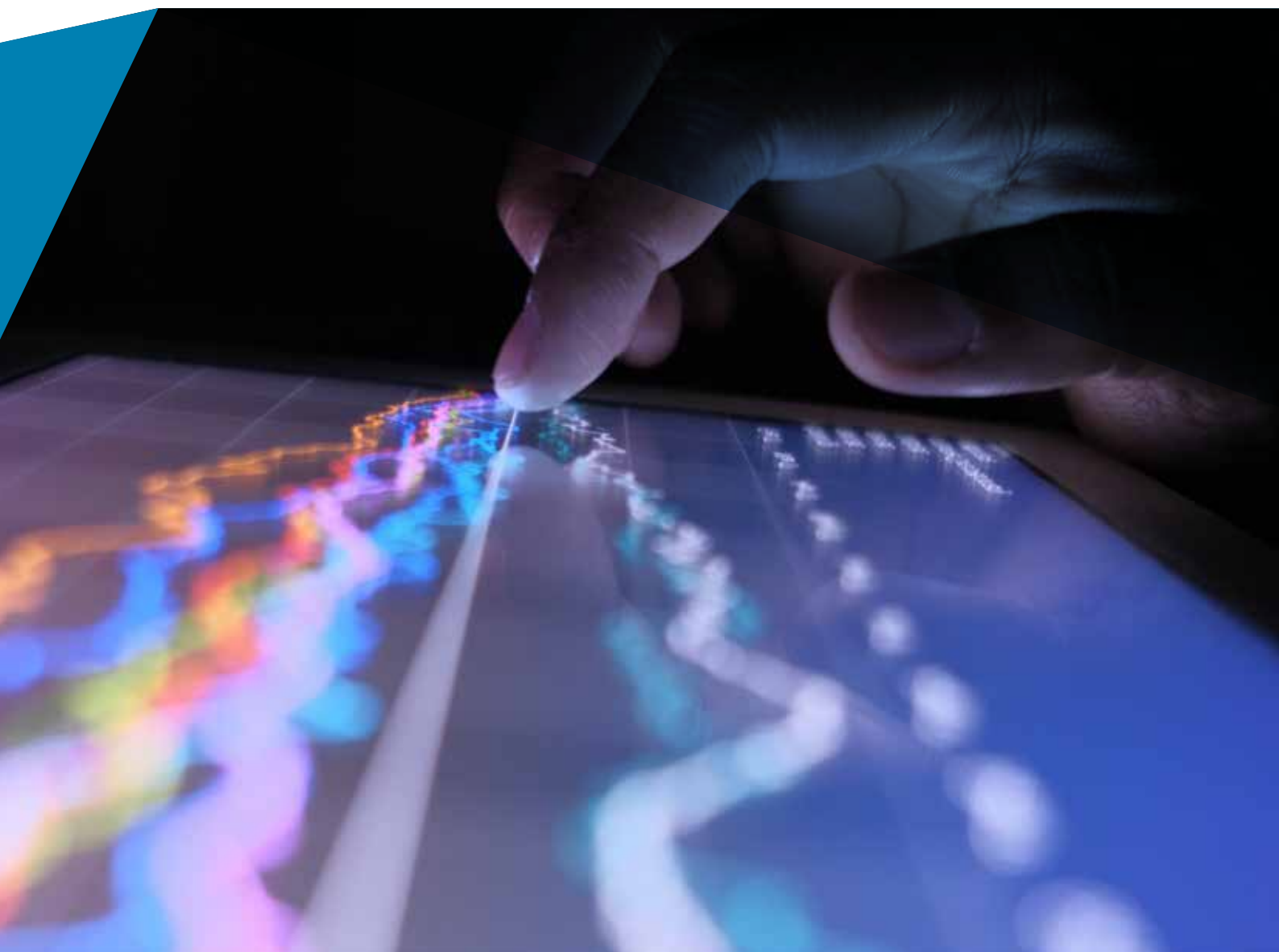


# SAMMANSLUTNING MOT FINANSIELL BROTTSLIGHET

Hur offentlig-privat samverkan kan  
förbättra arbetet mot penningtvätt



# SAMMANFATTNING

Allmänhetens medvetenhet och samhällets fokus på området finansiell brottslighet och penningtvätt har ökat drastiskt de senaste åren. De negativa samhälleliga effekterna av penningtvätt är betydande. Från samhällets perspektiv leder penningtvätt till allvarliga konsekvenser och bidrar bland annat till att olaglig vapenförsäljning, narkotikahandel, prostitution, människohandel och annan organiserad brottslighet kan fortsätta löna sig.

Det finns flertalet brister i hur arbetet fungerar idag som gör att brottslingarna ofta ligger ett steg före trots att bankerna och samhället tillsammans har ett stort informationsövertag. De mest framträdande bristerna är:

- Bristen på samarbete och informationsutbyte mellan banker och myndigheter som gör identifieringen av penningtvätt svår samt medför extra arbete då det saknas synergier;
- Den höga graden av manuell hantering som gör arbetet mot penningtvätt ineffektivt och svårt att skala upp i takt med att omfattning och komplexitet i penningtvättsupplägg ökar

Mycket pekar på att omfattningen av penningtvätt ökar och till följd av de ovan angivna bristerna saknas det idag i viss utsträckning relevanta verktyg och processer för att effektivt motverka denna uppgång. På grund av dessa tillkortakommanden används de stora satsningar som görs inom detta område inte effektivt. Att åtgärda bristerna i systemet försvåras också av gällande lagstiftning. En översyn av lagstiftningen kombinerat med processerna och ansvarsfördelningen är därför befogad.

Penningtvätt är ett globalt problem. Det finns däremot vissa geografiska skillnader i hur arbetet för att upptäcka och motverka penningtvätt ser ut och är organiserat. Det finns exempel på initiativ mot penningtvätt som har visat lovande resultat. Ett sådant område är transaktionsmonitorering där ett utökat samarbete mellan banker och myndigheter, ökar möjligheten att bekämpa penningtvätt.

Denna rapport presenterar en vision för en ny svensk verksamhetsmodell för transaktionsmonitorering som i korthet innebär:

- Upprättande av en samarbetsorganisation mellan banker och myndigheter i arbetet mot penningtvätt för

att styra prioriteringar och stärka dialogen mellan den privata och offentliga sektorn

- En centraliserad analys av transaktionsdata: genom att banker rapporterar rena transaktionsdata till Finanspolisen kan en mer effektiv och avancerad analys göras än vad som är möjlig idag

Baserat på resultat av liknande offentlig-privata samarbeten mot penningtvätt i andra länder, bedöms förslagen som presenteras i denna rapport ha potentiellt stor inverkan mot penningtvätt och annan finansiell brottslighet. Även om uppsättandet av en ny verksamhetsmodell kommer att kräva nya investeringar, kommer den ökade operationella effektiviteten i systemet leda till ökad resurseffektivitet i både privat och offentlig sektor över tid. Detta betyder att kostnaderna för denna typ av verksamhet, som idag ökar kraftigt på grund av mängden manuella moment, på sikt kommer kunna minska. Eftersom bankerna är ansvariga för att övervaka de transaktioner som görs i verksamheten, bör de finansiera det tillkommande arbete och de nya investeringar som enligt våra förslag ska ske i offentlig regi. Givet att bankerna har getts en polisliknande uppgift i arbetet mot finansiell brottslighet men inte har getts tillräckliga legala förutsättningar för att utföra dessa uppgifter på ett effektivt sätt förutsätter förslagen att bankerna ges erforderliga verktyg och legala möjligheter att göra det.

Rapporten presenterar också ett antal förbättringar som kan göras på kortare sikt, som inte bedöms ha utmaningar som den långsiktiga visionen och som därför bör kunna implementeras snabbare. Genom att sätta upp en samarbetsorganisation mellan den offentliga och privata sektorn, kan dagens arbetssätt mot finansiell brottslighet förbättras och effektiviseras. Dels föreslås ett övergripande strategiskt samarbetsorgan, dels också ett operationellt samarbete som innebär att bankrepresentanter utstationeras hos Finanspolisen/ Underrättelseenheten för att tillsammans granska och utreda misstänkta fall av penningtvätt i realtid genom skapandet av en "safe harbour" mellan myndigheter och banker. Detta samarbete kan vidare användas för att leda utvecklingen och implementeringen av den långsiktiga verksamhetsmodellen.

# INNEHÅLLSFÖRTECKNING

<b>INLEDNING</b>	<b>4</b>
<b>DET NUVARANDE ARBETET MOT PENNINGTVÄTT OCH DESS UTMANINGAR</b>	<b>5</b>
Omfattning av penningtvätt och bekämpningens effektivitet	5
Organisering av det nuvarande arbetet mot penningtvätt och dess utmaningar	6
<b>INTERNATIONELLA ERFARENHETER VISAR ATT NYA SÄTT ATT SAMARBETA KAN GE STOR FÖRBÄTTRING</b>	<b>10</b>
<b>FÖRBÄTTRING GENOM UTÖKAD SAMVERKAN SOM ETT FÖRSTA STEG</b>	<b>12</b>
Styrgrupp för offentlig-privat samarbete	13
Operativ anti-penningtvättskommitté mellan banker och Polismyndigheten	14
En operativ samarbetsgrupp inom Fipo/Noa	14
<b>VISION FÖR EN NY VERKSAMHETSMODELL: EN OFFENTLIG-PRIVAT SAMVERKAN MOT PENNINGTVÄTT</b>	<b>16</b>
Den nya verksamhetsmodellen i praktiken	16
Fördelar och kostnader med den nya verksamhetsmodellen	20
Utmaningar som måste ses över i samband med den nya verksamhetsmodellen	22
<b>TIDSLINJE OCH IMPLEMENTERINGSPLAN</b>	<b>24</b>
<b>APPENDIX I: MYNDIGHETERNAS ROLL I DET SVENSKA ANTI-PENNINGTVÄTTSARBETET</b>	<b>25</b>
<b>APPENDIX II: PROCESSERNA I DEN LÅNGSIKTIGA VERKSAMHETSMODELLEN</b>	<b>28</b>
<b>APPENDIX III: CENTRAL ANALYSKAPACITET OCH DATABAS</b>	<b>30</b>

# INLEDNING

Allmänhetens medvetenhet och samhällets fokus på området finansiell brottslighet och penningtvätt har ökat avsevärt under de senaste åren. De negativa samhällseliga effekterna av penningtvätt är betydande. Från samhällets perspektiv leder penningtvätt till allvarliga konsekvenser och bidrar bland annat till olaglig vapenförsäljning, narkotikahandel, prostitution, människohandel och annan organiserad brottslighet kan fortsätta löna sig.

Banker spelar en avgörande roll i att förhindra att det finansiella systemet utnyttjas för penningtvätt på grund av deras fundamentala roll i det finansiella systemet. Kraven på bankernas åtgärder mot penningtvätt har även ökat markant det senaste årtiondet. Varje dag granskas miljontals transaktioner inom bankernas monitoreringssystem och tusentals larm om misstänkt penningtvätt utreds årligen av allt fler dedikerade anti-penningtvättsanalytiker på bankerna och utredare på myndigheterna.

Trots att bankerna generellt har väl utarbetade system, processer, och strategier på plats för att identifiera och förebygga penningtvätt tyder mycket på att dessa investeringar endast har begränsad påverkan på den faktiska bekämpningen av finansiell brottslighet. En allmän uppfattning, från såväl banker som myndigheter, är att regel efterlevnad inte i alla avseenden leder till att den faktiska risken för ekonomisk brottslighet hanteras.

I denna rapport, som har skrivits på uppdrag av Svenska Bankföreningen, beskrivs hur bristerna och problemen med arbetet mot penningtvätt i Sverige kan avhjälpas genom ett utökat samarbete mellan privat och offentlig sektor. Baserat på hur samarbeten ser ut i andra länder presenteras ett antal förslag och rekommendationer om hur effektiviteten i att motverka finansiell brottslighet skulle kunna förbättras, både på kort och lång sikt.

Eftersom penningtvätt ofta sker över landsgränser skulle arbetet bli mer effektivt ju fler länder som ingår i samarbetet. Men eftersom det krävs samarbete mellan privata aktörer och offentliga myndigheter blir komplexiteten snabbt alltför stor. I en framtid där flera länder lyckats skapa väl fungerande nationella samarbeten underlättas dock möjligheten att kunna samarbeta över nationsgränserna.

# DET NUVARANDE ARBETET MOT PENNINGTVÄTT OCH DESS UTMANINGAR

Banker och myndigheter, i såväl Norden som globalt, har under senare år genomfört omfattande förändringar i arbetet mot finansiell brottslighet. Även om det intensifierade arbetet och de stora investeringar som gjorts har förbättrat situationen, kämpar fortfarande banker och myndigheter med att på ett effektivt sätt hindra och försvåra finansiell brottslighet. Samtidigt blir tillvägagångssätten för att tvätta pengar alltmer sofistikerade och svåra att upptäcka.

## OMFATTNING AV PENNINGTVÄTT OCH BEKÄMPNINGENS EFFEKTIVITET

United Nations Office on Drugs and Crime (UNODC) uppskattar att global penningtvätt varje år uppgår till mellan 2-5 % av global BNP, vilket motsvarar 800 till 2000 miljarder dollar. Om motsvarande uppskattning skulle användas i Sverige skulle det innebära att omfattningen av penningtvätt varje år skulle uppgå till mellan 97 – och 242 miljarder SEK.<sup>1</sup> En annan uppskattning som ibland

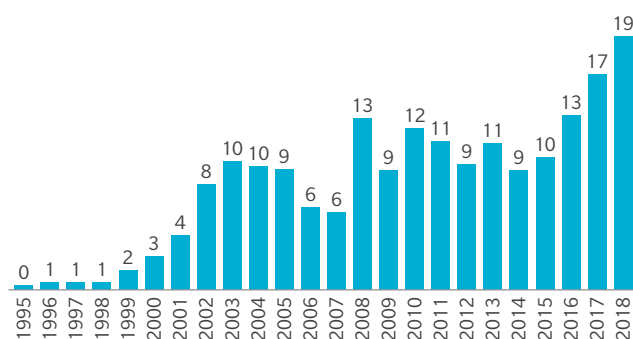
används är Skatteverkets beräkningar av det totala skattefelet i Sverige som är cirka 130 miljarder kronor om året, vilket ligger inom intervallet ovan. Skatteverkets beräkningar inbegriper dock en rad andra fel utöver de som utgör penningtvättbrott.<sup>2</sup>

I Finanspolisens (Fipo) statistik tydliggörs att antalet rapporter om misstänkt penningtvätt har ökat kontinuerligt de senaste åren.<sup>3</sup> Trots att antalet dispositionsförbud och värdet av det totala antalet beslut om dispositionsförbud ökade kraftigt 2018 jämfört med tidigare år, är det från mycket låga nivåer i förhållande till antalet inkomna rapporter om misstänkt penningtvätt (mindre än en procent).<sup>4</sup>

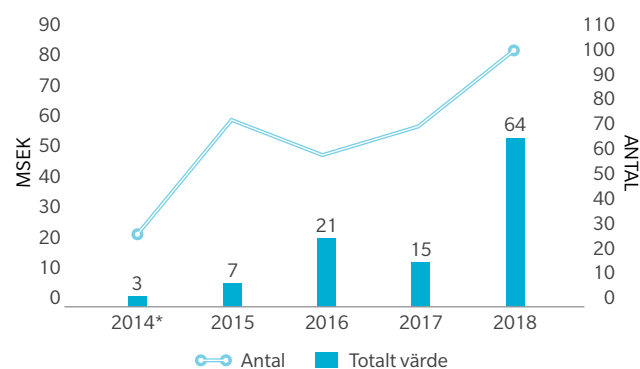
Figur 1: Utvecklingen av inkomna rapporter till Finanspolisen i förhållande till utfärdade dispositionsförbud visar på en stadig ökning och att det finns anledning att se över effektivitetsaspekter

Inkomna rapporter om misstänkt penningtvätt till Finanspolisen

Antal rapporter i tusen



Antal och värde av utfärdade dispositionsförbud



Källa: Finanspolisen

\* Endast data från juli-december

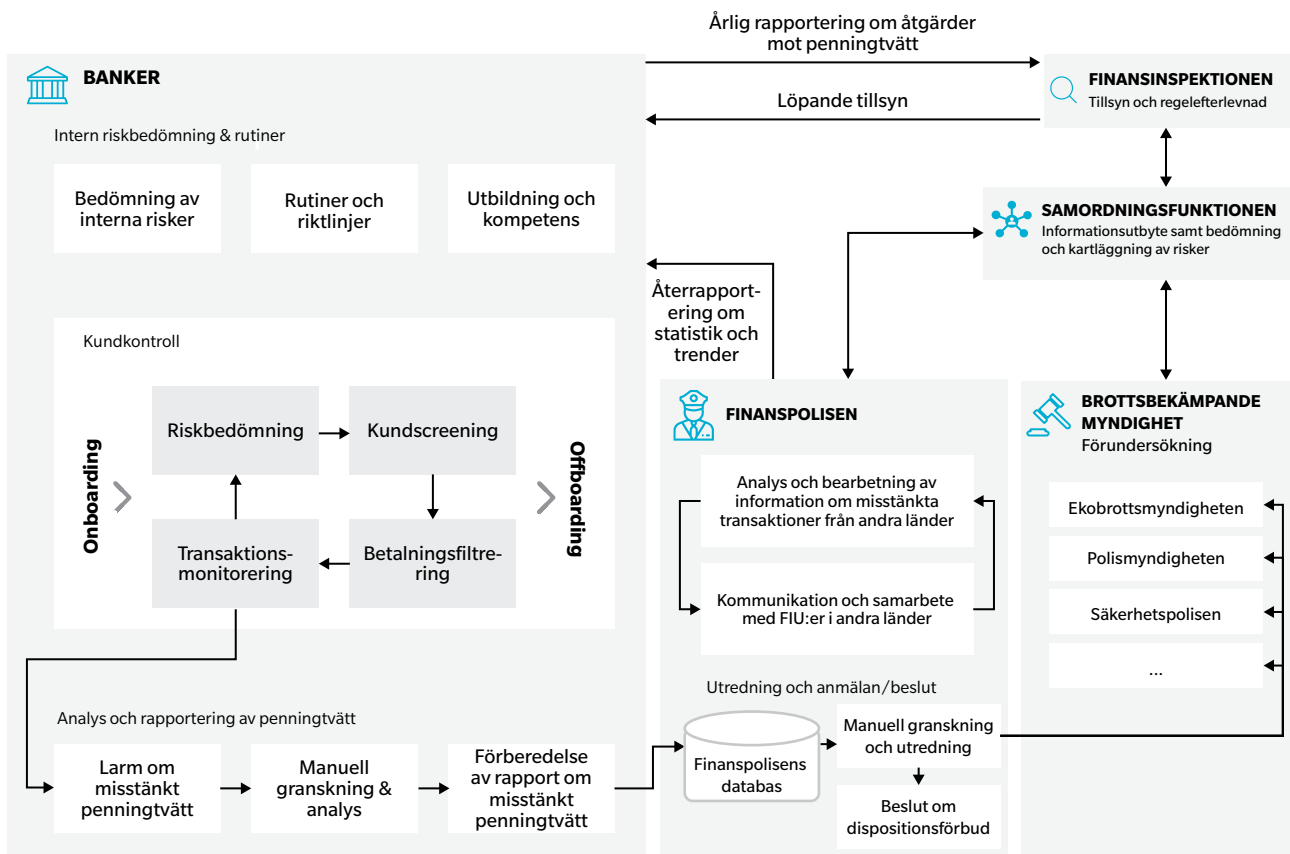
1. Statistiska centralbyrån, 2018  
2. Brottsförebyggande rådet (Brå)  
3. Finanspolisen  
4. Finanspolisen

# ORGANISERING AV DET NUVARANDE ARBETET MOT PENNINGTVÄTT OCH DESS UTMANINGAR

Nedanstående figur ämnar illustrera hur arbetet mot penningtvätt är organiserat i Sverige. För banker innebär arbetet att identifiera och hantera risker under kundens livscykel. För myndigheterna innebär det att bedriva tillsyn över bankerna, utbyta information

om trender och risker, granska och utreda misstänkt penningtvätt och väcka åtal. Några viktiga myndigheter för arbetet är Finansinspektionen (FI), Fipo (som är Sveriges Financial Intelligence Unit eller FIU) och de brottsbekämpande myndigheterna.

Figur 2: Övergripande illustration av det nuvarande arbetet mot penningtvätt



Bankernas arbete med att motarbeta penningtvätt och terroristfinansiering sker inom två huvudsakliga områden:

- **Kundkännedom:** Kravet på att uppnå kundkännedom gäller för varje bank och är centralt i introduktionsprocessen av nya kunder och i den fortlöpande riskbedömningen och övervakningen
- **Transaktionsmonitorering:** Transaktionsmonitoreringen avser att fånga kundernas beteenden och är en av de viktigaste övervakningsmekanismerna för att identifiera och motverka penningtvätt

Genom god kundkännedom och effektiv analys av kundernas transaktioner kan bankerna identifiera misstänkt penningtvätt och rapportera misstanken till Fipo, som därefter bedömer om ärendet ska tas vidare till de brottsbekämpande myndigheterna.

## KUNDKÄNNEDOM

Kundkännedom är en del av den introduktionsprocess som krävs för att en bank ska kunna inleda en affärsrelation med en kund. Kundkännedom ska därefter uppnås och bibehållas under hela affärsförbindelsen. Rent tekniskt kräver ett effektivt system för kundkännedom en central databas som hanterar komplett data om kunden från bankens olika system och avdelningar. Den interna information som banken har om kunden är oftast inte tillräcklig utan banker behöver normalt sett inhämta och bearbeta tredjepartsdata om kunden för att uppfylla kundkännedomskraven. De fortsatta investeringarna hos bankerna på detta område bedöms därför handla om att fortsätta att utveckla strukturerade datamodeller, att säkerställa en effektiv integrering av tredjepartsdata och att upprätta en samlad källa till all kunddata.

## IDENTIFIERING AV VERKLIGA HUVUDMÄN

Bakgrunden till det stora antalet källor som behövs är den omfattande kartläggning av ägarstruktur och identifiering av verkliga huvudmän som krävs för företagskunder. Identifiering av verkliga huvudmän är ofta en av de största utmaningarna för bankerna i kundkännedomsarbetet

då det kan handla om komplexa företagsstrukturer som kan sträcka sig över flera länder och ägande i flera led. Idag har också olika länder olika grad av transparens- och upplysningskrav avseende företags ägarstrukturer. Den information som enskilda banker har är inte nödvändigtvis tillräcklig. De externa källor som krävs och som måste integreras i existerande kundkännedomssystem för att kunna göra en fullständig analys av verkliga huvudmän sträcker sig från offentliga källor (såsom Bolagsverket), till kommersiella leverantörer av företagsinformation, data från tillsynsmyndigheter och andra myndigheter, samt media. Bolagsverket ansvarar idag för ett register av verkliga huvudmän, men det är svårt för banker att säkert veta att uppgifterna som rapporteras in är korrekta eftersom Bolagsverket inte är ansvariga för att löpande validera registret.

Utmaningen slutar inte när den första identifieringen och verifieringen är fullständig, utan bankerna måste kontinuerligt fortsätta att övervaka verkliga huvudmän. Det finns därför en stor praktisk svårighet i att säkerställa att rätt information om verklig huvudman hålls uppdaterad över tid eftersom juridiska personer tenderar att byta verklig huvudman.

## BEGRÄNSADE MÖJLIGHETER FÖR BANKER ATT SAMARBETA MOT OÖNSKADE KUNDER

Eftersom det inte är tillåtet att registrera eller informera om avslutade kunder, eller kunder som har bedömts utgöra hög risk för penningtvätt mellan banker, kan eventuella brottslingar fortsätta sin aktivitet genom att byta bank. I de fall en kund byter bank får följaktligen den nya banken starta om kundkännedomsprocessen med endast den informationsmängd som finns tillgänglig för den banken. Under gällande regelverk är det inte tillåtet att registrera avslutade kunder eller kunder som har bedömts utgöra hög risk för penningtvätt på en "svartlista" som är tillgänglig mellan banker vilket leder till att brottslingar kan fortsätta sin brottsliga aktivitet genom att byta bank.



## TRANSAKTIONSMONITORERING

Transaktionsmonitorering handlar om att skapa effektiva kontroller för att övervaka och granska de transaktioner som kunderna gör i banken. Trots det omfattande arbetet som de svenska bankerna har lagt på transaktionsmonitorering är det endast omkring 2-5 procent<sup>5</sup> av interna larm om misstänkt penningtvätt som faktiskt resulterar i en rapport om misstänkt penningtvätt som sedan skickas in till Fipo.

En hög andel falska larm har en negativ inverkan på såväl kostnader som den övergripande effektiviteten i utredningsarbetet. Eftersom bankernas interna data ofta inte räcker för att fatta ett definitivt automatiskt beslut om ett larm är falskt eller inte, behöver analytiker på banken förlita sig på externa informationskällor, såsom offentliga databaser och myndighetsregister, mediala källor, sociala medier, etc. Den manuella analysen och granskningen är tidskrävande och beroende av den enskilda analytikerns förmåga att länka ihop materialet från interna och externa källor.

Ett stort problem är att varje enskild bank inte kan skapa tillräckligt träffsäkra analysmodeller eftersom de inte har information om vilka historiska utfall av faktisk penningtvätt som har kunnat konstateras. Detta beror på att Fipo inte har möjlighet att ge banken återkoppling om individuella kunder. Det innebär att bankerna inte kan validera och justera sin transaktionsmonitorering baserat på verkliga utfall. Som jämförelse vore en kreditriskmodell (med syfte att förutsäga kreditförluster) utan fallissemangsdata svårskattad och troligen helt oanvändbar. Vidare är generell återkoppling till bankerna begränsad (gällande till exempel typologier och kvalitet på den rapportering som görs) vilket ytterligare begränsar bankernas förmåga att förbättra och öka effektiviteten i sina processer.

Varje mottagen rapport om misstänkt penningtvätt omhändertas manuellt av Fipo och en bedömning görs i varje enskilt fall. Fipo saknar idag det IT-stöd som krävs för att kunna utföra mer avancerad

analys (såsom nätverksanalys) av inrapporterade transaktioner. Det finns därför en risk att mer avancerade penningtvättsupplägg som involverar flera tillsynes orelaterade transaktioner kan passera genom Fipo:s kontroller obemärkt, eftersom de inte kopplas samman. Detta är också något som framhävs i FATF:s (The Financial Action Task Force) utvärdering<sup>6</sup> av det svenska arbetet mot finansiell brottslighet.

Hur snabbt banker och myndigheter hanterar misstänkt penningtvätt är avgörande för effektiviteten i kampen mot finansiell brottslighet. På grund av de orsaker som nämns ovan är det inte ovanligt att tidsåtgången från ett initialt larm, till att en rapport om misstänkt penningtvätt har fyllts i och skickats till Fipo, uppgår till flera dagar. Med flera dagars ledtid från att en misstänkt transaktion har skett till att Fipo mottar en rapport om misstänkt penningtvätt är sannolikheten låg att pengarna fortfarande finns kvar. Att den manuella granskningen och analysen hos Fipo tar ytterligare tid gör sannolikheten ännu lägre.

Bankernas kostnader för att motverka penningtvätt har stigit kontinuerligt och förväntas enligt majoriteten av svenska storbanker fortsätta stiga kommande år. Även om bankerna investerar i ny och mer avancerad analysförmåga kräver en effektiv monitorering en större informationsmängd än vad som finns tillgänglig inom en enskild bankkoncern. Investeringar och utveckling som görs av och inom enskilda banker riskerar därför att inte ge den positiva effekt som söks. Därtill kommer att myndigheterna har begränsade resurser att utreda fallen vidare. Behovet av samverkan mellan privat och offentlig sektor inom transaktionsmonitorering är därför helt avgörande för att uppnå effektivitet och ett tillräckligt starkt samhällsligt skydd framöver.

5. Oliver Wyman annual AML benchmarking survey

6. FATF är en global, oberoende organisation som arbetar med främja en effektiv bekämpning av penningtvätt, finansiering av terrorism och andra relaterade hot mot det internationella finansiella systemets integritet. Som en del av detta arbete utvärderas medlemsländerna i syfte att skapa rekommendationer kring förbättringsområden.



## Verksamhet

## Sammanfattning av utmaningar

Kundkännedomsprocessen präglas i stor utsträckning av manuell analys och kontroll, där effektivitetsperspektivet har kommit i skymundan. Identifiering och uppföljning av verkliga huvudmän lyfts fram som det främsta problemet

### Banker



Begränsningar i datahantering, system och automatiserad analysförmåga innebär att få transaktionslarm leder till rapport om misstänkt penningtvätt. Den höga andelen falska larm och efterföljande manuella analyser gör anspråk på stora resurser och kostnader

Frånvaro av återkoppling och information från Fipo och andra myndigheter till banker (gällande framförallt konstaterade fall av penningtvätt) gör det svårt för bankerna att skapa träffsäkra analysmodeller för att identifiera faktiska fall av penningtvätt

Begränsade möjligheter för banker att dela information om misstänkt penningtvätt mellan varandra

Fipo:s resurser är begränsade och myndigheten saknar tillräckligt avancerade IT-system för att hantera volymen av inkomna rapporter

### Fipo



Bearbetningen av inkomna rapporter är i hög grad manuell och möjligheten att avslöja mer komplexa penningtvättsupplägg är därför begränsad

Begränsad återrapportering från Fipo till bankerna hämmar bankernas möjlighet att förbättra rapportering och analys

### Samordningsfunktionen



Behov av högre grad av informationsutbyte mellan myndigheter inom Samordningsfunktionen krävs för att mer effektivt förebygga penningtvätt. Motstridiga prioriteringar mellan myndigheter inom funktionen försvårar samarbetet

### Finansinspektionen



Finansinspektionen har begränsade resurser, vilket försvårar möjligheten att bedriva en effektiv tillsyn av bankernas arbete för att motverka penningtvätt

### Brottsbekämpande myndigheter



En låg andel av de misstänkta fall som genereras används i faktiska utredningar och antalet dispositionsförbud som utfärdas är lågt

# INTERNATIONELLA ERFARENHETER VISAR ATT NYA SÄTT ATT SAMARBETA KAN LEDA TILL STOR FÖRBÄTTRING

De senaste åren har det initierats ett antal initiativ i omvärlden som visar på att effektiviteten i anti-penningtvättsarbetet kan förbättras av olika samarbeten mellan privata och offentliga aktörer, genom utbyte, tillgänglighet och analys av information. Dessa initiativ kan enkelt beskrivas i tre huvudkategorier, med olika grad av samarbete:



## PRIVATA SAMARBETSGRUPPER



## OFFENTLIG-PRIVATA TEMATISKA SAMARBETEN



## OPERATIVA OFFENTLIG-PRIVATA SAMARBETEN

Med ökad samarbetsgrad ökar ofta omfattningen av de förbättringar som kan göras, men dessa samarbeten kan också kräva stora investeringar och legala förändringar. Samarbetslösningar inom den privata sektorn utan inblandning av någon offentlig myndighet är svåra att genomföra inom transaktionsmonitorering på grund av de begränsningar som till exempel banksekretessen och meddelandeförbudet ger upphov till. För att skapa en långsiktig förbättring är det också viktigt att etablera ett övergripande och löpande samarbete, snarare än att fokusera endast på tematiska insatser. På grund av myndigheternas centrala roll i bekämpningen av penningtvätt krävs det också en samsyn mellan privat och offentlig sektor för att kunna skapa större förändringar och förbättringar. Även om lagstiftning kan behöva ses över i ett offentlig-privat samarbete (beroende på syfte och omfattning), visar de internationella exemplen att processen förenklas genom att både myndigheter och privata aktörer samlas vid samma bord. De illustrerar också att det finns alternativ som kan genomföras på kortare sikt, med viss del av informationsdelning (genom skapande av så kallade "safe harbours" mellan privata aktörer och offentliga myndigheter), som kan öka effektiviteten i arbetet mot penningtvätt.

För att skapa en lösning med stor genomslagskraft i arbetet mot penningtvätt krävs att ett större omtag görs, samtidigt som man bör beakta vad som kan göras på kortare sikt. Den långsiktiga vision som presenteras i denna rapport baseras på dessa lärdomar och bygger därför på att Sverige bör ha en operativ offentlig-privat samarbetslösning.

Det finns framför allt två operativa offentlig-privata samarbeten som bör lyftas fram: Storbritanniens JMLIT ("Joint Money Laundering Task Force") och Australiens Fintel Alliance. Dessa beskrivs vidare nedan. Både de aktiviteter som föreslås på kort sikt i denna rapport för att utöka samverkan mellan privat och offentlig sektor, och den långsiktiga visionen för en verksamhetsmodell baseras på dessa och andra lärdomar.

## STORBRITANNIEN: JMLIT

Införandet av JMLIT, som initialt drevs av bankerna, innebar att bankerna kunde dela information sinsemellan utan risk för rättsliga påföljder. Detta förutsatte att "The National Crime Agency" (NCA) inkluderades i informationsutbytet. Inom ramen för JMLIT-samarbetet har en central informationshubb etablerats som NCA har tillsyn över och som finansinstitutet och övriga medlemmar har tillgång till. Detta samarbete grundades med det specifika syftet att möjliggöra för finansiella institutioner och brottsutredande myndigheter att mer effektivt kunna dela och analysera information för att förebygga och underminera penningtvätt.

JMLIT har haft en positiv inverkan, både mätt i form av penningbeslag och faktiska arresteringar.<sup>7</sup> Ytterligare effekter associerade med samarbetet är bland annat kontinuerlig förbättring av rutiner och riskbedömning hos verksamhetsutövare genom att "best practice" sprids mellan banker inom forumet.

7. The National Crime Agency (NCA) - <https://nationalcrimeagency.gov.uk/what-we-do/national-economic-crime-centre>

Detta utbyte har förbättrats avsevärt genom möjligheten att dela data från fall under NCA:s tillsyn utan att exponeras för legala risker avseende persondatahantering.<sup>8</sup> Det brittiska samarbetet har särskilt lovordats i FATF:s utvärdering för dess innovativa modell för informationsutbyte.

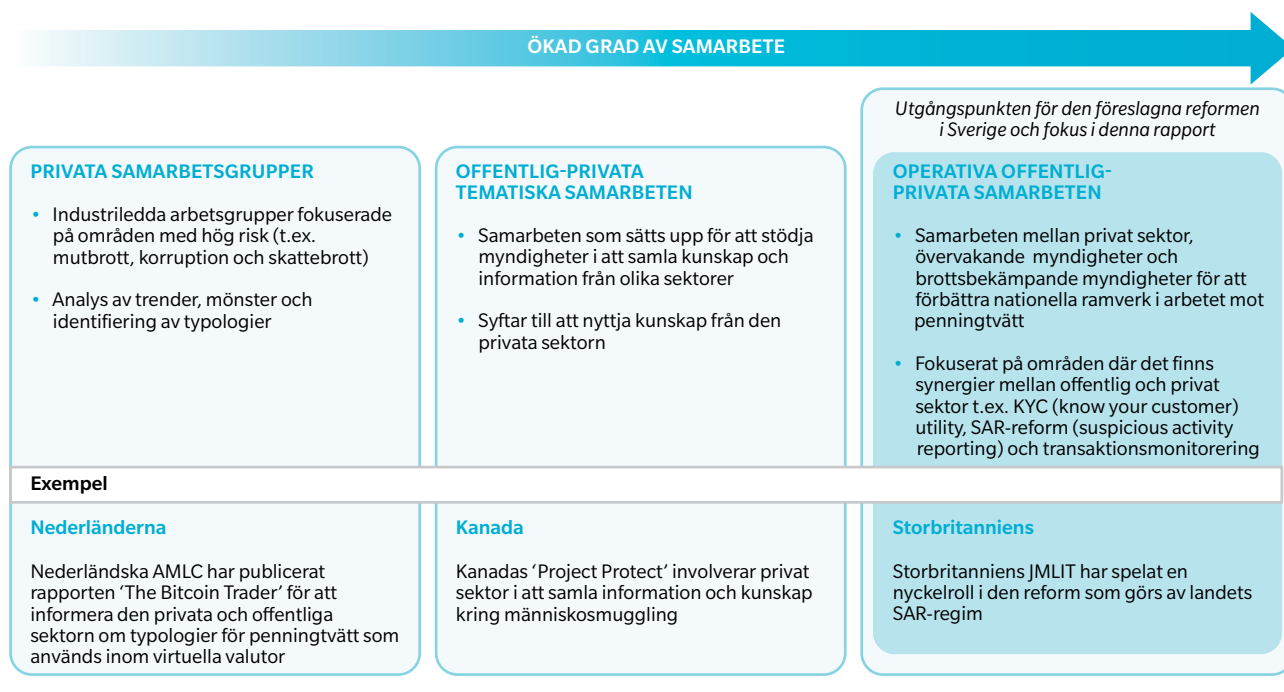
Det brittiska samarbetet utvecklas fortfarande och ett område som nu ses över är transaktionsmonitoreringen. Här undersöks hur hanteringen av misstänkta fall kan utvecklas och effektiviseras där man ämnar bygga ett komplett system för att motverka ekonomisk brottslighet. Ambitionen är att leverera betydligt högre nivåer av upptäckt, förebyggande och verkställande. Projektet inkluderar således utveckling och utökning av analys och IT-verktyg såväl som förbättring av feedback-processer både till rapporterande verksamheter och brottsbekämpande myndigheter. Projektet är fortfarande i en design- och utredningsfas och utvärdering av eventuella lagändringar som kan komma att krävas är ännu inte slutförd.

## AUSTRALIEN: FINTEL ALLIANCE

Australien är ytterligare ett exempel på där det upprättats ett framgångsrikt samarbete mellan privata och offentliga aktörer i arbetet mot penningtvätt. 2017 infördes det privat-offentliga partnerskapet "Fintel Alliance" i syfte att utöka samarbetet mellan myndigheter och verksamhetsutövare och därigenom förbättra informationsutbyte och analys för att motverka penningtvätt. Det australiensiska samarbetet utformades som en del inom AUSTRAC (The Australian Transaction Reports and Analysis Centre) som är landets FIU.

Det som pekas ut som särskilt unikt med Fintel Alliance är dess operationella hubb. Denna hubb utgörs av en fysisk plats där representanter från de olika parterna i samarbetet (banker, FIU, andra brottsbekämpande myndigheter, etc.) träffas för att dela och analysera information och misstänkta transaktioner i realtid. Dessutom driver Fintel Alliance en innovationshubb. Innovationshubben är en plattform som delas mellan medlemmarna för gemensam design och utveckling av nya teknologiska lösningar för datainsamling och analys.

Figur 3: Exempel på samarbeten i andra länder



8. <https://www.parliament.uk/documents/impact-assessments/IA16-011A.pdf>

# FÖRBÄTTRING GENOM UTÖKAD SAMVERKAN SOM ETT FÖRSTA STEG

Även om det krävs en mer omfattande översyn av nuvarande verksamhetsmodell på lång sikt är det viktigt att först etablera en organisation där offentliga och privata aktörer kan skapa ett gemensamt forum för arbetet mot penningtvätt. Parallellt med den utveckling som krävs av den långsiktiga verksamhetsmodellen har därför ett antal förbättringsåtgärder identifierats, som kan implementeras som ett första steg. Det handlar om utökat samarbete och koordinering mellan banker och myndigheter. Vi bedömer att dessa kan genomföras snabbt med ambitionen att bana väg för den långsiktiga visionen genom att skapa en bättre förståelse för vilka möjligheter och begränsningar de olika aktörerna har. Genom att kunna visa på tydliga förbättringsresultat bör arbetet mot den långsiktiga visionen kunna accelereras. Dessa förslag behöver emellertid prövas och utvärderas utifrån gällande lagstiftning och genomföras så gott det går under gällande förutsättningar. En statlig

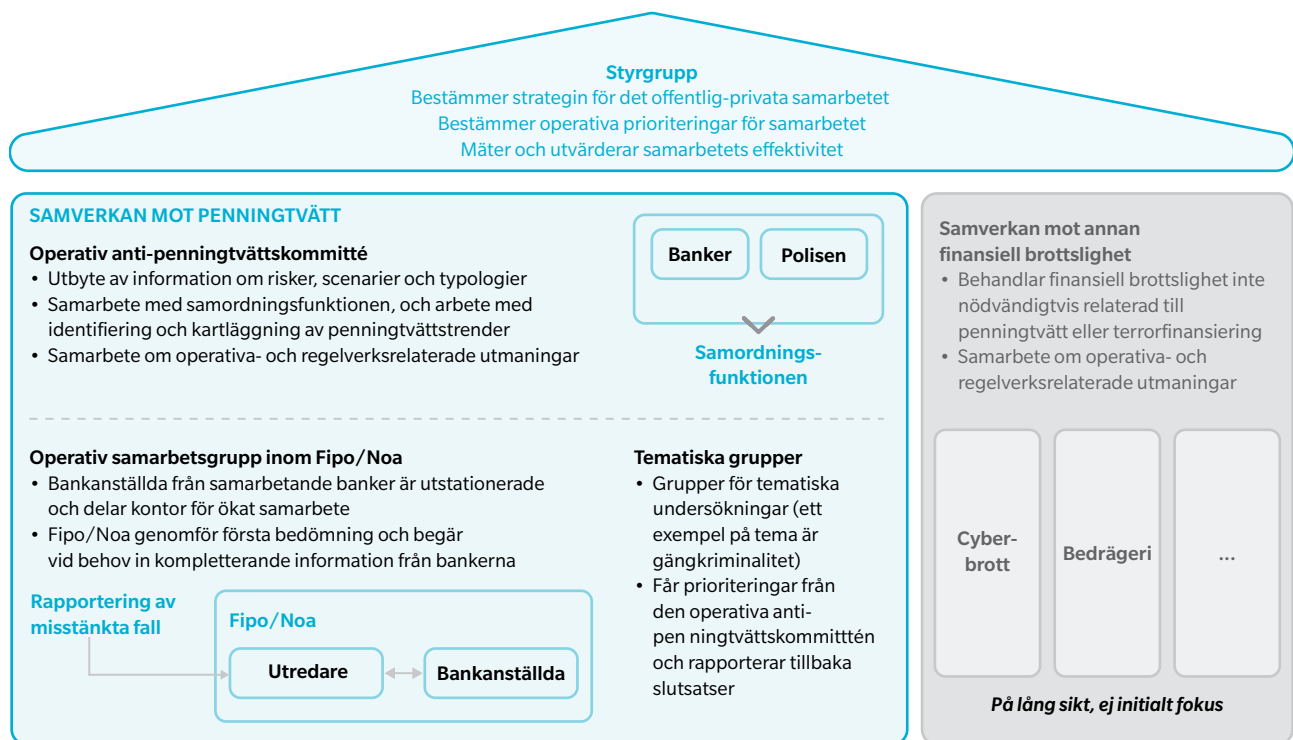
utredning är tillsatt för att vidare utvärdera möjligheter för bland annat informationsdelning mellan banker och myndigheter i arbetet mot penningtvätt, vilket kan förbättra möjligheterna på sikt.

Den utökade samverkan på kort sikt innefattar skapandet av:

- En styrgrupp för långsiktigt offentlig-privat samarbete
- En operativ anti-penningtvättskommitté med företrädare för banker och Polismyndigheten
- En operativ samarbetsgrupp med Fipo/Noa

Organisationen är illustrerad nedan. Utöver de ovannämnda funktionerna finns det anledning att inom samma organisation upprätta specifika projekt/tematiska grupper fokuserade på strategiskt viktiga områden, exempelvis gängrelaterad brottslighet.

Figur 4: Övergripande organisation för utökad offentlig-privat samverkan



På sikt kan organisationen, som initialt sätts upp för penningtvättsfrågor, även användas för samordning av andra aktiviteter och informationsdelning i bekämpningen av finansiell brottslighet. Så länge som det är tydligt att ingen transaktions- eller kunddata delas mellan bankerna är den kortsiktiga lösningen inte heller exponerad för samma legala utmaningar som den långsiktiga lösningen.

## STYRGRUPP FÖR OFFENTLIG-PRIVAT SAMARBETE

Det rekommenderas att en strategisk styrgrupp mellan relevanta myndigheter och banker etableras. Styrgruppens uppgift ska vara att bestämma den långsiktiga strategiska riktningen för samarbetet. För att underlätta etableringen av samarbetet och påbörja arbetet snabbare, rekommenderas att samarbetet etableras inom en existerande avdelning inom Polismyndigheten med relevanta behörigheter och befogenheter, till exempel Polismyndighetens Nationella Operativa Avdelning (Noa), som ansvarar för bland annat Fipo. Fördelen med att etablera samarbetet

inom Polismyndigheten är att medlemmarna i viss utsträckning kan förlita sig på befintlig lagstiftning och underlätta informationsdelning mellan intressenter. Förslagsvis leder relevant avdelning inom Polismyndigheten samarbetet med omfattande bidrag från andra myndigheter och banker inom samarbetet.

Styrgruppen skulle ansvara för att nödvändiga avtal, policydokument och riktlinjer etableras och upprätthålls inom samarbetet. Det behöver bestämmas vilka kommittéer och andra förberedande eller beslutande organ som behöver ingå i styrningen av samarbetet.

Baserat på den utarbetade strategin och de operativa prioriteringarna för det offentlig-privata samarbetet ansvarar styrgruppen för att upprätta nödvändig organisation. Förslag på den organisation som initialt kan upprättas för att förbättra arbetet kring transaktionsmonitorering presenteras nedan: en operativ anti-penningtvättskommitté mellan banker och Polismyndigheten och en operativ samarbetsgrupp med Fipo/Noa.

### STYRGRUPPEN BÖR HA TRE ÖVERGRIPANDE MÅLSÄTTNINGAR OCH UPPDRAG

---

#### Bestämma strategin för det offentlig-privata samarbetet

- Utarbeta en strategi för att implementera visionen och upprätta strategiska mål för samarbetet
- Ansvara för att kommunicera vision, syfte och strategiska mål både inom samarbetet och externt
- Löpande styra samarbetet baserat på den bestämda strategin

#### Bestämma operativa prioriteringar för samarbetet

- Genom informationsutbyte med Samordningsfunktionen gällande bland annat den nationella riskbedömningen samt andra källor bestämma prioriteringar för samarbetet
- Kontinuerligt omvärdera prioriteringar baserat på hur den nationella riskbilden förändras
- Kommunicera och styra prioriteringar inom det operativa arbetet

#### Mäta och utvärdera samarbetets effektivitet

- Löpande mäta effektiviteten av samarbetet baserat på den bestämda strategin
  - Utvärdera leveranser av både operativa prioriteringar och strategiska målsättningar
-

## OPERATIV ANTI-PENNINGTVÄTTSKOMMITTÉ MELLAN BANKER OCH FIPO/NOA

För att på kort sikt öka samarbetet och effektiviteten i arbetet mot penningtvätt föreslås att en operativ kommitté mellan banker och relevant avdelning inom Polismyndigheten etableras.

Ambitionen är att kontinuerligt utbyte av erfarenheter och utmaningar ska lägga grunden för en ökad förståelse

för respektive aktörers möjligheter och begränsningar. På så vis skapa förutsättningar för ett bättre samarbete. Initiala bedömningar är att den beskrivna kommittén inte skulle kräva vare sig lagförändring eller omfattande IT- eller resursmässiga investeringar.

### SYFTET MED DEN OPERATIVA KOMMITTÉN SKULLE VARA

---

#### Utbyte av information om risker, scenarier och typologier

Kommittén skulle analysera nya nationella risker och metoder, typologier, scenarier avseende penningtvätt och undersöka anonymiserade fallstudier av dessa i syfte att informera bankernas och myndigheternas fokus och prioritering. Banker skulle bidra med material från interna bedömningar om risker, tillvägagångssätt och typologier inom penningtvätt och dela med den operativa kommittén.

Kommittén skulle också utvärdera tematiska insatser på strategiskt viktiga områden, exempelvis gängrelaterad brottslighet eller människosmuggling. Beslut kring vilka tematiska insatser som bör genomföras kan till exempel ha den nationella riskbedömningen som utgångspunkt och tas baserat på förslag från kommittén, av styrgruppen

#### Utbyte av information om operativa- och regelverksrelaterade utmaningar

Kommittén bör vidare användas för att utbyta insikter och analyser om operativa erfarenheter och utmaningar, risker, regelefterlevnadsutmaningar, och andra problemområden som upplevs av deltagarna i arbetet mot penningtvätt i syfte att tydliggöra möjligheter och effektivisera processer

---

## EN OPERATIV SAMARBETSGRUPP INOM FIPO/NOA

Flera samarbeten i andra länder bygger på att banker och myndigheter arbetar tillsammans, ibland under samma tak, för att dela och analysera information och underrättelser i närapå realtid. På kort sikt föreslås att en operativ arbetsgrupp mellan banker och myndigheter etableras inom Fipo/Noa eller annan relevant polismyndighet. Grunden för den operativa arbetsgruppen skulle utgöras av att Fipo/Noa, bankanställda från samarbetande banker och representanter från relevanta brottsbekämpande

myndigheter skulle sitta under samma tak och arbeta med verkliga fall i realtid.

Den övergripande strategiska styrgruppen för det privat-offentliga samarbetet skulle bestämma riktningen för den operativa arbetsgruppen för att säkra att prioriteringar, strategiska mål och syfte sätts gemensamt och är i linje med den övergripande visionen och strategin för samarbetet.

## ARBETET I PRAKTIKEN

I den operativa samarbetsgruppen skulle en Fipo/Noa-anställd genomföra en första bedömning av inkomna rapporter om misstänkt penningtvätt. Därefter beslutar Fipo/Noa om huruvida misstanken kan avskrivas omedelbart, om ärendet ska nedprioriteras eller om vidare analys behöver göras. Fipo/Noa kan sedan momentant begära kompletterande information från en eller flera av bankerna som ingår i den operativa samarbetsgruppen.

En ny bedömning kan därefter göras av Fipo/Noa. Om misstanken kvarstår involveras relevant brottsbekämpande myndighet som tar över ärendet och genomför ytterligare analys och genomsökningar i relevanta myndighetsregister. Beroende på misstankegraden kan Fipo/Noa enligt gällande regelverk besluta om dispositionsförbud under utredningsarbetet för att minska risken att medlen försvinner.

Förutsättningen för att denna modell ska fungera är att representanter från samarbetande banker och myndigheter som arbetar inom funktionen erhåller samma befogenheter avseende tillgång till data och omfattas av samma restriktiva lagar avseende delning av information som Fipo/Noa-anställda inom enheten. Likt hur Fintel Alliance i Australien är uppsatt skulle representanter från samarbetande organisationer få dessa behörigheter genom att formellt utstationeras till samarbetsgruppen.

## PROJEKTFOKUSERADE INSATSER

Utöver det löpande samarbetet bör möjligheter finnas för samarbetsgruppen att genomföra de projektfokuserade insatser inom strategiskt viktiga områden som bestäms av kommittén. Dessa projektfokuserade insatser skulle göra det möjligt för banker och myndigheter att mer pricksäkert identifiera scenarier och kriterier för att upptäcka relevant misstänkt aktivitet och data. Det skulle möjliggöra en snabb återkoppling på vad som fungerar bra och vad som fungerar mindre bra.

## INFORMATIONSDELNING

Trots att det råder bred enighet om att ökad informationsdelning mellan banker och myndigheter skulle leda till ett effektivare arbetssätt, råder det också enighet om vikten av att skydda och försvara den personliga integriteten.

I och med att bankanställda och andra myndighetsanställda inom samarbetsgruppen skulle erhålla en högre befogenhetsnivå behöver tydliga regler för hur informationsdelning får gå till inom medlemskapet etableras. Dessa måste rymmas inom gällande regelverk för sekretess och dataskydd som kan begränsa möjligheter för informationsdelning. Man bör dock ha för avsikt att så långt som möjligt anonymisera data för att motverka dessa hinder och värna integriteten. Avtal, ramverk och regler ska verka för att minska risken för rregelefterlevnadsbrister förknippade med samarbetet och se till att ett etiskt tillvägagångssätt används när man handskas med data. Det är samtidigt viktigt att säkra att den operativa processen blir så effektiv som möjligt. Utgångspunkten är att ingen information om individuella kunder eller enskilda fall får återföras till den egna organisationen.

Principerna och riktlinjerna för informationsdelningen inom samarbetsgruppen behöver inte bara beakta utmaningar som har att göra med gällande lagar och regler, utan även tillit mellan deltagande organisationer. Antagandet är att samlokaliseringen som föreslås i denna modell kommer att bidra till att tilliten mellan deltagande organisationer kommer att underlättas, och kontinuerligt öka med tid.



# VISION FÖR EN NY VERKSAMHETSMODELL: EN OFFENTLIG-PRIVAT SAMVERKAN MOT PENNINGTVÄTT

För att effektivt motverka penningtvätt framöver krävs att nuvarande arbetssätt och verksamhetsmodell kopplat till transaktionsmonitorering ses över. Syftet med visionen för en ny verksamhetsmodell är att öka effektiviteten i de system som finns hos banker och myndigheter för att motverka finansiell brottslighet. Detta genom att skapa förutsättningar för ett mer effektivt utredningsarbete genom centralisering av transaktionsdata, centralisering av resurser och investeringar i moderna analystekniker samt en ökad samordning av insatser mot finansiell brottslighet. Det kommer också krävas en ordentlig genomlysning av lagstiftningen för att kunna verkställa den beskrivna visionen.

En viktig utgångspunkt är att bankerna fortsatt är ansvariga för de transaktioner som sker i bankerna. Utöver bankernas viktiga roll i samarbetet och de nya processerna är det därför också viktigt att bankerna finansierar det arbete och de investeringar som föreslås ska ske i offentlig regi.

Den föreslagna verksamhetsmodellen presenteras nedan och en sammanfattning av processerna i den nya modellen finns detaljerad i Appendix II.

## DEN NYA VERKSAMHETS- MODELLEN I PRAKTIKEN

### FÖRBÄTTRAD OCH EFFEKTIVARE TRANSAKTIONSMONITORERING

I den nya verksamhetsmodellen kommer banker och andra rapporterande verksamheter fortsättningsvis övervaka kunders transaktioner och aktiviteter. Men istället för att manuellt undersöka larm och slutligen producera rapporter om misstänkt penningtvätt skulle bankerna, genom utveckling av ett automatiskt signalsystem, automatiskt skicka transaktioner som möter förutbestämda kriterier direkt till relevant utredande del av Polismyndigheten. Den utredande avdelningen inom Polismyndigheten skulle sedan aggregera all

transaktionsdata från rapporterande banker på nationell nivå. Genom användning av nya teknologiska verktyg och kapaciteter, såsom mönsterigenkänning, klustring och artificiell intelligens för att upptäcka misstänkt aktivitet mer pricksäkert, och som är anpassade för att hantera "big data", skulle den utredande avdelningen inom Polismyndighetens data-science team analysera datan aggregerat och göra kopplingar mellan transaktioner och kunder som inte tidigare har varit möjligt. Det är viktigt att den myndighet som ansvarar för den centraliserade analysen och utredningen har rätt kompetens och mandat. Exakt ansvarsfördelning bör därför utredas vidare i en fortsatt detaljering.

Användning av centraliserad och mer sofistikerad teknik i transaktionsanalysen tillsammans med annan data som inte är tillgänglig för privata aktörer (t.ex. belastningsregister och annan myndighetsdata) skulle ge förutsättningar för att producera högkvalitativa utredningar om misstänkt penningtvätt. Se vidare i Appendix III för beskrivning av den centrala analysfunktionen.

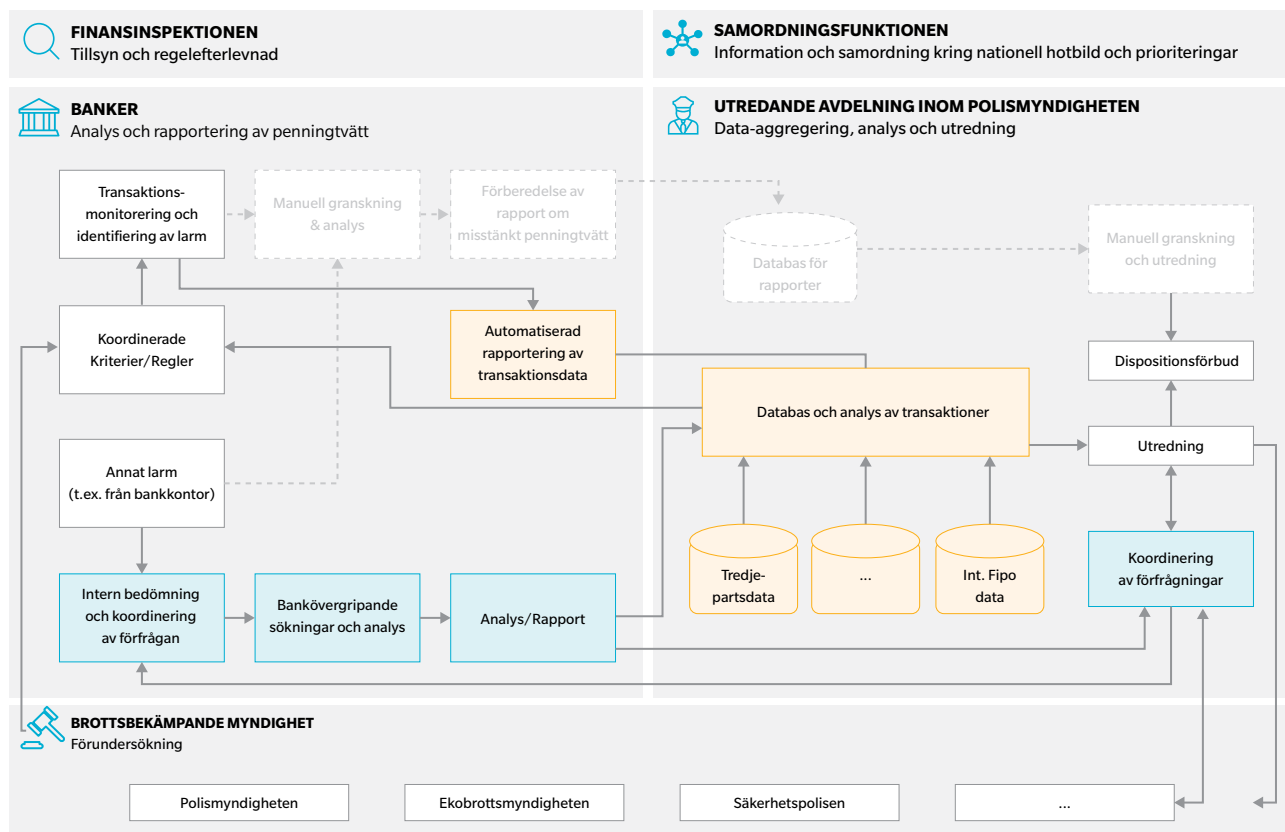
Den utökade rapporteringen kommer att möjliggöra analys av inrapporterade transaktionsdata tillsammans med andra tredjepartsdata och myndighetsdatakällor (t.ex. brottsregistret, bolagsverket, DowJones, World-Check och internationella rapporter om misstänkt penningtvätt), och på så sätt skapa en mer komplett bild än tidigare.

Den nya modellen skulle möjliggöra en betydligt snabbare hantering av misstänkta ärenden. Istället för den tunga proceduren med manuell granskning och förberedelse av rapporter om misstänkt penningtvätt, skulle analyser automatiseras och ske kontinuerligt. Ambitionen är att under samma dag, och så nära realtid som möjligt, kunna fatta informerade beslut om rapportering till relevant myndighet eller lämplig rättslig åtgärd. Den automatiserade analysen skulle även hjälpa brottsbekämpande myndigheter att fokusera sina manuella insatser på större och mer betydelsefulla utredningar.

En större mängd data till Fipo/Noa och en utökad analys skulle vidare möjliggöra en mer noggrann kalibrering av tröskelvärden, scenarios och vad som klassas som misstänkta transaktioner. Detta skulle sedan rapporteras

tillbaka till banker för justering av systeminställningar för att kontinuerligt öka relevansen av inrapporterad data.

Figur 5: Övergripande målbild för den nya verksamhetsmodellen för transaktionsmonitorering och rapportering



### Banker

- Bankintern manuell granskning och förberedelse av rapport om misstänkta transaktioner (baserad på interna regler) fasas ut
- Istället ersätts denna fas av en direktrapportering av transaktionsdata baserad på bestämda kriterier/regler
- Banker får löpande feedback på kriterier/typologier/regler baserat på den centraliserade analysen samt input från andra relevanta myndigheter och samarbetsorgan
- Andra typer av larm (från t.ex. bankkontor eller fysiskt möte) hanteras fortsatt inom banken genom en koordinerad process där syftet är att:
  - Det finns större möjlighet till återkoppling från den utredande Polismyndigheten
  - Förfrågningar och uppföljningar från myndigheter utformas mer effektivt då bland annat prioritering centraliseras hos den utredande avdelningen inom Polismyndigheten

### Utredande avdelningen inom Polismyndigheten

- En förbättrad och effektivare utredning av misstänkta fall skapas inom relevant utredande avdelning av Polismyndigheten:
  - En centralisering av transaktionsdata tillåter avancerad analys av data från alla rapporterade banker samt berikning av data från tredjepartskällor (i närapå realtid)
  - Misstänkta fall utreds, i likhet med tidigare, men prioriteras baserat på sannolikhet och omfattning/volym
- En centraliserad mekanism för förfrågningar från myndigheter skapas där den utredande avdelningen inom Polismyndigheten sammanställer och prioriterar inkomna förfrågningar, innan de skickas vidare till bankerna för datainsamling och eventuell analys

### Brottsbekämpande myndighet

- Som tidigare inleder brottsbekämpande myndigheter förundersökningar i relevanta fall
- Den koordinerade förfrågningsmekanism som skapas utgör en motpart i sina förfrågningar om ytterligare information

### Andra myndigheter

- Utökad informationsutbyte mellan den utredande avdelningen inom Polismyndigheten och FI om trender, typologier, risker, etc.
- Löpande informationsutbyte mellan Samarbetsfunktionen och den utredande avdelningen inom Polismyndigheten om den nationella riskbilden för att informera scenarier och typologier

Processnyckel:  Ny centraliserad transaktions-rapportering  Ny koordinerad förfrågning och utredning  Befintlig process  Tidigare process som på sikt ej behövs

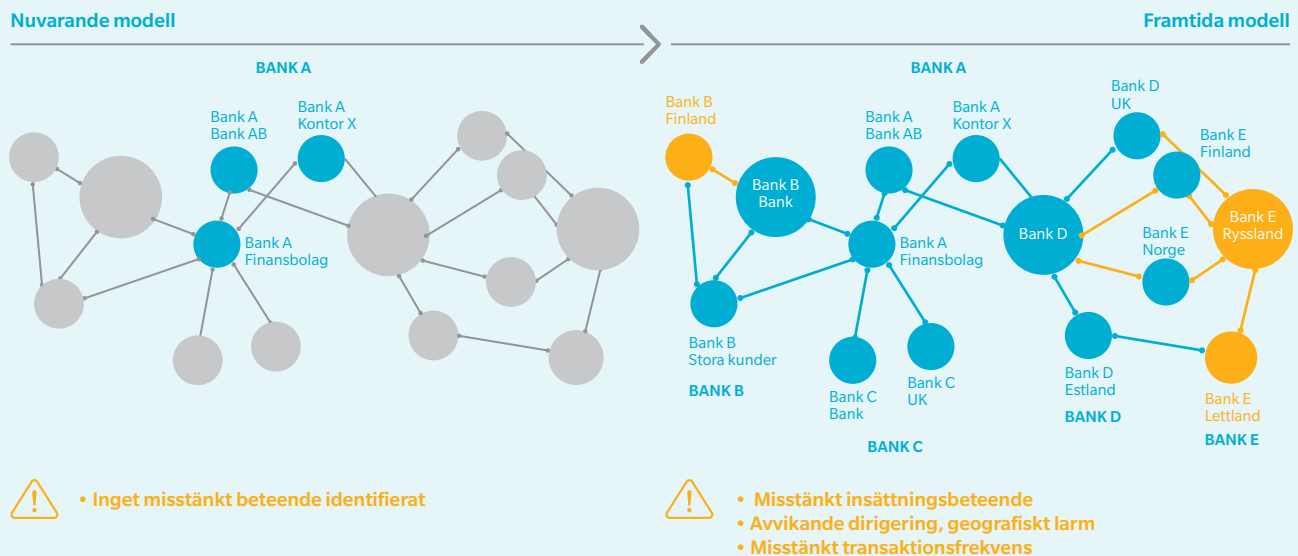
## RUTA ETT: SAMLAD TRANSAKTIONSDATA MÖJLIGGÖR EFFEKTIV IDENTIFIERING AV KOMPLEXA PENNINGTVÄTTSUPPLÄGG

Idag kan en bank endast se en begränsad del av en kunds transaktionskedja, det vill säga den del som sker inom bankkoncernen. Banken producerar därför endast rapporter om misstänkt penningtvätt i de fall då det finns tillräckligt underlag inom den enskilda banken för att ana misstanke. Eftersom Fipo endast har tillgång till dessa rapporter begränsas deras möjlighet att avslöja större och mer komplexa fall av penningtvätt.

Idag kan därför brottslingar undkomma att bli upptäckta genom att skicka runt transaktioner mellan olika banker, och dela upp och ändra transaktionsmönster. Vad som hos en enskild bank inte orsakar misstanke skulle potentiellt orsaka misstanke om hela transaktionskedjan uppenbarades.

Med den vision som presenteras kan information från olika banker och myndigheter bindas samman och mer avancerade penningtvättsupplägg kan därför identifieras.

Figur 6: Illustration av nuvarande och framtida transaktionsmonitorering



## HANTERING OCH KOORDINERING AV MANUELLT RAPPORTERADE LARM

Möjligheten till manuella larm ska finnas kvar hos de rapporterade bankerna, exempelvis när misstanke uppkommer från interaktioner med kunder på bankkontor. Dessa manuella larm kommer granskas internt och när det är relevant leda till en manuell rapportering till den centrala databasen.

## CENTRALISERAD MEKANISM FÖR FÖRFRÅGNINGAR FRÅN MYNDIGHETER

Vidare kan nuvarande arbetssätt stärkas genom ett mer strukturerat och koordinerat tillvägagångssätt för brottsbekämpande myndigheter att begära information och specifika analyser av bankerna, något som idag saknas. Genom att även centralisera förfrågningsmekanismen skulle brottsbekämpande myndigheter genom en enskild begäran/förfrågan kunna få information från en mängd rapporterade verksamheter, och på så sätt mer effektivt utveckla en omfattande underrättelsebild. Centraliseringen kommer i detta upplägg därmed spela en viktig roll i att sammanställa och prioritera inkomna förfrågningar innan de skickas vidare till rapporterade verksamheter för datainsamling och vidare analys. Underlaget från de rapporterade verksamheterna analyseras sedan innan de sedan skickas tillbaka till brottsbekämpande myndighet. Analyserna kan berikas ytterligare genom till exempel information från Samordningsfunktionen kring den nationella hotbilden och aktuella scenerier och typologier.

## YTTERLIGARE ASPEKTER PÅ SAMARBETEN INOM DEN NYA VERKSAMHETSMODELLEN

Den utökade mängden data och den förbättrade analyskapaciteten kommer förbättra möjligheten att genomföra nationell och lokal trendanalys, t.ex. hot, sårbarheter, risker per sektor/geografi, samt kunna identifiera typologier och indikatorer som hissar röd flagg och dela dessa med rapporterade verksamheter och Samordningsfunktionen.

I beskrivningen av verksamhetsmodellen ovan är det framför allt de olika brottsbekämpande myndigheterna som beskrivs. Det är dock även viktigt att till exempel FI hålls informerad för att mer effektivt kunna sköta sin tillsyn. Över tid finns det också fördelar av att inkludera andra myndigheter i samarbetet, såsom Skatteverket.

## FÖRDELARNA MED EN MER EFFEKTIV VERKSAMHETSMODELL MOT PENNINGTVÄTT

Syftet med visionen för ny verksamhetsmodell är att den kommer att förstärka skyddet mot penningtvätt och finansiering av terrorism.

Det är svårt att konkret uppskatta vilka fördelar en förändrad verksamhetsmodell mot penningtvätt skulle innebära. Trots att såväl JMLIT i Storbritannien som Fintel Alliance i Australien har visat lovande resultat från sina respektive samarbetsmodeller är det fortfarande för tidigt att avgöra kvantitativt hur stora effekterna har blivit, och framför allt kommer att bli. Nedan sammanfattas kvalitativt de fördelar som den nya verksamhetsmodellen kan komma att bidra till.



### **Minska brottslighet genom ett mer effektivt sätt att upptäcka och förebygga penningtvätt.**

Genom den ökade informationsdelningen och de avancerade analysmetoderna kommer den nya modellen möjliggöra effektivare brottsbekämpande åtgärder. Detta informationsövertag gentemot kriminella aktörer kan över tid leda till en lägre brottslighet.



### **Bevara integriteten i det svenska finansiella systemet.**

Ett starkare system för att motverka penningtvätt ökar attraktionskraften för det svenska finansiella systemet genom den minskade risken för penningtvätt och bättre mekanismer för att förhindra olagliga finansiella flöden.



### **Främja ett bättre privat-offentligt samarbete.**

Förbättrad dialog med den privata sektorn genom feedback och vägledning gör det möjligt för den privata sektorn att lära av den offentliga sektorn, och tvärtom. Organisationen som skapas för ökad samverkan kan också, med fördel, utvidgas till andra områden över tid, såsom till exempel cyberrisk eller annan typ av bedrägeri.



### **Minskad regulatorisk risk och konsekvent hantering av penningtvätt.**

Den föreslagna verksamhetsmodellen innebär en standardiserad rapportering från banker. De typologier som används kommer utvärderas för systemet som helhet och sedan återkopplas till bankerna. Denna standardisering kommer leda till att beroendet av bankens egna processer minskar och arbetet kommer därför bli mindre utsatt för eventuella brister hos enskilda banker.



### **Bankernas bidrag till ett effektivare anti-penningtvättsarbete minskar deras risk för sanktioner och ryktesmässiga konsekvenser.**

Banker är fortsatt ansvariga för det arbete som de gör kring penningtvätt. Om en bank har bristfälliga processer för att hantera penningtvätt står de därför en risk, både för regelmässiga brott (som kan leda till sanktioner) och för kritiska ryktesmässiga konsekvenser. Ett mer effektivt arbete mot penningtvätt kommer därför minska denna risk.



### **Ökad effektivitet av utredningar och operationell effektivitet.**

Med den nya verksamhetsmodellen kommer mindre tid spenderas på att granska fall som inte leder till något rättslig åtgärd. Minimerad manuell hantering ger också en möjlighet att omfördela resurser till aktiviteter som är mer värdeskapande i arbetet att motverka penningtvätt. Även om den nya modellen på kort sikt kommer leda till ökade kostnader, så kommer den effektivitet som systemet skapar över tid leda till att kostnadstillväxten som nu är kraftig, kan minska.

## RUTA TVÅ: EN NY VERKSAMHETSMODELLEN KAN ÖKA DEN OPERATIONELLA EFFEKTIVITETEN I ARBETET MOT PENNINGTVÄTT

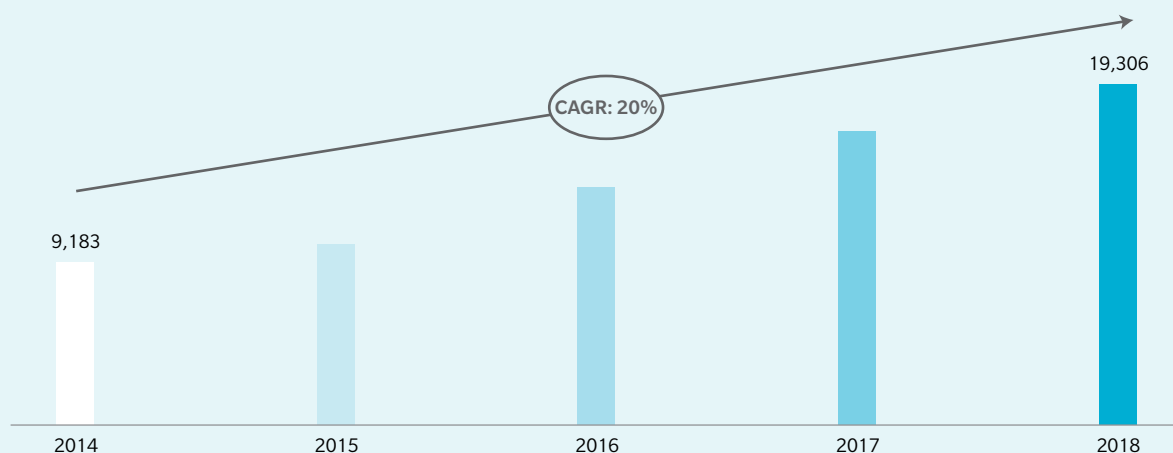
Svenska banker har under de senaste åren anställt allt fler för att hantera den ökande mängden rapporter av misstänkta transaktioner till Fipo. Under de senaste fem åren har rapporteringen av misstänkta transaktioner i Sverige ökat med en genomsnittlig årlig tillväxt på ca 20 procent (se figuren nedan). Mycket tyder på att om arbetet fortsätter som nu så kommer allt fler rapporter behöva utredas och antalet anställda i dessa funktioner fortsätta att öka.

Eftersom den långsiktiga samarbetsmodellen baseras på automatiserad transaktionsrapportering, analys och utredning, kommer det nuvarande manuella arbetet med att granska olika nivåer av larm och genomföra utredningar på sikt kunna fasas ut. Därmed kommer personalbehovet inom transaktionsmonitorering på sikt inte behöva fortsätta växa i linje med rapporterade, misstänkta fall. Den nya modellen kommer därför att kunna leda till påtagliga kostnadsbesparingar för systemet som helhet i framtiden.

Syftet med den reviderade verksamhetsmodellen är emellertid inte främst att driftskostnaderna ska sänkas, utan snarare att systemets effektivitet i att motverka penningtvätt och finansiell brottslighet förbättras.

Figur 7: Rapporteringstillväxten i Sverige, 2014-2018

Antal rapporter



Källa: Finanspolisen

## UTMANINGAR SOM MÅSTE SES ÖVER INFÖR DEN NYA VERKSAMHETSMODELLEN

Det finns flera utmaningar med att införa ett nytt arbetssätt, inte minst legala. Det är nödvändigt att dessa utmaningar ses över i samband med detaljeringen och implementeringen av en ny verksamhetsmodell. Som redan presenterats finns det åtgärder som kan göras på kort sikt som inte är exponerade mot samma utmaningar och som kommer kunna hjälpa till att bana väg för den långsiktiga lösningen.

En mer djupgående juridisk utredning kommer att krävas för det föreslagna systemet, och behöver vägas mot den samhällsnytta som förväntas. Skydd av data och personuppgifter och försvar av personlig integritet är av vital betydelse i Sverige. Det krävs därmed en balansgång mellan ett effektivare arbete mot penningtvätt och skydd av den personliga integriteten. Nedan beskrivs några av de områden som måste ses över.



## LEGALA UTMANINGAR

RISKOMRÅDE	BESKRIVNING OCH EXEMPEL
<b>Delning av information</b>	Lagar om sekretess och personlig integritet, som till exempel GDPR, begränsar möjligheter för informationsdelning. <sup>9</sup> För banker som vill förbättra informationsdelning i syfte att motverka penningtvätt, skapas det en problematisk balansgång (med höga potentiella böter vid överträdelse av båda). <sup>10</sup> Det krävs därmed en "safe harbour" för att underlätta denna process, exempelvis en "information sharing gateway" som har upprättats av NCA under JMLIT. <sup>10</sup> Relevant utredande avdelning inom Polismyndigheten skulle behöva spela en liknande roll i det svenska systemet. Detta måste dock utvärderas juridiskt
<b>Delning av transaktionsdata utan tydlig misstankegrad</b>	Det föreslagna systemet bygger på att transaktionsdata över vissa tröskelvärden eller som möter vissa bestämda kriterier, automatiskt skickas till relevant utredande avdelning inom Polismyndigheten, med endast begränsad manuell granskning innan delning. För att en effektiv analys ska kunna göras krävs därför att en större mängd transaktioner skickas, vilket kräver att dessa tröskelvärden troligtvis behöver vara relativt generiska. Detta betyder att de transaktioner som kommer skickas inte kommer ha samma misstankegrad som de fall som idag skickas till Fipo. Det kan tolkas som en ansvarsförflyttning från bankerna till Polismyndigheten för bedömning av potentiella överträdelse, vilket kan anses vara i strid mot gällande lagstiftning.
<b>Centralt person- och transaktionsregister hos relevant utredande Polismyndighet</b>	Ett centralt register för kunder och transaktioner kommer krävas hos relevant utredande avdelning inom Polismyndigheten, och detta register kommer även behöva en viss historik innan det rensas för att kunna identifiera penningtvätt över tid. Eftersom skälig misstanke inte alltid kommer föreligga väcker det frågor kring GDPR och banksekretessen. En utredning kommer krävas rörandes hur detta system kan hanteras legalt.

## BANKINTERNA UTMANINGAR

RISKOMRÅDE	BESKRIVNING OCH EXEMPEL
<b>Riskbedömning</b>	Den transaktionsmonitorering och analys som sker idag används också vidare i den löpande riskbedömningen av bankernas kunder. När delar av detta flyttas till Polismyndigheten krävs det någon form av återkoppling tillbaka till bankerna. Detta kan även ha legala konsekvenser som bör utredas.
<b>Implementering av system för informationsdelning</b>	Bankernas infrastruktur och IT-plattformar skiljer sig väsentligt åt, och det kommer därmed finnas en varierande grad av utmaning för att säkra det systemstöd som krävs för partnerskapet, vilket troligen kommer att vara både resurs- och tidskrävande för bankerna. Detta gäller exempelvis leveransen av kvalitativa data, utvecklandet av sofistikerade algoritmer för att identifiera misstänkt aktivitet, samt centralisering av kundkännedomdata. Riskaptit och risknivå mellan banker skiljer sig även åt, vilket kan innebära inkonsekvent data. Slutligen behöver de algoritmer som utvecklas på banksidan vara dynamiska så att de kontinuerligt kan uppdateras efter feedback ifrån relevant utredande avdelning inom Polismyndigheten

## FINANSIERING OCH SAMARBETE

RISKOMRÅDE	BESKRIVNING OCH EXEMPEL
<b>Investeringskostnad</b>	Implementeringen av visionen för verksamhetsmodell innebär en betydande investering. Utgångspunkten är att denna finansiering kommer att ske av bankerna. Kostnaderna drivs dels av den projektledningsorganisation som krävs för att designa och upprätta en ny verksamhetsmodell men också av den IT-infrastruktur som måste byggas ut, integreras och utvecklas. En tydlig modell behöver etableras för kostnadsfördelning sinsemellan de privata aktörer som kommer finansiera investeringen.
<b>Löpande finansiering och resurssättning</b>	De löpande kostnaderna, efter implementering, inom den myndighet som bestäms sköta driften kommer att öka som ett resultat av det behov som finns för underhåll och löpande analys. Utgångspunkten är att även detta finansieras av bankerna, på ett likande sätt som till exempel tillsynsmyndigheter idag finansieras av instituten under deras tillsyn. Givet att det fortfarande kvarstår att detaljera designen av den långsiktiga lösningen är det i nuläget svårt att göra en relevant uppskattning av denna ökade driftskostnad.
<b>Hantering av komplexa beroenden och projektstyrning</b>	Implementeringen av denna modell kommer att vara mycket komplex, på grund av exempelvis de många olika involverade parterna (banker, myndigheter, departement), kraven på IT och system. Tre faktorer är därför särskilt viktiga: transparens och balans mellan incitament, utformning av en tydlig kommunikationsstrategi, samt effektiv styrning och övervakning. För att uppnå de eftersträfvade förbättringarna i systemet på lång sikt krävs det att motiv och incitament mellan intressenter klargörs samt att en långsiktig finansieringsplan etableras.

9. Anti-money laundering and counter-terrorist financing measures: Sweden, FATF, April 2017

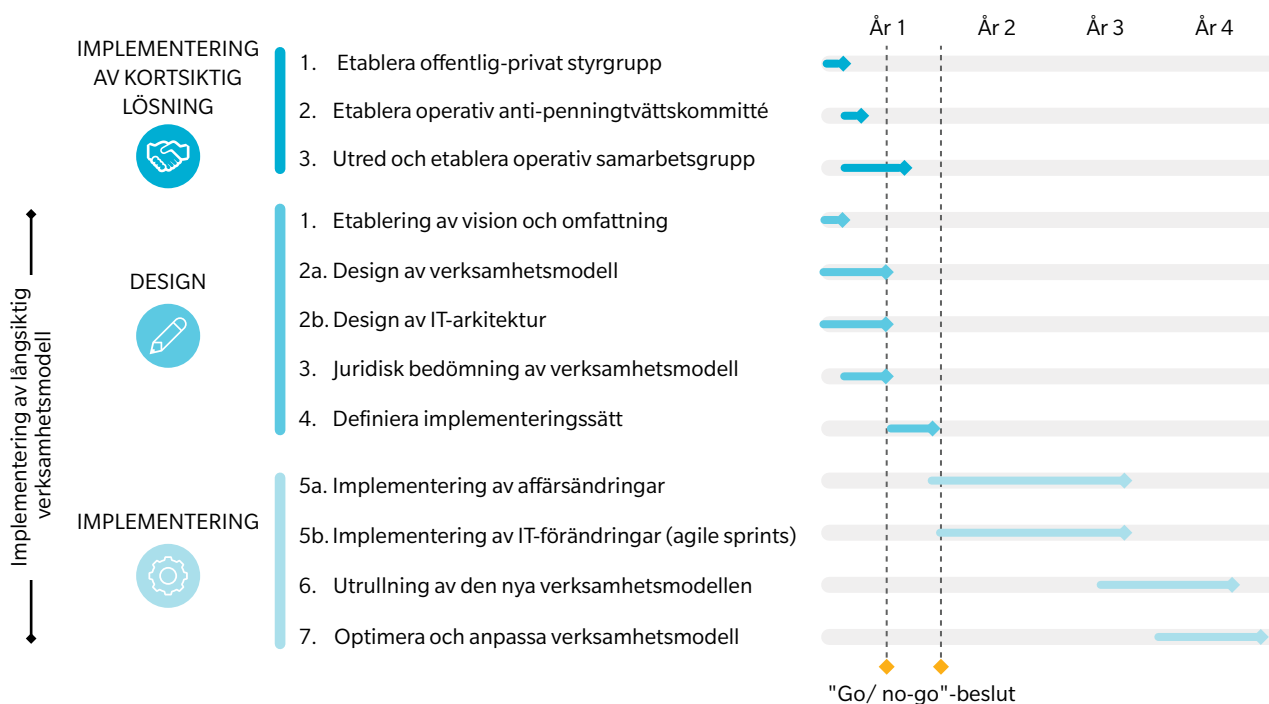
10. White & Case

# TIDSLINJE OCH IMPLEMENTERINGSPLAN

Implementeringen av den långsiktiga verksamhetsmodellen förväntas ta fyra till fem år. För att på kortare sikt kunna förbättra det arbete som görs kring penningtvätt finns det därför anledning att skapa en samarbetsmodell som verkar för att bättre samordna arbetet fram tills effekterna av den nya verksamhetsmodellen har realiserats. Parallellt med arbetet med den långsiktiga modellen föreslås därför att den föreslagna samarbetsorganisationen sätts upp, som redan inom ett år kan leverera förbättringar.

Det långsiktiga programmet kommer att fortskrida genom sekvenserade faser som visas i figuren nedan och kommer att leverera ett system som är mer effektivt och lättare att använda för såväl banker som myndigheter. Detta arbete kommer detaljeras i en initial designfas för att sedan fokusera på utveckling och implementering. En mer detaljerad beskrivning av de aktiviteter som bör ske är presenterade i Appendix.

Figur 8: Övergripande tidslinje för implementering (illustrativ)



# APPENDIX I: DET SVENSKA ANTI-PENNINGTVÄTTSARBETET

Det svenska regelverket avseende penningtvätt och finansiering av terrorism inbegriper straffrättsliga såväl som administrativa inslag för åtgärder, motverkan och förhindrande av penningtvätt och terrorfinansiering.

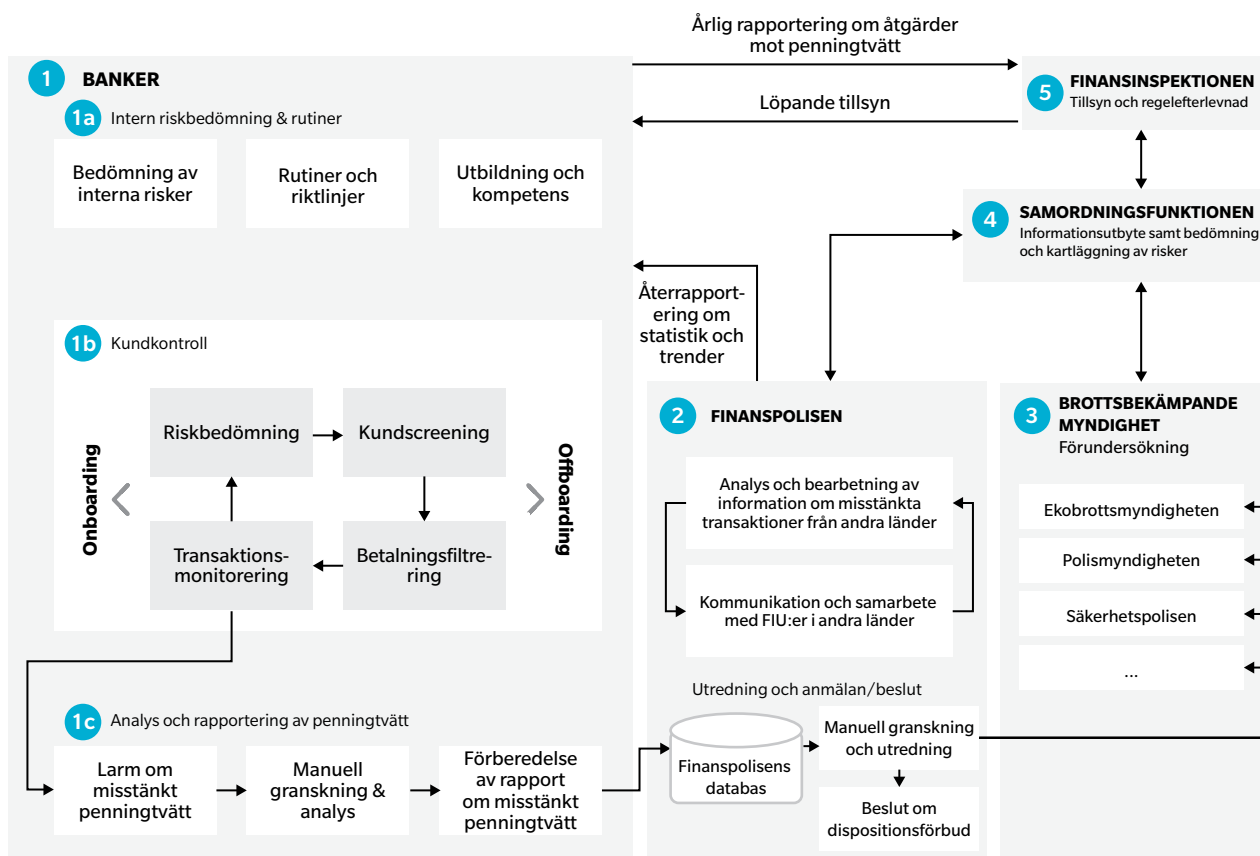
Ekosystemet består övergripande av

- **Regeringen:** ansvarar för att genomföra riksdagens beslut och att implementera internationella standarder i det svenska systemet
- **Myndigheter och samarbetande organisationer:** utgörs av de myndigheter som arbetar med åtgärder mot penningtvätt samt advokatsamfundet. Myndigheterna delas upp i tillsynsmyndigheter och brottsbekämpande myndigheter.

- FI, Lotteriinspektionen och Revisorsnämnden är exempel på myndigheter som bedriver tillsyn över att penningtvättsregler efterlevs inom specifika branscher. Brottsbekämpande myndigheter inkluderar i sin tur Polismyndigheten, Åklagarmyndigheten och Ekobrottsmyndigheten vilka arbetar med bland annat förundersökning och åtal av penningtvättsbrott.
- **Verksamhetsutövare:** inkluderar samtliga företag som inbegrips av penningtvättslagen, exempelvis banker, spelverksamhet och fastighetsmäklari.

Nedan beskrivs några av de parter som huvudsakligen är involverade i arbetet kring transaktionsmonitorering.

Figur 9: Övergripande illustration av det nuvarande arbetet mot penningtvätt



## 1 BANKER

Bankernas roll i arbetet mot penningtvätt delas in i tre övergripande delar: A. Riskbedömning och rutiner, B. Kundkontroll samt C. Rapportering och granskning.

### A. Intern riskbedömning och rutiner

**Bedömning av interna risker:** Banker måste utföra en bedömning av riskerna för att verksamheten kan komma att utnyttjas för penningtvätt. Riskbedömningen ska ta hänsyn till faktorer såsom bankens storlek, bankens kunder och distributionskanaler, produkter och tjänster som tillhandahålls, samt geografiska riskfaktorer. Banken ska även ta hänsyn till information som härstammar från misstänkt aktivitet och återkoppling från myndigheter. För att riskbedömningen ska hållas aktuell krävs det att den dokumenteras och uppdateras löpande.

**Säkerställande av rutiner och riktlinjer:** Baserat på riskbedömningen och gällande regelkrav ska banker utforma dokumenterade rutiner och riktlinjer för åtgärder inom kundkännedom, övervakning samt behandling av personuppgifter. Dessa ska kontinuerligt uppdateras och anpassas för att åtgärda brister till följd av nya och förändrade risker avseende penningtvätt. Det krävs även att banken upprättar särskilda funktioner för intern kontroll. Detta inkluderar bland annat en särskild befattningshavare med ansvar för uppdatering av den allmänna riskbedömningen samt upprättande av en oberoende granskningsfunktion med uppgift att granska och utvärdera effektiviteten i exempelvis riskhantering.

**Utbildning och kompetens:** Anställda, uppdragstagare och andra som deltar i verksamheten måste ha tillräcklig utbildning och kunskap för att kunna följa bankens uppsatta rutiner och riktlinjer. Banken behöver därför se till att de som utför arbetsuppgifter av betydelse för att förhindra penningtvätt fortlöpande får utbildning. Utbildningen ska utöver fakta även ge personalen information kring nyheter och trender avseende penningtvätt.

### B. Kundkontroll

#### **Inledande av kundrelation och riskbedömning av kund:**

I inledningen av en affärsrelation har banken i uppgift att identifiera kunden och anknutna personer så som verklig huvudman, förmånstagare eller juridiska representanter. Dessa identiteter ska därefter verifieras genom kontroll mot oberoende och pålitliga källor. Banken måste även kontrollera affärsrelationens syfte och natur. Baserat på informationen som insamlats och kontroller som gjorts görs en riskbedömning av kunden vilken resulterar i en riskklassificering där nivåerna betecknas låg, medel eller hög. I de fall kunden bedöms utgöra en hög risk behöver banken utföra en utökad kundkontroll, eller så kallad "enhanced due diligence" (EDD). EDD inkluderar bland annat ytterligare kontroll av verklig huvudman bakom ett företag.

#### **Löpande bedömning av kund (periodvis och händelsedrivnen):**

All information från den inledande processen och kundscreeningen dokumenteras och utgör grunden för löpande kontroll av kundens aktivitet hos banken. Exempelvis måste kundens engagemang och riskklassificering följas upp om uppdateringar av sanktionslistor eller dylikt ger utslag när affärsrelationen redan inletts.

#### **Kundscreening (Sanktioner och PEP):**

Kundens, förmånstagares och andra anknutna personers identiteter kontrolleras mot sanktionslistor, register över politiskt utsatta personer och andra bevakningslistor. Detta då dessa typer av kunder bedöms utgöra en förhöjd risk för att banken kan utnyttjas för penningtvätt. I de fall som kundens eller anknutna personers namn matchar med register och listor utreds och bedöms risker och konsekvenser för att avgöra om banken överhuvudtaget kan ingå affärsrelationen. Karaktäristika som automatiskt kan resultera i en hög riskklassificering är bland annat kunder som är registrerade som politiskt utsatta, har en koppling till högriskländer eller som har till synes ogrundat komplexa företagsstrukturer.

**Betalningsfiltrering:** Banken övervakar betalningar till och från kundens konto som filtreras mot lokala och internationella sanktionslistor och register över politiskt utsatta personer.

Betalningsfiltrering görs innan en transaktion genomförs för att förhindra illegala transaktioner medan transaktionsövervakning sker kontinuerligt av samtliga transaktioner.

**Transaktionsmonitorering:** Banken utför löpande övervakning av kunders aktivitet för att identifiera misstänkta transaktioner. Banken övervakar transaktioner i syfte att identifiera avvikelser från det förväntade beteendet eller andra anledningar som ger skäl till misstanke om penningtvätt. Kundens förväntade aktivitet baseras på den förståelse för kunden som anskaffats under onboardingprocessen. I de fall kunden utför en transaktion som kan förknippas med hög risk måste banken vidta skärpta åtgärder för kundkännedom. Huvudsakliga orsaker till misstanke som anges av bankerna är till exempel upprepade eller stora överföringar till ett specifikt konto, ovanliga eller avvikande transaktioner och stora eller upprepade utlandsbetalningar.

**Avslutande av kundengagemang:** I de fall banken inte kan kontrollera identiteten på kunden eller den verkliga huvudmannen, få tag i information kring affärsrelationens syfte och natur eller att andra kriterier i processen för kundkännedom inte uppfylls ska affären nekas. Banken kan även välja att avsluta kundens engagemang i de fall kunden inte kan besvara frågor kring exempelvis misstänkta transaktioner.

### C. Rapportering och granskning

När avvikelser identifieras av banken och inte kan förklaras efter vidare granskning upprättas en rapport om misstänkt penningtvätt som inkluderar den misstänkta transaktionen, orsak till misstanke, uppgifter om omständigheter samt potentiellt ytterligare underlag. Rapporten skickas därefter till Fipo för analys och beslut om vidare åtgärd.

## 2 FINANSPOLISEN (FIPO)

Fipo är Sveriges Financial Intelligence Unit (FIU). I denna roll ingår bland annat att ta emot, registrera, bearbeta och analysera rapporter om misstänkta transaktioner som bankerna skickar in. I de fall Fipo misstänker penningtvätt upprättas en brottsanmälan. Brottsanmälan och informationen skickas sedan vidare till berörd brottsbekämpande myndighet, till exempel andra delar inom Polismyndigheten, Ekobrottsmyndigheten eller Säkerhetspolisen, som då inleder en förundersökning. Fipo kan även besluta om dispositionsförbud av konton som är under misstanke. Dispositionsförbud gäller i max två dagar i avvaktan på att åklagare kan besluta om penningbeslag eller annan åtgärd.

Fipo ansvarar även för att återkoppla kontinuerligt till verksamhetsutövare och myndigheter. Återkopplingen inkluderar modus och trender för penningtvättshantering och har till syfte att sprida kunskap till övriga parter i ekosystemet. Information och statistik skickas även till tillsynsorgan som FI.

## 3 BROTTSBEKÄMPANDE MYNDIGHETER

De brottsbekämpande myndigheterna är de myndigheter som utreder brottsmisstankar genom förundersökningar och i förlängningen sköter lagföringar när det är möjligt. De har också egen underrättelse- och utredningsverksamhet. Exempel på myndigheter är Ekobrottsmyndigheten, Polismyndigheten och Säkerhetspolisen.

#### 4 SAMORDNINGSFUNKTIONEN

Utöver Fipo leder även Polismyndigheten en nationell Samordningsfunktion för åtgärder mot penningtvätt och terrorismfinansiering. Samordningsfunktionen består av diverse myndigheter och advokatsamfundet och har som uppdrag att främja informationsutbytet mellan de deltagande organisationerna, bedöma och kartlägga aktuella risker i systemet samt ge information till verksamhetsutövare för att bidra till deras interna riskbedömning, riskklassificering och rapportering av misstänkt aktivitet. Totalt ingår 17 organisationer i samarbetet, varav några är Ekobrottsmyndigheten, Skatteverket och FI.<sup>11</sup>

#### 5 FINANSINSPEKTIONEN

Finansinspektionen är den myndighet som har tillsyn över de finansiella företag som omfattas av penningtvättslagen. Myndigheten arbetar för att förebygga att dessa företag utnyttjas för penningtvätt men ska även se till att företag som står under tillsyn följer reglerna, samt att de kontinuerligt utvecklar och förbättrar arbetet mot penningtvätt. Samtliga företag som omfattas av penningtvättslagstiftningen och står under tillsyn av FI ska utöva årlig rapportering.

#### ANDRA MYNDIGHETER

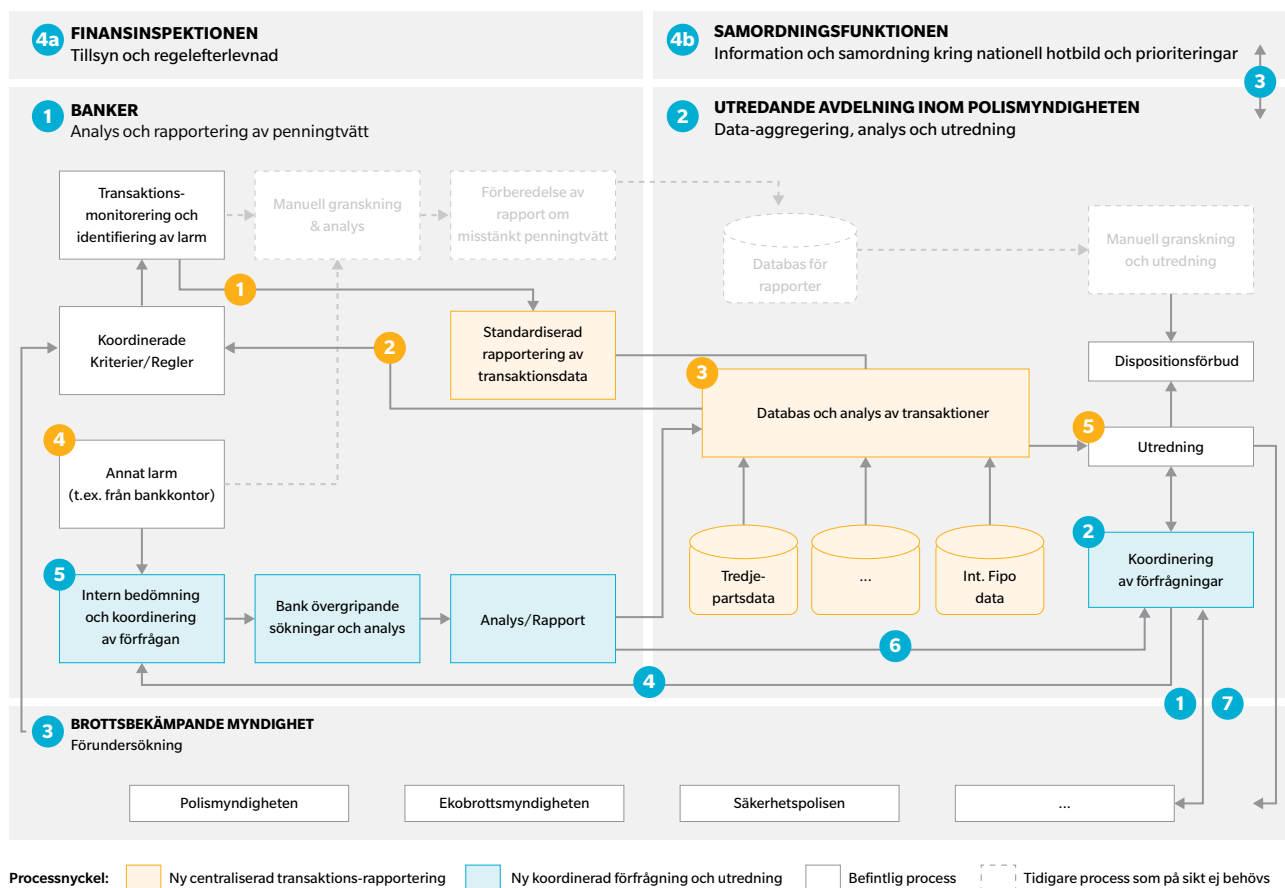
Det finns andra myndigheter som arbetar med bekämpning av och förebyggande arbete mot penningtvätt. En viktig sådan myndighet är Skatteverket, som har i uppdrag att utreda, förhindra och förebygga ekonomisk brottslighet inom skatteområdet i linje med Skattebrottslagen. Verksamheten som bedrivs inkluderar därmed både brottsutredningar (på uppdrag av t.ex. Ekobrottsmyndigheten eller Åklagarmyndigheten) och underrättelseverksamhet. Skatteverket spelar därför en central roll i arbetet mot finansiell brottslighet och samarbetar med Polismyndigheten (som till exempel Fipo).

11. De organisationer och myndigheter som ingår i Samordningsfunktionen är Bolagsverket, Brottsförebyggande rådet, Ekobrottsmyndigheten, Fastighetsmäklarinspektionen, Finansinspektionen, Kronofogdemyndigheten, Länsstyrelsen i Stockholm, Länsstyrelsen i Västra Götaland, Länsstyrelsen i Skåne, Polismyndigheten, Revisorsinspektionen, Skatteverket, Spelinspektionen, Sveriges advokatsamfund, Säkerhetspolisen, Tullverket och Åklagarmyndigheten

# APPENDIX II: PROCESSERNA I DEN LÅNGSIKTIGA VERKSAMHETSMODELLEN

De huvudsakliga delarna i en ny verksamhetsmodell består av automatiserad transaktionsrapportering men också den koordinerade granskningen och uppgiftsfördelningen. I figuren nedan beskrivs arbetsfördelningen mellan banker, relevant utredande avdelning inom Polismyndigheten och brottsbekämpande myndigheter.

Figur 10: Ny verksamhetsmodell; transaktionsrapportering och analys samt koordinerad förfrågning/ uppgiftsfördelning





### Automatiserad transaktionsrapportering och analys

Processen för automatisk transaktionsrapportering till utredande avdelning inom Polismyndigheten av "misstänkta" transaktioner och analys av dessa:

- 1 Transaktioner som möter bestämda kriterier kommer automatiskt att skickas till en databas via en säker filöverföring/API
- 2 Kriterierna och reglerna för automatisk rapportering kommer att kalibreras löpande baserat på feedback från Polisen och andra myndigheter
- 3 Den rena transaktionsdata som rapporteras kommer aggregeras och analyseras (se Appendix IV för detaljerad beskrivning av det centrala analyslagret)
- 4 Misstanke som uppstår vid ett fysiskt möte med en kund, till exempel på ett bankkontor eller i andra situationer utanför det löpande flödet av transaktionsdata, kommer att granskas och analyseras internt för manuell rapportering till utredande avdelning inom Polismyndigheten
- 5 Högkvalitativa utredningar baserat på inkomna data och genomförd automatisk analys kommer att ske och prioriteras utifrån bestämda kriterier (t.ex. konfidens och volym). Vid bekräftad/utökad misstanke skickas utredningsunderlaget till relevant brottsbekämpande myndighet

Det finns också en möjlighet att skapa lösningar för hur det ökade, anonymiserade informationsunderlaget kan nyttjas för att förbättra det analysarbete som sker inom banker såväl som tillsynsmyndigheter. Det skulle därför kunna utredas vad för typ av automatiserad rapportering och/eller självbetjäningssystem som bör och kan sättas upp.

### Koordinerad förfrågning och uppgiftsfördelning

Processen för en centraliserad förfrågningsmekanism från brottsbekämpande myndigheter för vidare analys:

- 1 Brottsbekämpande myndigheter framställer förfrågningar för prioriterade områden/utredningar som kräver ytterligare information
- 2 Utredande avdelning inom Polismyndigheten sammanställer, omarbetar och prioriterar de inkomna förfrågningarna
- 3 Information kring nationell hotbild, trender och typologier som utarbetats av Samordningsfunktionen granskas och integreras i underlaget
- 4 Förfrågningarna omarbetas till konkreta arbetsuppgifter som fördelas till banker för intern analys
- 5 Förfrågan verkställs av banker genom att utsedda specialister inom banken genomför bankövergripande genomsökningar och analyser baserat på inkomna förfrågningar
- 6 Analyser (inklusive transaktioner eller aktivitet av intresse) skickas från bankerna till utredande avdelning inom Polismyndigheten
- 7 Underlaget analyseras, relevanta kompletterande analyser görs och rapporteras sedan tillbaka till brottsbekämpande myndigheter

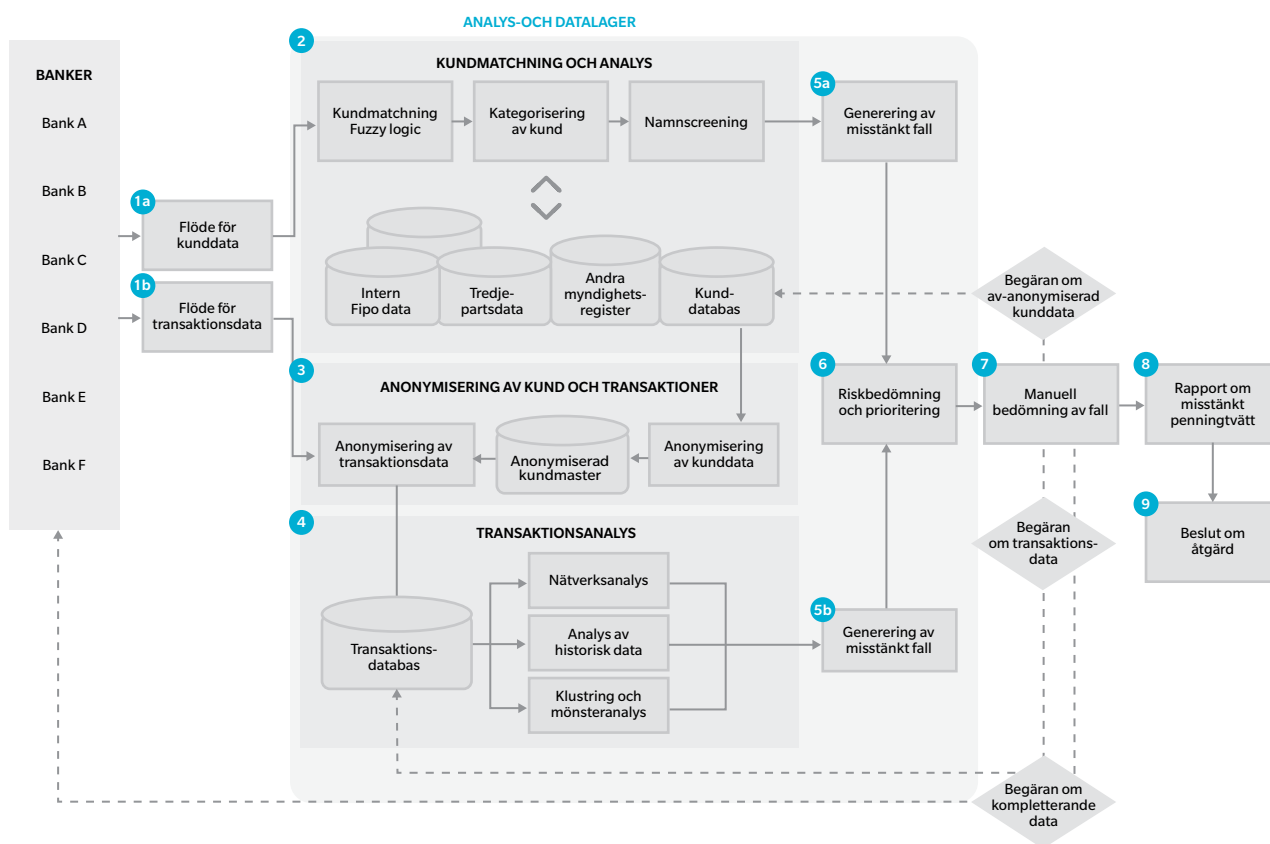
## APPENDIX III: CENTRAL ANALYSKAPACITET OCH DATABAS

I detta appendix beskrivs en hypotes kring hur den centrala analysen och databashanteringens skulle kunna se ut i den nya verksamheten och hur utökad samverkan och informationsdelning möjliggör en bredare och bättre analysförmåga. Denna hypotes måste dock vidareutvecklas och anpassas som en del i det framtida arbetet med detaljering av verksamhetsmodellen. Det bör också uppmärksammas att hur analysen och datalagret kan utformas är beroende av det legala ramverk man måste förhålla sig till.

Den utökade analyskapaciteten kommer att bestå av transaktionsanalys och kundanalys och kommer att

kontinuerligt berikas med data från andra källor och historiskt inrapporterade data. Det kommer finnas tydliga riktlinjer och regler kring hanteringen av data för att kunna försäkra att en etisk hantering av data sker. Dessutom kommer till exempel anonymisering av data ske och alla analyser ske på en anonym basis; bara när misstanke är fastställd tillåts identifiering av kunden. Efter vederbörlig analys i analyslagret kommer misstänkta fall av penningtvätt genereras och tilldelas en risk-klassificering och prioritering. Baserat på prioritering och risknivå fattas beslut om vidare åtgärd.

Figur 11: Övergripande hypotes, central analysmodell



## 1 FLÖDE FÖR KUND- OCH TRANSAKTIONSDATA

Transaktioner som möter fastställda kriterier skickas dagligen enligt ett förutbestämt och standardiserat format från bankerna. Filöverföringen tas emot och transaktionsdata separeras från kunddata innan vidare granskning och analys genomförs.

För att en central analyskapacitet och data skall tillföra en faktiskt förbättrad möjlighet att identifiera brott måste bredare data rörande transaktioner skickas in centralt än enbart sådan som redan har väckt en misstanke hos respektive bank. Grundtanken är att transaktioner som varje enskild bank och aktör inte ser ett problem med, kan visa sig vara misstänkta sett i ett större sammanhang. Noggranna och precisa kriterier för vilka transaktioner som skall analyseras centralt behövs tas fram där nyttan och integritetsaspekter vägs mot varandra.

Det är centralt för analysen att rapporterad data är kvalitetssäkrad och korrekt. Respektive rapporterande bank kommer att behöva genomföra ett omsorgsfullt datahanterings- och kvalitetsarbete för att säkerställa att transaktionsdata som skickas är komplett och möter uppsatta kriterier. Bankerna måste också säkerställa att deras tekniska infrastruktur är anpassad för att kunna automatisera repetitiva och tidskrävande processer såsom insamling, hantering och analys av data.

## 2 KUNDMATCHNING OCH ANALYS

I analyslagret för kunddata matchas kunder med varandra och kategoriseras. Namn screenas mot ett antal externa och interna databaser och register och lagras i en kunddatabas hos relevant utredande avdelning inom Polismyndigheten över verkliga huvudmän och annan kunddata. Kunddata anonymiseras sedan och lagras i en kundmaster.

### KUNDMATCHNING

För att skapa en mer komplett bild av transaktionskedjor mellan banker kommer möjligheten att matcha unika kunders identitet vara avgörande, det vill säga den verkliga huvudmannen. Den inrapporterade

kundidentiteten för en specifik kund i transaktionsdata kommer inte alltid vara identisk mellan banker och andra källor eller register. Samma kund kan till exempel stavas olika eller förkortas på olika sätt mellan olika banker och register. För att möjliggöra matchning av samma kund mellan dessa källor krävs att en metod som "fuzzy logic" används. Fuzzy logic är en algoritmisk metod som används för att upptäcka och utvärdera nära matchningar, och har potential att både effektivisera matchningsprocessen och göra mer precisa matchningar. Lösningen kommer dels att behöva stödja manuell verifiering av matchade kunder dels att stödja möjligheten att jobba med sannolikheter att två entiteter representerar samma fysiska eller juridiska person.

### KATEGORISERING AV KUND

Nya kunder kommer att kategoriseras utifrån ett antal bestämda kriterier, såsom privatperson/företag, typ av företag, ålder, transaktionsmönster etc. Kunder som redan finns i databasen kommer kontinuerligt att kategoriseras om baserat på förändringar från den ursprungliga kategoriseringen. Kategoriseringen kommer möjliggöra specifika sökningar efter avvikelser, klusteranalyser och skapa en bättre förståelse för större segment av kunder.

### NAMNSCREENING

Kunder som rapporteras in kommer att screenas centralt mot olika listor och register (till den mån det legalt är möjligt). Detta inkluderar till exempel sanktionslistor, intern Fipo-data, andra myndighetsregister (såsom belastningsregistret och spaningsregistret) såväl som information från Skatteverket, Bolagsverket och annan relevant tredjepartsinformation. Syftet är att genom denna kontroll fastställa om misstankegraden ökar och om vidare granskning och utredning krävs.

För att hantera och analysera den stora mängden ostrukturerad data som finns tillgängligt internt och externt behövs algoritmer för att mer effektivt dra slutsatser och identifiera användbara datapunkter från till exempel texttunga källor. Applicering av "natural language processing" eller datadriven språkbearbetning, som möjliggör för datorer

att tolka, förstå och manipulera texter, inom transaktionsmonitorering bör användas för att bearbeta ostrukturerad data och ytterligare berika analysen.

Den centrala kunddatabasen skulle successivt byggas upp och förädlas vartefter mer data flödar in till analyshubben. Databasen skulle vidare innehålla kända kopplingar till verkliga huvudmän och löpande genomföra riskbedömningar av kunderna, baserat på förutbestämda kriterier.

### 3 ANONYMISERING AV KUND OCH TRANSAKTIONER

Kunddata skulle sedan anonymiseras och lagras i en central kundmaster. En funktion för att anonymisera kundens identitet och kategorisera annan beskrivande information skulle säkerställa att transaktionsanalys kan genomföras utan att den verkliga identiteten hos kunden är känd eller kan härledas. Beständig nätverksanalys etc. kan fortfarande genomföras via så kallade pseudo-identiteter.

Vid misstanke och beslut enligt lämpligt regelverk skulle den verkliga personen eller juridiska personerna bli tillgängliga för brottsutredande personal.

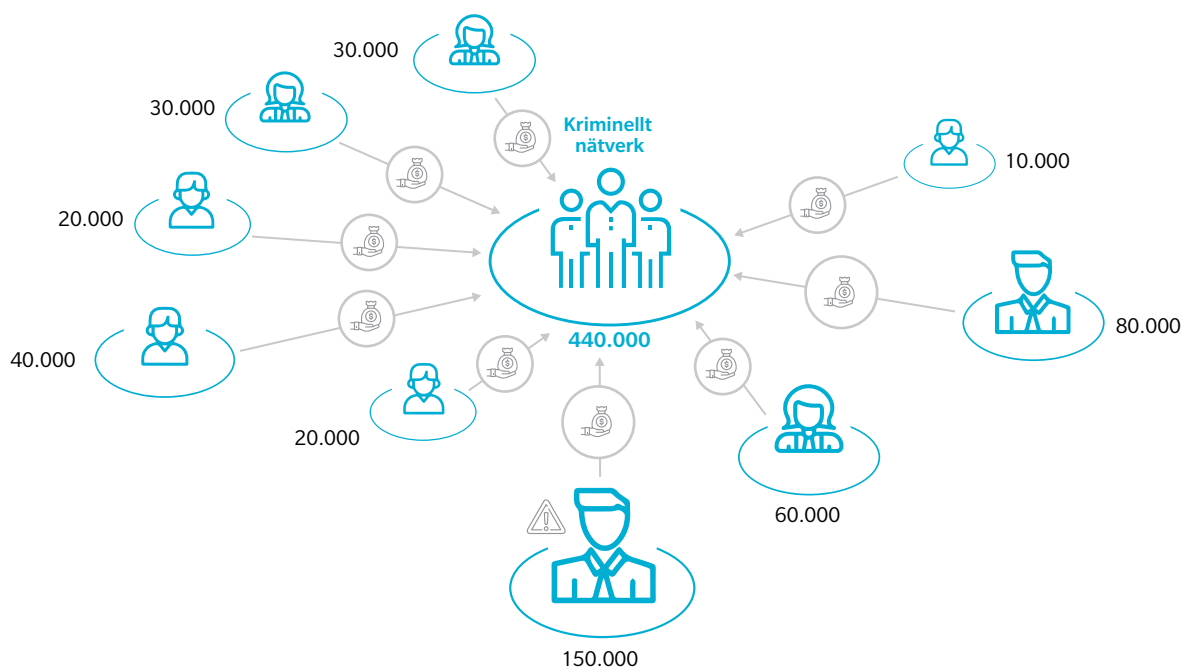
### 4 TRANSAKTIONSANALYS

I analyslagret för transaktionsdata genomförs nätverksanalys, klusteranalys och mönsteranalys samt analys av historiskt lagrad data om transaktioner. Dataunderlaget kommer endast innehålla information om transaktioner och den anonymiserade kundinformationen utan möjlighet att identifiera specifika personer eller företag.

#### NÄTVERKSANALYS

Kriminella aktörer som ämnar att tvätta pengar arbetar ofta i olika konstellationer av nätverk vari transaktionerna delas upp för att sedan konsolideras i ett senare steg för att minska risken att bli upptäckta. Nätverksanalys möjliggör identifiering av noder inom ett nätverk och relationerna mellan noderna. Genom att analysera gemensamma egenskaper mellan noder, och styrkan av länken kan nyckelpersoner inom nätverk identifieras. Genom tillgång till ett stort och växande dataunderlag av kunder och transaktioner och tillämpning av nätverksanalys som avslöjar hur olika noder förhåller sig till varandra kan större, mer komplexa nätverk av kriminella aktörer avslöjas.

Figur 12: Illustrerad användning av smurfing



Genom att kombinera data från flera finansiella institut kan dessa nätverk identifieras med mycket större precision, och möjligheten att undgå upptäckt kraftigt reduceras.

Exempelvis kan det visa sig att en kund kontinuerligt utför misstänkta transaktioner med relaterade kunder, men att dessa andra kunder inte identifierats som misstänkta baserat på analys av enskilda transaktioner i enskilda banker. Detta skulle kunna manifesteras i ett fall av så kallad "smurfing", där transaktioner under gränsvärden konsolideras till ett större flöde för att undvika identifiering. Transaktionerna från de enskilda personerna till ett internationellt konto kontrollerat av ett kriminellt nätverk är under gränsvärden för kontroller sett separat. Om däremot en transaktion identifieras som misstänkt kan övriga transaktioner identifieras som misstänkta till samma konto. Inkomna transaktioner kommer också löpande att jämföras mot historiskt inrapporterade transaktioner. Genom att löpande analysera ett växande underlag av transaktioner från flera banker kan identifiering av tidigare misstänkta transaktioner ske (som tidigare inte gav upphov till vidare misstanke) i ett större och längre perspektiv, och på så sätt avslöja systematisk penningtvätt som inte skulle upptäckas genom att observera isolerade transaktioner. Analysen kommer också göras mot samtliga inrapporterade bankers data, och på så vis bygga på ett betydligt bredare underlag än vad som hade varit möjligt inom en enskild bank.

## KLUSTERANALYS

Traditionella transaktionsmonitoreringssystem baseras ofta på förutbestämda regler och scenarier som utgår från relativt breda antaganden. Dessa regler och antaganden är ofta applicerade på stora segment av kunder utan att ta hänsyn till beteendet av enskilda

kunder. För breda regler och kriterier för vad som ska flaggas som misstänkt aktivitet kan således leda till att transaktioner flaggas som misstänkta trots att de inte är ovanliga för den individuella kunden.

Genom mönsteranalys och klusteranalys kan identifiering av transaktioner som avviker från typiska mönster ske, baserat på typ av kund, produkt eller geografi. Det underliggande antagandet är att avvikelser från kluster är mer benägna att representera misstänkt aktivitet och flaggas därför som en risk. I takt med att mer data och fler verkliga fall flödar in kan en mer komplett bild sammanställas.

## MASKININLÄRNING OCH AI

För framgångsrik maskininläring behövs det faktiska utfall av det man söker att träna på och ju fler fall desto bättre. Den föreslagna lösningen som ger en mer komplett bild av de finansiella flödena kommer att kraftigt förbättra förmågan att identifiera faktiska fall av kriminell aktivitet, och med detta också kraftigt förbättra möjligheterna för maximalt utnyttjande av maskininläring och AI för automation och identifiering av beteendeförändringar.

## 5 GENERERING AV MISSTÄNKT FALL

Om misstankegraden ökar efter att kunddata eller transaktionsdata har passerat respektive analysinstanser genereras automatiskt ett misstänkt fall om penningtvätt. Rapporten om misstanke kommer att innehålla en beskrivning om misstanken samt inom vilket konfidensintervall misstankegraden ligger inom.

## 6 RISKBEDÖMNING OCH PRIORITERING

För att mer effektivt hantera "false positives" som uppstår efter analysen kommer en avancerad riskbedömning och prioritering genomföras. Ambitionen är att denna typ av analys ska förutsäga hur sannolikt det är att ett specifikt larm resulterar i en brottsutredning eller annan rättslig åtgärd. Denna typ av analys innefattar till exempel utredningsparametrar såsom kundtyp, kundens risknivå, flaggade scenarier, och historisk data. Larmen prioriteras utifrån risknivån, och kan mer effektivt fördelas för vidare granskning. Varje larm får en riskbedömning (till exempel 1-100) och kategoriseras sedan som hög, medel eller låg risk. Baserat på kategoriseringen fördelas larm på olika sätt för vidare granskning. Larm med högre risk kan till exempel granskas innan larm med lägre risk, eller så kan larm med högre risk granskas av mer seniora analytiker än larm med lägre risk, osv.

## 7 MANUELL BEDÖMNING AV FALL

När den automatiska analysen och riskbedömningen har genomförts går ärendet, enligt prioriteringsordning, vidare för manuell hantering av utredande Polismyndighets granskande enhet. Beroende på om misstanken har uppstått från analys av kund eller transaktionsdata bedömer den granskande enheten om misstankegraden är hög nog för att berättiga en begäran om att övrig kunddata anonymiseras för utredningssyfte. Den granskande enheten bedömer också om kompletterande eller förtydligande information behöver inhämtas från rapporterade banker. Nödvändig information inhämtas även från andra myndigheter och andra FIU:er runt om i världen.

## 8 RAPPORT OM MISSTÄNKT PENNINGTVÄTT OCH BESLUT OM ÅTGÄRD

När den initiala utredningen är genomförd sammanställs en underrättelsestyrd rapport om misstänkt penningtvätt och utredande Polismyndighet beslutar om åtgärd (dispositionsförbud, vidare handläggning av brottsbekämpande myndighet, nedläggning av utredning, etc.).

## ABOUT OLIVER WYMAN

Oliver Wyman is a global leader in management consulting. With offices in 60 cities across 29 countries, Oliver Wyman combines deep industry knowledge with specialized expertise in strategy, operations, risk management, and organization transformation. The firm has more than 5,000 professionals around the world who work with clients to optimize their business, improve their operations and risk profile, and accelerate their organizational performance to seize the most attractive opportunities. Oliver Wyman is a wholly owned subsidiary of Marsh & McLennan Companies [NYSE: MMC].

For more information, visit [www.oliverwyman.com](http://www.oliverwyman.com). Follow Oliver Wyman on Twitter @OliverWyman.

### ASIA PACIFIC

+65 6510 9700

### AMERICAS

+1 212 541 8100

### EMEA

+44 20 73333 8333

## AUTHORS

### MARTIN ANDERSSON

Partner

[Martin.Andersson@oliverwyman.com](mailto:Martin.Andersson@oliverwyman.com)

### RIKARD LIND

Engagement Manager

[Rikard.Lind@oliverwyman.com](mailto:Rikard.Lind@oliverwyman.com)

### CARL RANING

Partner

[Carl.Raning@oliverwyman.com](mailto:Carl.Raning@oliverwyman.com)

### SEAN CORY

Partner

[Sean.Cory@oliverwyman.com](mailto:Sean.Cory@oliverwyman.com)

### SARA JONSSON

Engagement Manager

[Sara.Jonsson@oliverwyman.com](mailto:Sara.Jonsson@oliverwyman.com)

Copyright © 2019 Oliver Wyman

All rights reserved. This report may not be reproduced or redistributed, in whole or in part, without the written permission of Oliver Wyman and Oliver Wyman accepts no liability whatsoever for the actions of third parties in this respect.

The information and opinions in this report were prepared by Oliver Wyman. This report is not investment advice and should not be relied on for such advice or as a substitute for consultation with professional accountants, tax, legal or financial advisors. Oliver Wyman has made every effort to use reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied. Oliver Wyman disclaims any responsibility to update the information or conclusions in this report. Oliver Wyman accepts no liability for any loss arising from any action taken or refrained from as a result of information contained in this report or any reports or sources of information referred to herein, or for any consequential, special or similar damages even if advised of the possibility of such damages. This report may not be sold without the written consent of Oliver Wyman.