande arbetet utan kan fungera som en objektiv, kritiskt granskade part. Huruvida detta är genomförbart eller inte är förstås beroende av verksamhetens storlek. Det bör även vara möjligt att låta exempelvis internrevisionsfunktionen utföra granskningen och utvärderingen.

En löpande sammanställning av en riskbedömning för hela företagets verksamhet underlättar vid identifieringen av de risker som finns och därmed också vilka kontroller som krävs. Kontrollerna bör vara som starkast när det gäller de allvarligaste riskerna som har identifierats och kan vara enklare när det gäller mindre risker.

3.4.6 Dokumentera den allmänna riskbedömningen

Den allmänna riskbedömningen ska dokumenteras (2 kap. 2 § penningtvättslagen). Det finns många sätt för att göra detta. Oavsett hur dokumentationen görs, är den viktig av flera skäl. Dokumentationen är del av det underlag som tillsynsmyndigheten har för att förstå de beslut som fattas av verksamhetsutövare under dess tillsyn. Dokumentationen utgör inte bara ett viktigt stöd för verksamhetsutövare att vidta vissa åtgärder. Den ger också ett viktigt stöd för att åtgärder inte vidtas i vissa situationer.

3.4.7 Hålla den allmänna riskbedömningen uppdaterad

Den allmänna riskbedömningen ska hållas uppdaterad (2 kap. 2 § penningtvättslagen). Företaget ska regelbundet, minst årligen, utvärdera sin allmänna riskbedömning och när det behövs uppdatera den. Företaget ska dessutom uppdatera sin allmänna riskbedömning innan det erbjuder nya eller väsentligt förändrade produkter, tjänster, riktar sig till nya marknader eller gör andra förändringar som är relevanta för verksamheten (2 kap. 1 § FFFS 2017:11).

Eftersom företagets riskbedömning utgör grunden för företagets rutiner, riktlinjer och övriga åtgärder mot penningtvätt och finansiering av terrorism är det av avgörande betydelse att riskbedömningen är aktuell och svarar mot bl.a. företagets utbud av produkter och tjänster för att fylla sin funktion. Det är av stor vikt för att upptäcka och förebygga risker för penningtvätt och finansiering av terrorism att företagen ser över riskbedömningen vid lanseringen av nya produkter eller tjänster m.m. men även när företaget vänder sig till nya marknader (Finansinspektionens beslutspromemoria FI Dnr 16–2467 s. 8).

Aktiviteterna inom penningtvätt och finansiering av terrorism utvecklas ständigt. Bedömningen av hur verksamhetens produkter och tjänster kan utnyttjas är ett löpande arbete och det är viktigt att i verksamheten ha en process för detta. Utöver att årligen se över sin allmänna riskbedömning finns det flera situationer som innebär att bedömningen bör revideras (se illustration).

Illustration av det löpande arbetet med den allmänna riskbedömningen

Omvärldsbevakning – Omvärldsbevakningen handlar närmast om att hålla sig uppdaterad i fråga om rapporter och annat från myndigheter, t.ex. Finanspolisen och Säkerhetspolisen samt i fråga om sådant som nationell riskbedömning och beslut från Finansinspektionen.

Lärdomar från verksamheten – I verksamheten finns det mycket kunskap. Lärdomarna från sådant som sker i verksamheten är oerhört viktiga att ta tillvara. Det handlar t.ex. om att agera utifrån iakttagelser i fråga om förändrat kundbeteende.

Nya eller förändrade produkter eller tjänster – Vid utvecklande av nya produkter och tjänster ska risken för att produkten eller tjänsten utnyttjas för penningtvätt och finansiering av terrorism analyseras samt åtgärder vidtas för att mitigera riskerna. Vissa risker kan mitigeras genom själva produkten i stället för exempelvis genom monitorering. Det handlar här om att göra medvetna val. I vissa fall kan en högre initial kostnad kompenseras genom att undvika kostnader som kan uppstå senare, om det skulle visa sig att produkten innebär hög risk för penningtvätt eller finansiering av terrorism.

Ny eller förändrad teknik eller process – Process som påverkar kundbeteende, nya marknader/kunder, ny teknik (t.ex. digitalisering), omorganisation eller nya system. Nya eller förändrade processer kan

leda till att företagets sårbarhet ökar eller minskar. Det är därför viktigt att företaget analyserar vilka riskfaktorer som påverkas och vilka åtgärder som behöver vidtas.

Nya eller förändrade regelverk – Nya eller förändrade regelverk kan indikera att riskfaktorer har förändrats. Detta kan även i sig innebära att vissa riskfaktorer förändras, t.ex. om ett regelverk bidrar till att en sårbarhet i systemet täpps till.