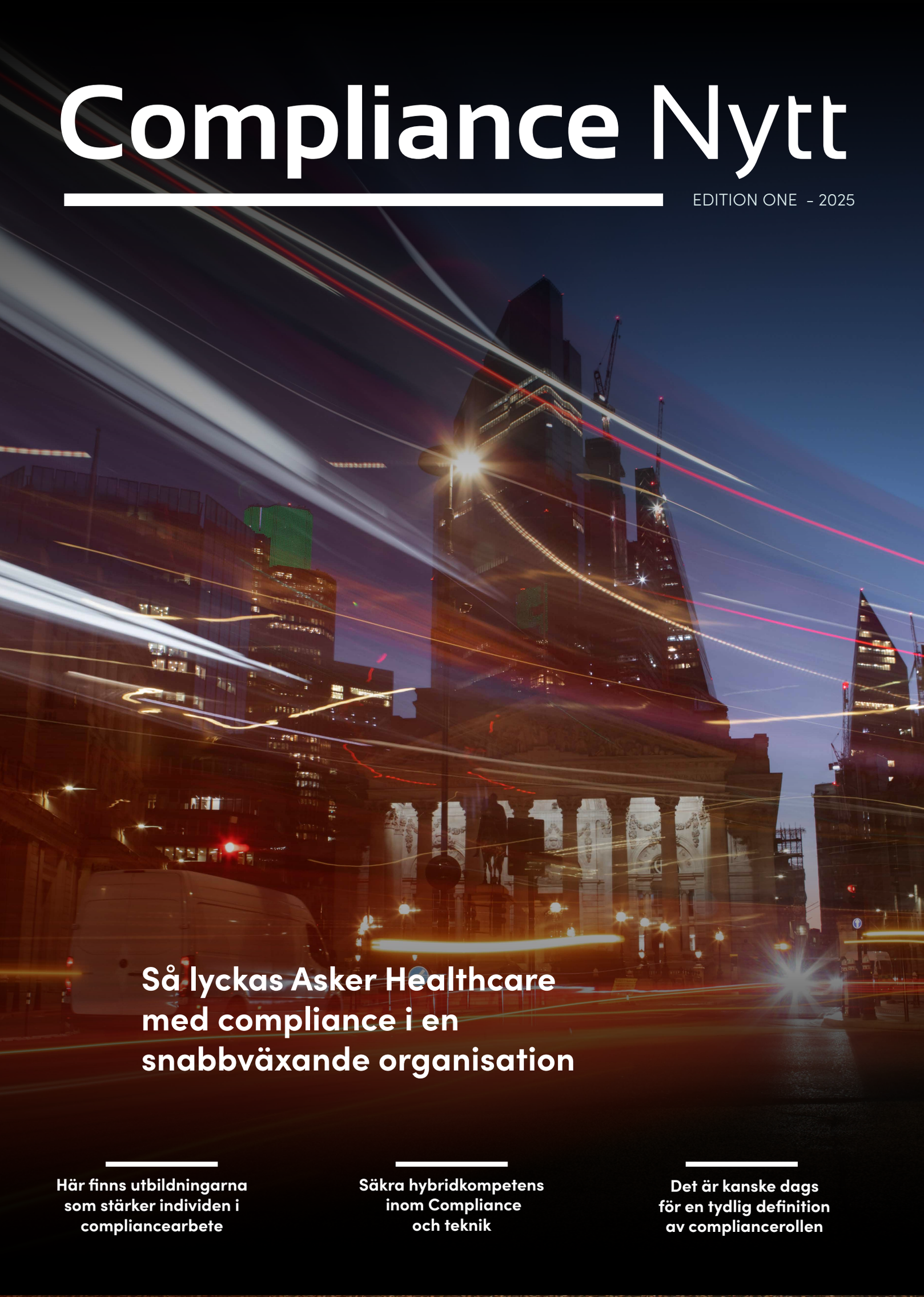
Compliance Nytt

EDITION ONE - 2025



Så lyckas Asker Healthcare med compliance i en snabbväxande organisation

Här finns utbildningarna som stärker individen i compliancearbete

Säkra hybridkompetens inom Compliance och teknik

Det är kanske dags för en tydlig definition av compliancerollen



LEDARE

Compliance 2025 ställer nya krav på kompetens och innovation



Complianceområdet befinner sig just nu i en transformativ fas som ställer höga krav på företagens anpassningsförmåga. Med ökande regulatoriska krav, teknologisk utveckling och ett växande fokus på hållbarhet är det tydligt att compliance inte längre är en isolerad funktion – det är en strategisk nödvändighet för att möta morgondagens affärsutmaningar.

Under de senaste åren har en av de mest utmärkande trenderna varit den växande regulatoriska komplexiteten. Med en ständig tillkomst av nya nationella och internationella regelverk blir det allt viktigare att förstå hur dessa samverkar och påverkar olika marknader. Företag som agerar globalt måste navigera mellan överlappande krav inom dataskydd, finans och anti-korruption, vilket gör experter med djupgående juridisk och operativ kunskap ovärderliga. Samtidigt spelar teknologin en allt större roll i hur compliancearbetet utvecklas. Med hjälp av AI och maskininlärning kan processer som riskbedömningar och övervakning automatiseras och göras mer träffsäkra. Den stora utmaningen ligger därmed i att hitta rätt kompetens – personer som kan integrera tekniska lösningar med regelefterlevnad på ett sätt som inte enbart effektiviserar arbetet, utan även förstärker dess kvalitet.

Ett ökat fokus på ESG (Environmental, Social, and Governance) förändrar också spelplanen. Hållbarhet och socialt ansvar har blivit affärskritiska faktorer, där både lagstiftare och investerare ställer krav på transparenta och trovärdiga rapporter. Specialistkompetens inom ESG-regelverk och hållbarhetsarbete blir därför allt viktigare för företag som vill säkra sitt anseende och sin konkurrenskraft på en marknad där hållbarhet numera är en självklarhet.

Det är emellertid inte bara nya regelverk som ställer krav på kompetensutveckling inom compliance – även gränsdragningen mellan riskhantering och compliance förändras. Allt fler företag ser compliance som en del av sin övergripande riskhantering, vilket ökar behovet av personer med erfarenhet av både operativa risker och regulatoriska krav. Denna utveckling förstärks av en accelererande digitalisering, vilken hårt reglerats av EU och lett till ökat tryck på både cybersäkerhet och dataskydd. Här efterfrågas talanger som kan kombinera juridisk förståelse med teknisk kunskap – en kombination som blir avgörande för att skydda företag mot de växande hoten i den digitala eran.

En av de mest positiva utvecklingarna som fortlöper under 2025 är hur compliance i allt högre grad integreras som en del av företagskulturen, snarare än betraktas som en isolerad funktion. Framtidens företagsledare måste kunna bygga organisationer där regelefterlevnad genomsyrar allt från styrelserum till verksamhetsnära processer. Det handlar om att skapa en miljö där etik och transparens inte enbart är mål och riktlinjer, utan en självklar del av det dagliga arbetet. För att möta såväl förväntningarna som utmaningarna inom compliance behöver företag därmed utveckla nya sätt att attrahera och behålla talanger. Kombinationen av juridisk, teknisk och operativ kompetens är redan idag en eftertraktad resurs – och behovet av en bredare kompetensbas kommer med säkerhet att fortsätta växa.

Ron Cohen,
Co-founder & Partner på Sharp Recruitment & Consultants

Compliance Nytt

Publisher
Dejan Smiljanic
dejan@compliancetoday.se
0706-77 50 76

Compliance Conference & Awards
Besök hemsidan: www.cmcawards.se

Redaktion och skribenter
Selma Louf
Johannes Hägglund

Post
Konceptsälj i Sverige AB
Vasagatan 28
111 20 Stockholm

Personuppgifter
Personuppgifter Compliance NYTT som ges ut av Konceptsälj i Sverige AB, Konceptsälj i Sverige AB, behandlar alla kunduppgifter elektroniskt. Kunduppgifterna används för att fullgöra kundrelationer som leverans av produkter, fakturering, analys samt marknadsföring av egna och andras produkter.



Tone Bergfelt:

Compliancefunktionens roll för effektiv hantering av DORA

Den digitala utvecklingen medför både möjligheter och risker, särskilt inom den finansiella sektorn där beroendet av teknik och tredjepartsleverantörer ökar. För att stärka motståndskraften inom EU har DORA, Digital Operational Resilience Act, införts, som bl.a. ställer krav på riskhantering, incidentrapportering, testning samt kontroll och styrning av tredjepartsleverantörer. Bolag och compliancefunktioner står således inför en ny verklighet 2025 när DORA-kraven ska omsättas i praktiken.

Hur ska compliancefunktioner hantera regelverkskraven i DORA för att säkerställa en långsiktig efterlevnad?

För att säkerställa långsiktig efterlevnad av DORA, bör compliancefunktioner under 2025 fokusera på att stötta verksamheten avseende integreringen av regelverket i de operativa processerna. Många bolag har arbetat med fokuserade implementeringsprojekt och tagit fram nya och/eller ändrade processer och rutiner som nu ska börja efterlevas i praktiken. Med förändrade arbetssätt uppstår nya utmaningar där anpassningar kommer behöva göras löpande under året och det är viktigt att efterlevnaden inte enbart handlar om dokumentation och rapportering.

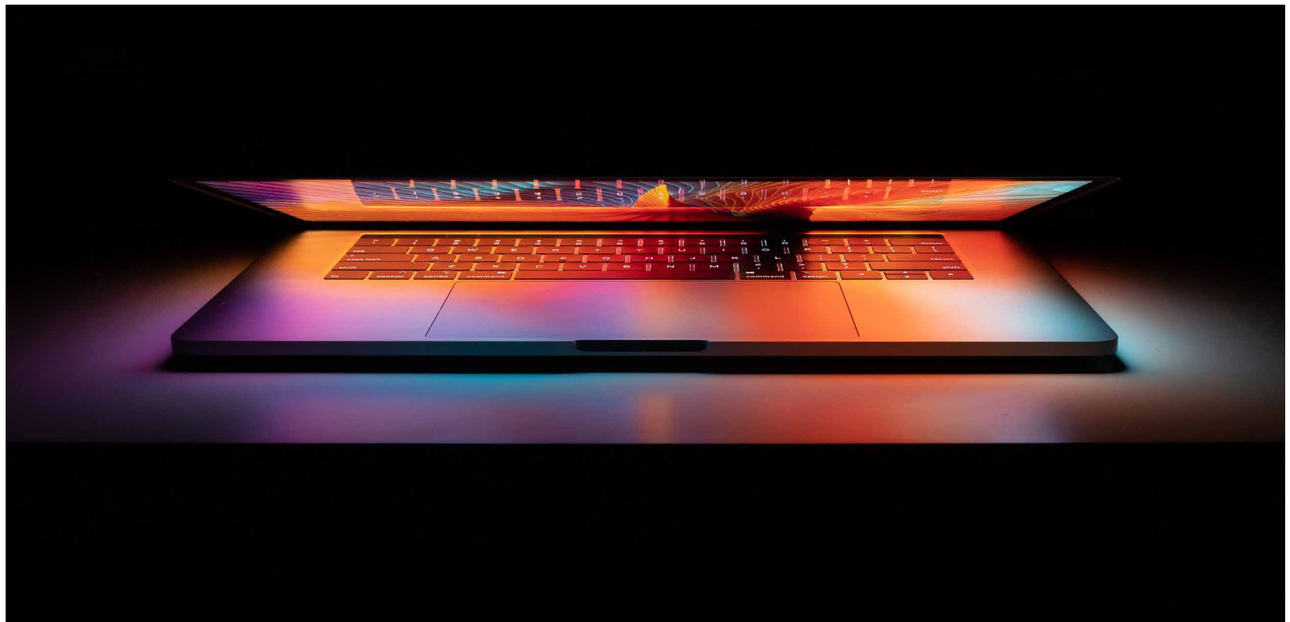
Ett område där vi särskilt ser att compliancefunktioner har en viktig roll är i hanteringen av de informations- och kommunikationsteknologiska tjänster, IKT-tjänster, som tillhandahålls av en tredjepartsleverantör. Tredjepartsrisker och hanteringen av uppdragsavtal är en compliancerisk som många compliancefunktioner fokuserar på generellt men som här får ett ökat fokus. DORA omfattar bl.a. bestämmelser om hantering av risker i samband med att bolag använder IKT-tjänster som tillhandahålls av en tredjepartsleverantör inbegripet krav vid ingåendet av sådana avtal, inklusive avtalsbestämmelser, samt uppföljning av sådana avtalsförhållanden. Utöver det ställs det även krav på att de bolag som har att efterleva DORA ska ha en policy som reglerar den hanteringen. Dessa krav är sedan innan välbekanta för många bolag utifrån andra regler avseende utläggning av verksamhet och uppdragsavtal. Vi tror här att compliancefunktionen kan bidra med råd och stöd avseende hantering av tredjepartsrisk enligt DORA och då dra nytta av erfarenheter från arbetet avseende utläggning av verksamhet från andra regelverk. Möjligen finns det även vissa synergieffekter i arbetet genom att implementera kraven från DORA i de processer och rutiner som etablerats sedan tidigare.

Sammanfattningsvis ser vi att compliancefunktionen har en viktig roll i att, genom råd och stöd, hitta rätt väg framåt där regelefterlevnaden och det övergripande syftet att stärka den digitala operativa motståndskraften säkerställs, samtidigt som arbetet är effektivt och inte onödigt betungande. Compliancefunktionen behöver arbeta nära verksamheten för att stötta i implementeringen av DORA i det dagliga arbetet och säkerställa att de åtgärder som vidtas är funktionella, realistiska och anpassade efter organisationens faktiska riskexponering. Genom att arbeta nära verksamheten, identifiera risker och skapa en struktur för kontinuerlig anpassning kan en stabil grund läggas innan mer omfattande kontroller införs. Att våga arbeta riskbaserat är en förutsättning för att kunna säkerställa god regelefterlevnad men framför allt för att hantera digitala risker och eventuella avbrott i verksamheten relaterat till avbrott i IKT-tjänster.

Advisenses tips till compliancefunktioner är således följande

- Fokusera på en övergripande förståelse av DORA (för verksamheten och compliancefunktionen).
- Hur har implementeringen fortskridit? Finns kvarstående delar som behöver hanteras? Vad är riskerna kopplat till regelefterlevnad?
- Hitta en lagom ambitionsnivå och förstå var bolaget står idag samt planen framåt, arbeta riskbaserat och fokusera på de delar där compliancerisken är som störst.
- Gå inte ”i fållan” och granska processer och rutiner utifrån de detaljerade kraven i DORA. Detta kräver sannolikt ett nära samarbete mellan compliancefunktionen och verksamheten.

Avslutningsvis kan det konstateras att det är viktigt att säkerställa att DORA integreras i organisationens verksamhet och inte blir en isolerad efterlevnadsfråga, och för att lyckas med detta krävs ett nära och strukturerat samarbete mellan kontrollfunktionerna och verksamheten. Genom att koppla efterlevnad till affärsnytta och säkerställa att varje krav i DORA bidrar till en starkare operativ resiliens, blir regelverket ett verktyg för långsiktig stabilitet snarare än en administrativ börda.





Ronny Gustavsson
Director & Head of AML hos Advisense

AML-förordningen – Ett avgörande steg i kampen mot penningtvätt

EU:s nya AML-paket är en välkommen och nödvändig utveckling i kampen mot penningtvätt och finansiering av terrorism. AML-förordningens högre krav på kundkännedom och snabbare hantering av misstankar kommer att bidra till ett mer effektivt förhindrade av finansiell brottslighet. För att lyckas krävs det dock att företag investerar i rätt teknik, utbildar sin personal och har en proaktiv inställning till riskhantering. Med en tydlig AML-strategi, ändamålsenliga förberedelser och IT-verktyg kan företag inte bara uppfylla kraven utan även skapa konkurrensfördelar. Därför är AML-förordningen kritisk för samhället och en nyckel för att stärka förtroendet och transparensen för den finansiella branschen i stort, säger Ronny Gustavsson.

I **senaste numret** av ComplianceNytt listades ”AML” (Anti-Money Laundering) som ett av de hetaste områdena inom compliance för året 2025. AML-förordningen som träder i kraft i juli 2027 ligger just nu på de allra flestas bord i den finansiella sektorn. Samtidigt finns det när man läser mellan raderna en tendens till ’AML-trötthet’ efter många års regulatoriska förändringar. Det finns finansiella institut som fortfarande arbetar med att så att säga komma i kapp, och ett viktigt råd i och med den nya förordningen är att inte ta med sig gamla regelefterlevnadsbrister in i det kommande implementeringsarbetet.

Som utgångspunkt, men också för att väcka de eventuellt compliance-trötta, är det oerhört viktigt att sätta AML-förordningen i en kontext. Myndighets- och forskningsrapporterna om utvecklingen av den kriminella ekonomin duggar tätt. Det finns ett enormt behov för finansiella bolag att förstå vad som sker inom den globala organiserade brottsligheten och vad det innebär för arbetet mot penningtvätt men också finansiell brottslighet i vidare mening, inklusive bedrägerier och korruption.

En klarare syn på anledningen

Vi är på väg mot en tsunami, men det är inte en regelverkstsunami som bekant myntats av en svensk bank-vd. Det är en tsunami i form av den femte vågens organiserade brottslighet på global nivå som pekar rakt mot en kriminell guldålder, enligt de rapporter som extrapolerat den utveckling som vi ser nu och framåt i tiden mot år 2040. Utvecklingen rör sig redan exponentiellt från cyberbrott mot ytterligare skalbarhet med hjälp av AI. Open payments, snabbare transaktioner, krypto, big data och molntjänster innebär nya sårbarheter och sporrar dynamiska samarbeten mellan kriminella nätverk, nya svarta marknader för högteknologisk brottslighet som tjänst (high-tech crime as a service).

Samtidigt pågår ett slags konsolidering av den organiserade brottsligheten som tar form genom hypersammankopplade kriminella supernav i Dubai och Marbella. Därifrån styrs och bedrivs brottsligheten i hybridform, det vill säga både på distans och digitalt (bedrägerier, cyberbrott, utpressning mm), och i form av fysisk handel med t.ex. narkotika och vapen. Utifrån ett svenskt perspektiv är detta ingen nyhet. Svenska kriminella gäng är redan en integrerad del av den infrastrukturen. I sammanhanget är det viktigt att vara varse om att Sverige nu ligger på plats 24 av 44 länder i Europa enligt Organised Crime Index, med en negativ utveckling sett i ’criminality score’. Positivt är att vår motståndskraft bedöms som god, med en viss negativ rörelse där vi nu befinner oss på plats 13 av 44. Det är denna realitet som torde vara utgångspunkten i alla resonemang om AML-compliance som behöver föras, nämligen förmågan att strypa penningtvätten för att stoppa brottsligheten. Det är dramatiska verb för en dramatisk realitet.

Den europeiska unionen har tagit ett betydande steg framåt i kampen mot penningtvätt och finansiering av terrorism genom att introducera sitt nya AML-paket (Anti-Money Laundering). Paketet består av en ny förordning som blir direkt tillämplig i hela EU, etableringen av en europeisk tillsynsmyndighet och en harmonisering av grundläggande delar inom AML, såsom KYC (Know Your Customer)-inhämtning. Denna utveckling kommer att gynna finansiella företag som verkar över nationsgränser inom EU och samtidigt skärpa kraven på kundkännedom och reaktionsförmåga vid misstanke om penningtvätt.

Enhetliga Regler och Fördelar för Finansiella Företag

Ett av de främsta målen med det nya AML-paketet är att minska den fragmenterade tillsynen inom EU. Genom att harmonisera reglerna för grundläggande AML-processer såsom KYC och transaktionsmonitorering, behöver finansiella företag inte längre navigera genom olika nationella tolkningar av EU-direktiv. I framtiden får företag som verkar i flera länder i EU därför en mer förutsägbar efterlevnadsmiljö och därmed en minskad administrativ börda.

En gemensam europeisk tillsynsmyndighet kommer också att erbjuda tydligare vägledning och skapa en jämnare spelplan för marknadens aktörer, vilket kommer kunna minska risken för snedvriden konkurrens och bidra till att säkerställa att höga standarder efterlevs över hela unionen. För finansiella aktörer innebär det nya regelverket att de kan implementera en mer enhetlig och skalbar AML-strategi.

AML-förordningen kommer innebära skärpta åtgärder på kundkännedom och förändrade krav på utredning av verklig huvudman. Därtill inkluderas internationella sanktioner vilket blir en tydlig central del i AML/CTF-arbetet. Ytterligare minimi-tillfällen då fördjupad kundkännedom (EDD) måste tillämpas, särskilda högriskscenarion för TM kommer behövas, och det tillkommer vidare att kunder med tillgångar över 50M EUR ska särbehandlas. Vidare ges medlemsstaterna, AMLA och kommissionen framöver mandat att definiera fler högrisksektorer.

De ökade kraven på kundkännedom bedöms vara en av de mest betydande förändringarna i det nya AML-paketet. Finansiella företag kommer att behöva

”Ett viktigt råd i och med den nya förordningen är att inte ta med sig gamla regelefterlevnadsbrister in i det kommande implementeringsarbetet.”

samla in mer detaljerad information om sina kunder och vara beredda att uppdatera denna information på löpande basis. Detta sker redan idag men kraven blir mer detaljerade. Det handlar inte bara om att ha rätt information från början, utan även om att övervaka förändringar i kundens beteende och affärsförbindelser. Regelverket ställer också högre krav på skyndsamhet vid misstanke om penningtvätt. Företag måste kunna identifiera och rapportera misstänkta transaktioner i realtid eller nära nog, vilket förutsätter effektivare interna processer och högre krav på tekniska lösningar.

En ytterligare viktig nyhet att ta fasta vid är att även att oförmåga att utföra KYC kan utgöra grund för rapportering. Prioritering av larm kommer tillåtas uttryckligen utifrån ett antal datapunkter, vilket är värt att beakta också som en effektiviseringspotential givet långt pågående problematik med falska positiva larm. En tidsfrist för rapportering etableras också i och med förordningen, där regeln blir fem arbetsdagar i normalfallet men i brådskande ärenden kan det sänkas till 24h av FIU. I praktiken kommer det innebära krav på någon form av jourarbete.

Bredare kompetenser utöver juridiken behövs

Erfarenheten visar att en strikt regulatorisk tolkning utan operationell förståelse ofta leder till suboptimala lösningar. Regelverkens intentioner kan missas, och implementeringar riskerar att bli ineffektiva, dyra eller rent av kontraproduktiva. Det är också tydligt att verksamheter idag i vissa fall fortfarande har utmaningar med befintliga regelverkskrav, och därmed kommer att ta med sig sina regelefterlevnadsbrister in i kommande implementeringsarbete.

Den ökade komplexiteten i både regelverket och brottslingarnas metoder kräver att finansiella företag utvecklar en djupare förståelse för modus operandi för penningtvätt. Kriminella nätverk använder allt mer sofistikerade metoder för att dölja sina spår, vilket gör att AML-funktioner måste hålla sig uppdaterade om nya trender och risker. Enligt AML-förordningen kommer också en något utökad lista över källor (SNRA, NRA, sektorsspecifika RA samt “relevant information från internationella normgivare samt kommissionen eller AMLA) samt tillägg att kundbasen ska ingå i bedömningen. Utvecklingen pekar som ovan kort beskrivet bara åt ett håll, vilket gör det än mer kritiskt att med hjälp av mer och bättre data, skala upp kapaciteten att uppnå nödvändig fördjupad kundkännedom, uppbackat av klusteranalyser som kan knäcka den alltmer tech-drivna och uppskalade brottslighet som vi står inför.

Ökade krav kommer driva på behovet att automatisera

I det fortsatta arbetet framåt, är en bredare kompetens avgörande och förutsätter en mer proaktiv inställning till utbildning inom AML-området. Företag måste se till att deras anställda inte bara förstår de nya reglerna, utan även vet hur de ska tillämpas i praktiken och vilka riskindikatorer de ska vara uppmärksamma på. Den ökade detaljregleringen genom AML-förordningen innebär ofrånkomligen att företag kommer behöva hantera större mängder data, ha större analyskapacitet och en snabbare rapportering. Det betyder vidare en rörligare och mer anpassningsbar riskklassificering.

Dessa förändringar bör ses i ljuset av potentialen att automatisera olika processer. Bankernas AML-avdelningar har växt exponentiellt på senare år, och det råder brist på erfarna och kompetenta resurser på marknaden. Det är orimligt att anta att compliance-avdelningar kan fortsätta att växa i termer av antal anställda på samma sätt som under senare år.

De ökade kraven kommer kräva nya arbetssätt. De flesta finansiella aktörer arbetar med komplexa IT-miljöer, där AML-system måste kunna kommunicera smidigt med andra system inom tex CRM, transaktioner, depåer, konton, krediter och rapportering. För att uppnå detta krävs en teknisk förståelse för API:er, dataintegration och systemarkitektur. En ineffektiv integration kan leda till att kritiska AML-processer blir fördröjda, inte får de data-uppgifter som krävs eller att viktig information inte flödar korrekt mellan de olika systemen.

För att kunna lyckas med implementeringen av AML-förordningen, behöver finansiella institut kombinera kunskap om tekniska processflöden med operationell och regulatorisk expertis och bygga system som inte bara är kompatibla med regelverket, utan som också möjliggör automatiserad övervakning och analys av transaktionsdata. AI och maskininlärning erbjuder stora möjligheter att identifiera avvikande mönster i realtid. Automatiserade verktyg för KYC-inhämtning och riskbedömning kommer att spela en viktig roll för att säkerställa regelefterlevnad och effektivt motverka penningtvätt.

Att ha tillgång till korrekta och uppdaterade data möjliggör inte bara bättre övervakning utan ger även företagen en möjlighet att agera snabbt vid misstänkta transaktioner. Systemintegration och ytterst datakvalitet kommer i nästa steg vara kritiska faktorer. Därför kan AML-förordningen bli den trigger som behövs för att jobba smartare inom AML.

Juridik, Compliance, Ekonomi
Vi är brobyggarna mellan expertis ...



... och framgång.

sharprecruitment.se

Ett av Sveriges mest specialiserade, erfarna och personliga konsult- och rekryteringsföretag inom juridik, compliance och ekonomi. Vi kombinerar djup branschkunskap med ett exklusivt nätverk av toppkandidater som ofta inte finns på den öppna marknaden. Genom vår skräddarsydda och datadrivna process levererar vi inte bara en kandidat – vi hittar den rätta personen som kan lyfta både företaget och teamet till nästa nivå.

SHARP
RECRUITMENT & CONSULTANTS





Så lyckas Asker Healthcare med compliance i en snabbväxande organisation

Hur fungerar compliance i en organisation som växer snabbt både organiskt och genom förvärv? Jennie Espelund och Mathilda Tergou arbetar båda med compliance på medtech-koncernen Asker Healthcare Group. Vi träffas för att diskutera förutsättningarna för skalbar compliance och fördelarna med decentralisering.

Asker Healthcare Group är en ledande partner för både vårdgivare och patienter inom medicintekniska produkter och tjänster i Europa. Koncernen fokuserar på att utveckla och förvärva innovativa företag som stärker vården genom att förbättra vårdresultat, minska totalkostnader och säkerställa en hållbar och rättvis värdekedja. Sedan januari 2019 har Asker förvärvat över 50 företag och har idag mer än 4 000 anställda i 17 länder.

För att uppnå sina mål tillämpar Asker en strategi kallad ”twin engine”, som kombinerar organisk tillväxt med strategiska förvärv. Koncernen erbjuder ett brett sortiment av omkring 50 000 produkter från över 1 500 leverantörer, inklusive både produkter från stora internationella varumärken samt egna varumärken och egna märkesvaror.

Jennie Espelund är chefsjurist på Asker, och hanterar de övergripande legala frågorna, samt compliance och governance. Hennes kollega Mathilda Tergou ansvarar för compliance i koncernen genom bland annat utbildning och kommunikation, och hjälper till med implementering av ramverk rörande compliance och governance.

Att implementera ett framgångsrikt complianceprogram i en snabbväxande koncern med verksamhet i flera olika marknader är ingen enkel uppgift. Men Asker har en tydlig strategi.

”Ett riktigt bra complianceprogram är en säkerhet mot risker – både interna och externa – vilket kan bygga trygga relationer med kunder och leverantörer och därmed också en trygg tillväxt.”

Jennie Espelund

– Hälso- och sjukvårdssystemen i Europa styrs av olika nationella regler och därför är en decentraliserad styrmodell viktig. De lokala bolagen har fullt operationellt ansvar såsom kund- och produktsortiment. För att inte tappa kontrollen behöver vi däremot en tydlig och övergripande styrning över de viktigaste. Därför har vi tagit fram ett governance ramverk som vi kallar för, Asker Management Standard, som består av 12 kapitel där bl a finansiell rapportering och kontroll, riskhantering, affärsetik, HR, IT-säkerhet och integritet samt legala och regulatoriska krav finns med, berättar Jennie.

För att bidra till tydliga roller och ansvar, har varje kapitel i Asker Management Standard en person inom koncernledningen som är ytterst ansvarig för sitt kapitel. Inom det ansvaret ligger att löpande göra riskutvärderingar, ta fram styrdokument som policies och processer, utbilda organisationen samt sätta kontoller. Vi kallar ramverket för vår interna lagbok. Den finns tillgänglig för alla på vårt intranät och vi arbetar löpande med att göra innehållet lättillgängligt för alla medarbetare. Det ska inte finnas några oklarheter i vilka krav som ryms inom respektive del eller vem som är ansvarig, fortsätter Mathilda.

Eftersom vi växer så snabbt både organiskt och genom förvärv är just utbildning en central del vilket sker genom koncernens egen akademi: Asker Business School. Inom den finns både nätverk, e-learnings och fysiska utbildningstillfällen uppsatta. Varje halvår träffar vi ledningsgrupperna i de nyförvärvade bolagen och andra nyckelpersoner och går igenom bl a Asker Management Standard. Att tidigt kommunicera förväntansbilden men också att lära känna varandra och tillsammans identifiera best practice och synergier är viktigt, berättar Jennie.

För de nyförvärvade bolagen finns en tydlig 100-dagars plan formulerad med viktiga milstolpar som vi följer upp på. Det är en process som anpassas efter mognadsgraden hos bolaget. Områden som Uppförandekoden, finansiell rapportering och IT har hög prioritet.
– En nyckel är att komma in i ett tidigt stadium. Bolagen varierar i storlek, vissa består endast av två personer som gör allt, medan andra har ett eget complianceteam på plats. Det handlar till stor del om att hjälpa dem prioritera och successivt implementera Asker Management Standard – annars blir det lätt övermäktigt. Det är också viktigt för oss att bygga tillit och skapa nätverk. Vi vill att de ska ringa oss om de har frågor eller om någonting händer, förklarar Mathilda.

Asker arbetar även med en årlig uppdatering av Asker Management Standard, där både styrelse och koncernledning men också de lokala bolagen ombeds lämna synpunkter. Vi ser att det är minst lika viktigt att kunna omvärdera de regler vi redan har på plats som att lägga till nya. Ett uppdaterat och relevant ramverk är viktigt i takt med att vi växer, kommer in på nya marknader men också då omvärlden förändras, fortsätter Mathilda.
Inte heller Asker har varit oberörda av den regelverksvåg som sveper över Europa. Jennie och Mathilda beskriver att utmaningen ligger i hur man implementerar allt som krävs, utan att dränka verksamheten i compliance och administration.
– Inom medicinteknik är kraven strikta och alla produkter måste hålla hög kvalité, detta kan vi aldrig frångå ifrån, men nya regler tillkommer inom alltifrån IT säkerhet till hållbarhet vilket kan upplevas som betungande för verksamheten. Dessa lagkrav måste vi få in i Asker Management Standard. Tillsammans med ESG teamet gjorde vi en stor översyn för att fånga alltifrån utvärdering av leverantörer till koldioxidrapportering. Det fina arbetet återspeglas i det Platinum-betyg som Asker erhållits från EcoVadis men också då vi är ett av få bolag som redan i år rapporterar enligt CSRD, berättar Jennie.

Vi avslutar mötet med att diskutera värdet av compliance. Både Mathilda och Jennie betonar vikten av att få med sig styrelse och ledning i arbetet men också personer ute i verksamheten. Uttrycket ”train the trainers” är högst relevant när man är verksam i en decentraliserad organisation. Hitta ditt nätverk och var närvarande i uppbyggnaden av strukturen. Se till att alla förstår värdet i varför compliance är viktigt och vad det faktiskt bidrar till. Ett riktigt bra complianceprogram är en säkerhet mot risker – både interna och externa – vilket kan bygga trygga relationer med kunder och leverantörer och därmed också en trygg tillväxt, avslutar Jennie.

Text: Selma Louf



Säkra hybridkompetens inom Compliance och teknik

I en värld där teknologisk utveckling sker i ett allt högre tempo, samtidigt som regelverk och compliance-krav blir mer komplexa, står företag och organisationer inför en avgörande fråga: hur säkrar vi kompetens som kombinerar compliance och teknisk expertis? Denna kombination, ofta kallad hybridkompetens, har blivit en strategisk förutsättning för att hantera digitaliseringens möjligheter och risker. Samtidigt är försörjningen av denna kompetens en av de mest kritiska frågorna för framtidens arbetsmarknad.

Under de kommande fem åren förväntas efterfrågan på hybridprofiler inom compliance och teknik att öka markant, drivet av trender som automatisering, skärpta regulatoriska krav och den växande betydelsen av cybersäkerhet. För att möta denna efterfrågan kommer nya strategier och utbildningsinitiativ att bli avgörande, inte bara för företag utan också för samhällens förmåga att hantera en digitaliserad och reglerad värld.

Hybridkompetensens roll i en digital era

Hybridkompetens inom compliance och teknik innebär en kombination av regulatorisk och teknisk expertis för att hantera komplexa regulatoriska krav och digitala utmaningar. På compliance-sidan krävs kunskap om till exempel regelverk som GDPR, MiFID II och AML, samt nya AI-relaterade bestämmelser såsom EU:s AI Act, som syftar till att reglera riskerna med automatiserade beslut.

Inom cybersäkerhet är efterlevnad av NIS 2-direktivet och ISO 27001 avgörande för att skydda digital infrastruktur, medan DSA och DMA sätter ramar för digitala plattformar och marknadsaktörer. Teknikkompetensen omfattar djupare kunskap och förståelse för cybersäkerhet, AI, dataskydd och automatiserade compliance-system, vilket gör denna hybridkompetens central för att navigera en alltmer digitaliserad och reglerad affärsmiljö.

”Hybridkompetens är inte längre en lyx, utan en nödvändighet.”

Sharp Recruitment & Consultants har över tio års erfarenhet av rekrytering och konsultuthyrning inom compliance. Vi genomför årligen cirka 200 rekryteringar, intervjuar runt 3 000 kandidater och har ett nätverk med omkring 400 konsulter.

Läs mer på:
www.sharprecruitment.se

Ett exempel är arbetet med AI-reglering. Tekniken har snabbt blivit en integrerad del av compliance-funktioner, men användningen av AI står inför stora juridiska och etiska utmaningar. Hur säkerställer man att framtidens AI-system som hanterar kunduppgifter efterlever exempelvis GDPR? Hur förhindrar man diskriminering i automatiserade beslut? Här krävs personer som inte bara kan tolka regelverk utan också förstå AI-modellers funktion och begränsningar på en teknisk nivå.

Ett annat område är cybersäkerhet. När cyberhoten blir allt mer sofistikerade, är det avgörande att ha compliance-kompetens för att hantera de regulatoriska konsekvenserna av dataintrång, samtidigt som man har teknisk förståelse för hur hoten uppstår och hur skydd kan implementeras. Kombinationen av dessa kunskaper är sällsynt, vilket gör rekryteringen av hybrida profiler till en central utmaning.

Utmaningar i kompetensförsörjningen

Traditionellt har områdena compliance och teknik behandlats separat, vilket har lett till en brist på yrkesverksamma med hybridkompetens. Samtidigt ställer arbetsmarknaden höga krav på kandidater, där både teknisk och compliance-relaterad erfarenhet ofta efterfrågas.
Företagen har ett stort ansvar att identifiera och stötta talanger som vill utveckla hybridkompetens. Genom vidareutbildning, mentorprogram och utmanande projekt kan organisationer skapa en miljö där medarbetare utvecklas inom båda områdena. Att aktivt arbeta med att behålla dessa talanger genom attraktiva karriärmöjligheter och stimulerande arbetsuppgifter är avgörande för långsiktig kompetensförsörjning.

Rekryterarens roll i att hitta hybridkompetens

En bra rekryterare kan spela en avgörande roll i att identifiera och attrahera talanger med hybridkompetens inom compliance och teknik genom att:
Förstå hybridkompetensens kärna – Ha djup kunskap om både compliance och teknik för att identifiera kandidater med rätt mix av kunskap och potential.
Proaktiv talangjakt & nätverkande – Använda branschspecifika nätverk, headhunting, sociala plattformar och delta i relevanta evenemang för att hitta rätt profiler.

Bedömning av överförbara kompetenser – Identifiera kandidater med en bakgrund inom antingen teknik eller compliance och bedöma deras potential att utveckla den andra kompetensen.

Utforma strategiska rekryteringsprocesser – Implementera case-intervjuer och tekniska tester för att säkerställa att rätt kompetens matchas med företagets behov.

Stödja företag i att behålla talanger – Ge insikter om marknadstrender, utvecklingsplaner och lönenivåer för att säkerställa långsiktig retention av hybridkompetenta medarbetare.

Konkurrensen om dessa talanger är global och intensiv, vilket ytterligare försvårar kompetensförsörjningen. Därför krävs fler utbildningsprogram, strategier och en aktiv roll från rekryterare för att utveckla hybridkompetens tidigt i karriären och stärka organisationers framtida kompetensförsörjning.

Framtidens framgång ligger i hybridkompetensen

Hybridkompetens inom compliance och teknik är inte längre en lyx, utan en nödvändighet i en värld där digitalisering och regulatoriska krav ständigt utvecklas. Företag som investerar i rätt strategier för kompetensförsörjning – genom rekrytering, vidareutbildning och talangutveckling – kommer att ha ett tydligt försprång.

För att lyckas krävs en långsiktig strategi där teknik och regelverk ses som två sidor av samma mynt, och där företag, rekryterare och utbildningsaktörer arbetar tillsammans för att säkerställa att framtidens arbetsmarknad har de hybridprofiler som behövs. De organisationer som tar detta på allvar kommer inte bara att uppfylla regulatoriska krav – de kommer också att stärka sin konkurrenskraft i en alltmer digital och komplex värld.



Här finns utbildningarna som stärker individen i compliancearbetet

Vad behöver egentligen en compliance officer kunna? Hur långt kommer man med att behärska regelverken?
– Compliance är det som händer mellan regelverk och individers beteende i en organisation. Därför behöver en compliance officer behärska många områden, men det kan vi lära de som kommer till oss, säger Viveka Strangert, compliance-expert.

Företagsuniversitetet erbjuder sedan några år tillbaka utbildningar som stärker den complianceansvarige i hela sin yrkesroll.

– Med våra utbildningar får man verktyg att navigera så att det blir både rätt och bra, säger Milica Milic, programansvarig.

Att compliancefunktionen blir allt viktigare i många företag beror bland annat på ökad reglering och kraftiga sanktioner. Det ställer nya krav på den som är compliance officer.

– Många behöver bli bättre på att förstå affären i sitt företag och att jobba proaktivt med riskhanteringen för att på så sätt bli ännu mer relevanta i sin organisation, säger Ingrid Harbo, ordförande för branschorganisationen Compliance Forum och föreläsare på Företagsuniversitetet.

Företagsuniversitetet erbjuder flera utbildningar inom complianceområdet, bland annat kurserna "Certifierad Compliance Officer" och "Hantering av compliancerisker".

– Förutom att man lär sig teorier rörande compliancemetod och specifika regelverk får man som deltagare praktiskt träna på olika situationer som en compliance officer kan hamna i. Dessutom ger utbildningarna en möjlighet att diskutera gemensamma utmaningar med andra inom compliance och man får ett bra tillfälle att bygga ett värdefullt nätverk, säger Viveka Strangert, som är en av utbildningens föreläsare.

Kursledarna har lång erfarenhet av compliance

Kursledarna är verksamma experter med gedigen praktisk erfarenhet av compliancefrågor i sina ordinarie yrkesroller. Under kurserna delar de med sig av sina erfarenheter.

– Målet är att bygga en inneboende säkerhet hos deltagarna och känsla för vad som är best practice så att de kan gå till styrelserummet med ännu mer trygghet i att det man säger är relevant och viktigt, avslutar Ingrid Harbo.

Om Företagsuniversitetet

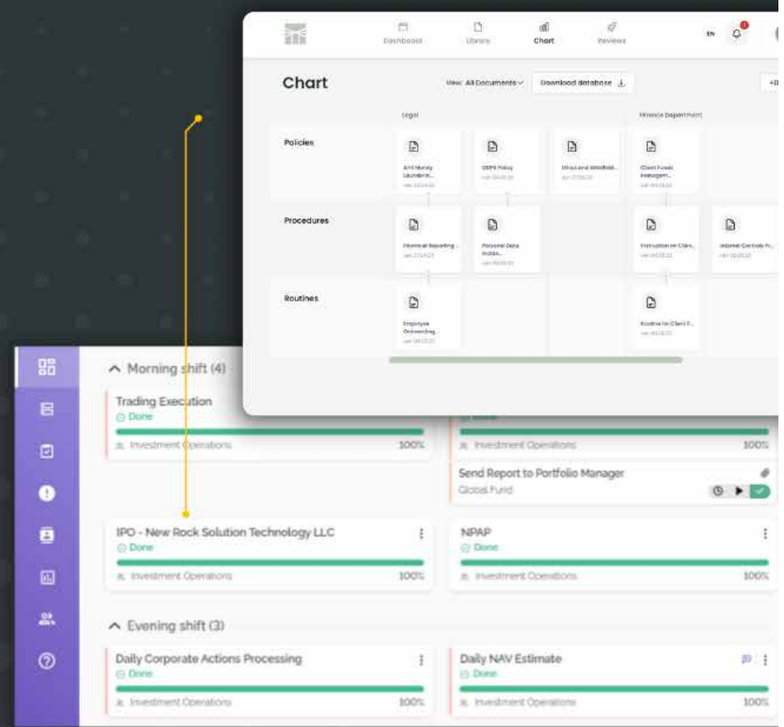
Företagsuniversitetet är ett av Sveriges ledande utbildningsföretag och har som mål att leverera utbildningar av högsta kvalitet, som ger praktiska och aktuella kunskaper att använda direkt efter kursen. Varje år välkomnar man runt 5000 kursdeltagare.

Läs mer på:
www.foretagsuniversitetet.se

NORTH HOUSE + Daymi

Transform How You Manage Compliance

Move from Policy to Execution with Confidence – Book a Demo now!



northhouse.se

daymi.co

Artikelförfattarna



Om Nils Oppelstrup:

Nils Oppelstrup ansvarar för affärsområdet Managed Services som stöttar kunder genom att ta över hela eller delar av det operativa arbetet mot penningtvätt, inklusive dokumentation, KYC, riskklassifi cering, screening och transaktionsmonitorering, utredningar och utbildning.
Bolaget Nils representerar heter Verifi ed och är är en ledande leverantör av helhetslösningar inom AML, e-sign och CLM i Europa



Om Rätt Nu - Marie Wallin

Rätt Nu AB grundades 2019 av juristen och tidigare kammaråklagaren Marie Wallin. Rätt Nu erbjuder specialistkompetens inom ämnena penningtvätt, förmögenhetsrätt, straffrätt och processrätt genom såväl utbildningar, skräddarsydda expertuppdrag som utgivning av böcker.
Marie utsågs 2024 till Årets Kredit Profi l av Svenska Kreditföreningen.

Agera mot penningtvättsrisker på riktigt

– då följer du också PTL

Vad är penningtvätt egentligen? Och räcker verkligen åtgärderna som krävs enligt PTL för att förhindra att en verksamhet utnyttjas? Att det går att bredda riskperspektivet blir uppenbart när Verifi ed och Rätt Nu utbyter erfarenheter kring de här frågorna. En bättre startpunkt än PenningTvättsLagen kan vara att utgå från kriminella metoder och brottsmanus när du vill skydda din verksamhet och förhindra penningtvätt.

De fl esta verksamhetsutövare som omfattas av PTL har god kännedom om vad som krävs i åtgärder enligt lagen och ungefär vad som kommer att granskas vid en eventuell tillsyn, men inte alltid hur helheten kring penningtvättsriskerna ser ut. Då det saknas gemensamma, tydliga och handfasta råd i Sverige i dag om hur AML-arbetet bör drivas skapar det inte sällan en känsla av osäkerhet. Även ambitiösa, kunniga företagsledare som investerar tid och resurser i AML-arbetet känner sig inte säkra på att det arbete de gör är tillräckligt bra. Så vad är egentligen 'tillräckligt bra'? I denna artikel ger vi några perspektiv på hur du som verksamhetsutövare kan komma dit.

1. Börja med de straffrättsliga riskerna

För att en verksamhet inte ska bli en del av ett kriminellt upplägg och de anställda inte heller ska riskera att begå brottet näringspenningtvätt med ett likgiltighetsuppsåt på jobbet gäller det att se över sin hantering av straffrättsliga risker. Ett första steg är att förstå vad brottet näringspenningtvätt handlar om och hur det kan begås. Det är ett brott som funnits i Sverige sedan 2014 och som handlar om att gärningspersonen agerat uppsåtligt med ett så kallat klandervärt risktagande. Översatt till PTL:s terminologi handlar det om att om en verksamhet brister i det riskbaserade förhållningssättet, till exempel inte gör en korrekt KYC-bedömning eller inte följer upp en misstänkt transaktion eller affärshändelse, så fi nns det även en straffrättslig konsekvens i brottet näringspenningtvätt.

2. Använd brottsmanus för att identifi era risker i din verksamhet

För att ha en chans att arbeta på rätt sätt med dessa frågor måste vi ”på den goda sidan” komma ihåg att de kriminella är kreativa. De ligger i framkant och är beredda att agera både kraftfullt och hänsynslöst för att hitta användningsområden för sina brottspengar. För att lyckas behöver de ofta agera tillsammans med, eller genom, aktörer inom det legala samhället. Som enskild aktör är det därför avgörande att ha kunskap om så kallade brottsmanus. Lämpliga frågor att ställa sig kring detta är:

- Hur ser det faktiska tillvägagångssättet ut för aktuella penningtvättsupplägg från de kriminellas håll?
- Vilka aktörer behöver de kriminella för just detta specifi ka upplägg?
- Hur kan min verksamhet utnyttjas?

För att kunna besvara dessa frågor behövs både straffrättslig kunskap och erfarenhet av kriminella metoder. En verksamhet behöver också orka se sig själv utifrån ett kriminellt perspektiv och förstå hur verksamheten kan användas för att begå brott.

3. Samla kunskapen i din allmänna riskbedömning

När du vet hur din verksamhet skulle kunna utnyttjas i ett kriminellt upplägg är nästa steg att gå till reglerna i PTL. Upprätta din allmänna riskbedömning så att den stämmer överens med de yttre hot och de inre sårbarheter som gäller för just dig. Att innehållet i din allmänna riskbedömning är av kvalitet och speglar din verksamhet och dina risker är helt avgörande för att du ska kunna lyckas med ett högkvalitativt och kostnadseffektivt AML-arbete. Det är ingen slump att de fl esta besluten om sanktionsavgift från till exempel länsstyrelsen pekar på brister i den allmänna riskbedömningen. Den utgör ju grunden, likt navet i ett cykelhjul, i allt efterföljande riskarbete. Den skall användas när du skapar processer för och agerar på alla identifi erade och nödvändiga motåtgärder. En allmän riskbedömning med kvalitet är en förutsättning för ett effektivt riskarbete. Den behövs för att veta vilka åtgärder som ska sättas in i din verksamhet. Ett riskbaserat förhållningssätt enligt PTL innebär inte att arbeta på samma sätt med alla tjänster som erbjuds. Att arbeta professionellt mot dina kunder i ett KYC-fl öde med exakt rätt frågor till rätt kund, sätta passande riskklasser för en tjänst som erbjuds, eller identifi era misstänkta mönster i transaktioner i en viss bransch. Inget av dessa exempel är möjliga utan att först ha gjort en bra riskbedömning.

Att skapa sin riskdokumentation utifrån kraven i PTL uppfattas av många som tungt och som en process vid sidan av det dagliga arbetet. Ett annat sätt att se på det är att det i allra högsta grad handlar om kärnan i din verksamhet och att du med stöd av PTL-processerna bygger ett skydd mot de kriminella pengarna. Det ger dig en möjlighet att se din affär från ett nytt perspektiv. Du bör veta vem du gör affärer med, och ingen kan din verksamhet bättre än du. Eller hur?

4. Ta hjälp av teknik där du kan – fokusera på de viktigaste besluten

Många verksamhetsutövare har tusentals kunder, erbjuder ett stort antal tjänster och underlättar hundratusentals transaktioner varje år. Kraven på insyn och övervakning kvarstår dock oavsett komplexitet. För att klara av att hålla en hög och jämn kvalitet behövs bra teknikstöd. Vissa steg är svåra eller inte tillåtna att automatisera, som att få in uppdaterad KYC-information från kunder, eller att fatta beslut om att godkänna en kundrelation med en viss riskfaktor. En heltäckande tekniklösning för AML kan dock underlätta arbetet signifi kant, och låta din tid gå till de viktigaste momenten och besluten. Ett perspektiv som är viktigt i valet av teknikleverantör är användarupplevelsen. Bland skall-krav, börkrav, features och pris är det lätt att tappa bort. Titta på helheten från användarnas ögon, eller med andra ord vad du och dina medarbetare ser och gör i och utanför systemen varje dag.

5. Samarbeta med partners som kompletterar dig

Utöver teknik behövs specifi ka kompetenser för att motarbeta penningtvätt. Spetskompetenser som är orimliga att anställa som litet eller medelstort bolag. Det fi nns dock hjälp att få på andra sätt. Att kartlägga vilka styrkor och brister just du har i din verksamhet, det senare ofta benämnt som ”sårbarheterna”, är avgörande för att du ska kunna förstå just ditt behov av extern kompetens. Något som är viktigt att tänka på är kontinuiteten i utförandet av uppdrag eller arbetsuppgifter som utförs av människor utanför din organisation. Försök att hitta människor och företag som kompletterar din verksamhet, och kan erbjuda ett uthålligt stöd vid behov, år efter år. Inget beslut kring arbetet mot penningtvätt är lika viktigt som vem du väljer att jobba med. Integritet, driv och en vilja att motarbeta kriminalitet är egenskaper som är av stor vikt hos dina medarbetare och partners.

Det är trots allt så vi effektivt motverkar penningtvätt och fi nansiell brottslighet: tillsammans.



Strategier för att hantera den nya regulatoriska komplexiteten

Den nya regulatoriska verkligheten ställer nya krav

Medan vissa reglerade branscher, såsom tex finansiell sektor, är vana vid omfattande regleringar och ofta har stora interna apparater för att hanteras regler som en naturlig del av sin verksamhet, har bolag i traditionellt sett mindre reglerade branscher under de senaste åren behövt vänja sig vid en helt ny regulatorisk verklighet som markant förändrat spelplanen, med allt mer generellt tillämpliga regleringar.

De nya regulatoriska kraven, och inte minst regleringspaketen från EU, är omfattande och komplexa i bemärkelsen att de ofta är svåra att tolka rent juridiskt, allt eftersom en föränderlig värld kräver alltmer principbaserade regler och ramverk snarare än detaljreglering.

Men de nya regleringarna skapar också stora utmaningar för organisationer utifrån governance-perspektivet. Vem ansvarar egentligen för vad och hur ska roller och ansvar allokeras och styrning ske? Många av de nya regelverken, såsom AI-förordningen, Dataförordningen, ESG-regelverken och den nya cybersäkerhetsregleringen – är breda i sin tillämpning. De påverkar inte sällan stora delar av organisationens strukturer, processer och arbetssätt. Detta gör det svårt att allokera ett tydligt ansvar internt, både vad gäller implementationsprojekten - där nya regelverk tolkas och förändringsplaner formuleras - och i fråga om ansvaret operativt i den löpande verksamheten där regelefterlevnad ska säkerställas.

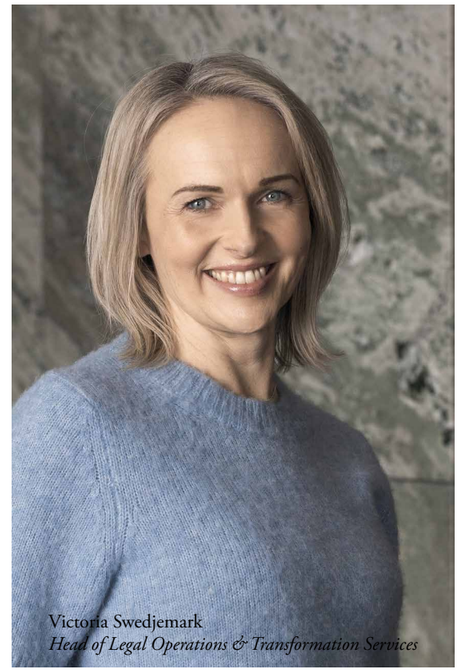
Organisationer behöver ha en plan för hur risker för otydlighet kring ansvar bör hanteras, så att saker inte faller mellan stolarna. Ett relevant synsätt här är att tänka att regleringarna är allas ansvar, eller i alla fall ett tydligt tvärfunktionellt ansvar och att det krävs ett strukturerat samarbete, där alla behöver hitta en relevant roll och samverka.

Svårt i decentraliserade organisationer

Särskilt utmanande blir det i stora, internationella och kraftigt decentraliserade organisationer, där man är van vid att hantera olika typer av frågeställningar lokalt ute i affärsområden, regioner eller dotterbolag - när de nya regleringarna ofta slår över hela verksamheten, tvärs över sådana organisatoriska silos. Om regleringarna då ska hanteras i varje sådan del av verksamheten separat blir det inte bara suboptimalt med risk för dubbelarbete och resursslöseri utan också ofta inkonsekvent, med olika tolkningar och tillämpningar inom olika delar av verksamheten. Det blir också svårt att överblicka den koncernövergripande riskbilden. Vidare försvåras hanteringen av regelverksfrågor i internationella



Theodor Forsberg
KPMG Compliance Consulting



Victoria Swedjemark
Head of Legal Operations & Transformation Services

organisationer verksamma i flera jurisdiktioner av att olika länder eller regioner har olika regleringar inom ett och samma område, t.ex. vad gäller AI, dataskydd eller ESG, vilket ställer krav på olika hantering i olika delar av verksamheten.
Riskerna som detta medför ökar också i takt med att de nya regleringarna ålägger organisationer allt högre monetära sanktioner vid regelbrott och mer långtgående ansvar för ledande befattningshavare. Det blir ofta svårt för högsta ledningen och huvudkontoret att på ett effektivt sätt överblicka och känna trygghet kring regelefterlevnaden inom organisationen i stort. Dessa utmaningar behöver hanteras.

Krävs effektiv samverkan, organisering och resurssättning

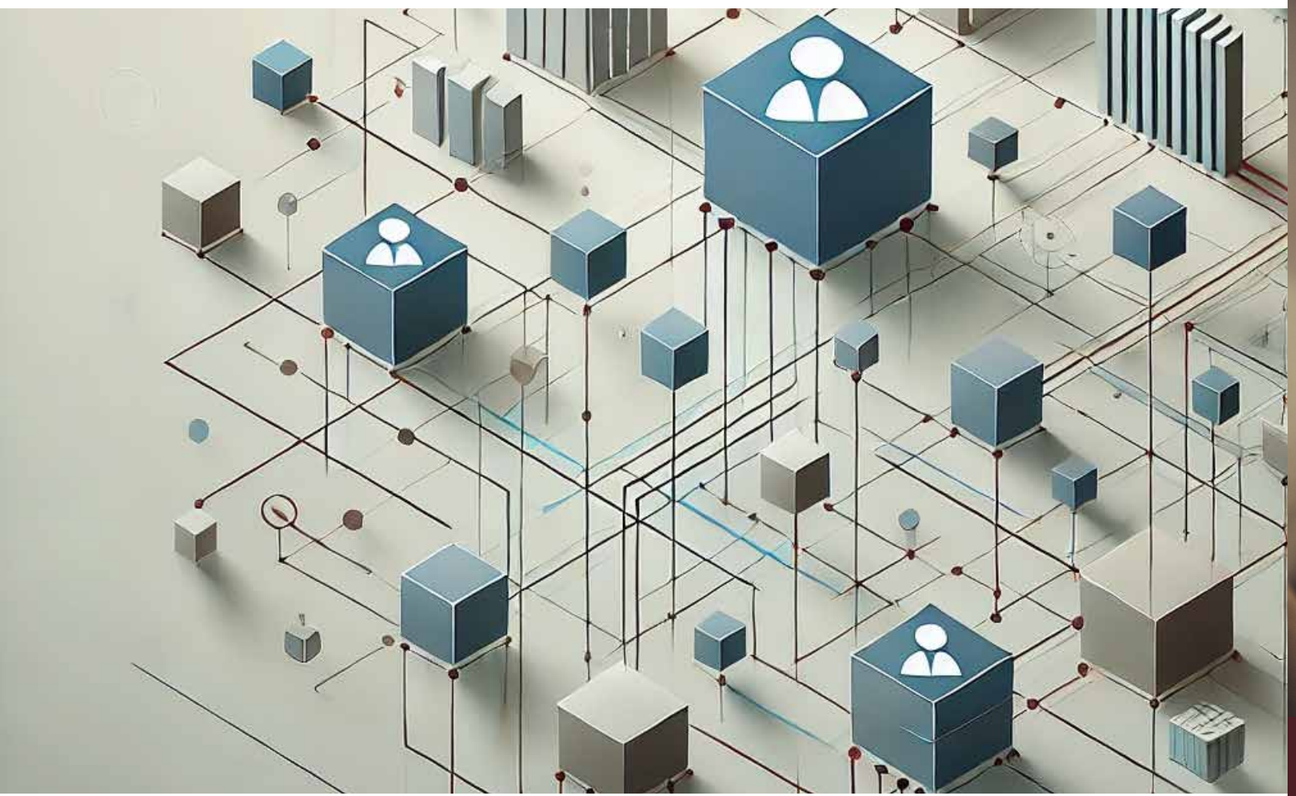
Här finns det ofta skäl att se över den interna förmågan att hantera just regulatoriska projekt och program. De nya kraven föranleder ofta behov av mer resurser till regulatoriska arbete, eller att se över organiseringen av det regulatoriska arbetet, t.ex. fördelningen av resurser och arbete på central nivå i relation till decentraliserad hantering. Även resurssättningsmodellerna kan behöva ses över. En modell är att bygga upp t.ex. ett centralt Project Management Office, med syfte att just designa och bemanna upp regleringsprojekt inom koncernen effektivt, tex kopplat till AI-förordningen eller ESG-området. En sådan central hub kan ha som uppgift att beakta både huvudkontorsperspektivet och perspektiv från affärsområden, regioner och dotterbolag och att säkerställa att relevant intern samordning sker och uppföljning sker. En sådan central projektledningsresurs kan också ta in relevant externt stöd - kring juridisk analys, projekt- eller programdesign eller planering, eller implementeringen för ökad kostnadseffektivitet och för att säkra upp en bra förändringsledning och en hållbar operationalisering.

En sådan central hub kan ta rollen som ett Center of Exellence där kompetens och relevanta resurser kring vissa regleringsområden samlas och vid behov kan nyttjas för eller allokeras ut inom organisationen. Detta kan också utgöra en del av kompetensförsörjningsstrategin, i en tid där intern kompetens inom centrala regleringsområden blivit allt viktigare att säkra upp och utveckla över tid. Här finns också anledning att analysera vilka kompetenser som är relevanta att ha internt och vilka kompetenser som behöver säkras upp från externa parter.

Som ett minimum behöver man etablera former för samverkan över organisatoriska silos kopplat till regleringsområdena, t.ex. kommittéer eller arbetsgrupper, för att utbyta kunskap och erfarenheter och linjera kring juridiska tolkningar och risktolerans och fånga kollektiv kunskap och underlätta delning av juridiska analyser, best practices, och olika dokument och verktyg som är relevanta för flera delar av verksamheten.
Här kan det också finnas skäl att öka graden av standardisering över hela verksamheten, och besluta om vissa gemensamma teknologiinvesteringar. Även enhetlig och sammanhållen rapportering kopplad till compliance är ofta värdeskapande, liksom att öka förmågan till gemensam eller samlad dataanalys inom compliance-området.

Krävs en professionalisering av compliance-arbetet över hela livscykeln

Den strida strömmen av nya regleringar gör det allt svårare för organisationer att följa med i utvecklingen. Vad är på gång, vad är relevant för oss (och på vilket sätt) och hur förbereder vi oss och anpassar vi oss? Här behövs en organisatorisk förmåga att på ett effektivt sätt scanna horisonten vad gäller kommande regleringar, eftersom en ostrukturerad eller summarisk bevakning lätt leder till att viktiga regulatoriska krav missas eller upptäcks för sent. Givet hur regelförslag kan förändras



över den regulatoriska beslutsprocessen behöver denna bevakning och analys också vara agil. Även här kan det vara relevant att ta ställning till om denna bevakning ska byggas upp centralt, för att stödja organisationen brett, eller om olika delar av organisationen ska hantera detta var för sig, respektive om denna förmåga ska byggas internt eller ska outsourcas.

Denna fas, bevakningen, är första steget i compliance-livscykeln, och den följs av regulatorisk förändringsledning, alltså förmågan att identifiera relevanta förändringsbehov och lyckas verkställa dessa. Här blir tvärfunktionella eller centralt samordnade initiativ som nämns ovan centrala. I nästa fas av livscykeln krävs en effektiv operationalisering av compliance-arbetet, så att man i verksamheten löpande säkerställer att processer, system och beteenden stödjer att reglerna också följs. Även här krävs en effektiv governance-modell internt som säkerställer att roller och ansvar för regelefterlevnad i den löpande verksamheten är tydliga. Och avslutningsvis behöver man säkerställa en väl fungerande löpande uppföljning, mätning och monitorering av regelefterlevnaden.

Fokus på Compliance operations och investeringar i teknologi blir allt viktigare

Allt fler organisationer ökar sitt fokus på att professionalisera och utveckla sitt compliance-arbete utifrån dessa olika aspekter, över hela hela compliance-livscykeln. Här krävs också ökade investeringar i, compliance operations och teknologi (s.k. compliance tech eller reg tech) för att understödja arbetet. Det har blivit allt svårare att säkerställa regelefterlevnad utan ett sådant strukturerat arbete och ett sådant teknologistöd. Det kan också krävas mer insamling och analys av data för att känna sig tillräckligt trygg med att regler följs.

De allra mest progressiva organisationerna bygger nu upp förmågor att med hjälp av AI och automatisering realtidsmonitorera sin regelefterlevnad, eller resilienstesta sitt compliance-program och exempelvis föreslå förbättringar i interna kontroller eller flagga compliancerisker proaktivt. Många jobbar också strukturerat med att brett identifiera och realisera relevanta tillämpningar (s.k. use cases) för AI inom compliance-området, t.ex. policy chatbots, att använda AI i policy managment- eller whistleblowingprocesserna eller för t.ex. regulatorisk monitorering.

Här finns en möjlighet för organisationer att bygga konkurrensfördelar genom att bli bättre på att anpassa sig till nya regelverk, lyckas med tvärfunktionell samverkan och effektiv governance och operationalisera sin regelefterlevnad. Särskilt kan konkurrensfördelar skapas om dessa förmågor dessutom kan hjälpa organisationen att också ta vara på affärsmöjligheter som de nya regelverken skapar, alltså vara opportunistiska och inte bara defensiva.

Ett sätt att identifiera vilka förbättringsområden som är mest relevanta för den egna organisationen kan vara att göra en mognadsanalys (s.k. maturity assessment) eller gap-analys (mot best practice) av sitt compliance-arbete eller sitt compliance-program, och också öka sin förståelse för vad de mest framstående organisationerna gör inom detta område. Och det kan vara hög tid att börja bygga business caset för de investeringar som kan vara nödvändiga för att optimera organisationen, samverkansmodeller och operations.,





Det är kanske dags för en tydlig definition av compliancerollen

Ola Sundborg tog i höstas emot priset Årets Complianceperson på CMC-galan. Han har lång erfarenhet av compliance, och har arbetat i branschen sedan området började växa fram i Sverige. Compliancenytt träffade Ola för att diskutera utmaningar i branschen, rekrytering, och behovet av en tydlig definition av rollen.

”Vi såg mycket av detta för några år sedan, när compliance blev allt viktigare att ha på plats. Då panikrekryterade man enorma avdelningar på många finansiella institut.”

Ola Sundborg är född och uppvuxen på västkusten, men flyttade efter sin examen till Stockholm för att jobba på advokatbyrån Lagerlöf och Leman (numera Linklaters). Redan efter ett par år fick han upp intresset för de regulatoriska krav som fanns mot finansbranschen, och när han bytte jobb 2004 för att gå till en aktiemäklarfirma blev han officiellt anställd som compliance officer.

– Det var ungefär under den tiden som compliance började ta fart även här i Sverige. Jag gick sedan vidare till Danske Bank där jag senare blev Compliancechef för den svenska verksamheten, även om det fortfarande inte var helt utkristalliserat vad den rollen innebar. Jag har helt enkelt varit med sedan starten, och sett compliance växa fram som område.

Sedan 2014 har Ola varit på Carnegie, där han idag är Compliancechef, och ansvarar för teamet på fyra compliance officers i Sverige och ytterligare fem i övriga länder där Carnegie är verksamt. Ola har en tydlig vision av vad han vill att compliancearbetet ska vara, och menar att de stora avdelningarna aldrig tilltalat honom.

– Jag tror det handlar om hur man definierar compliancerollen, vilket verkligen kan skilja från företag till företag. Jag har alltid sett compliancefunktionens uppdrag som en central kontrollfunktion för ledningen. Vi ska rita riskkartan, och bistå beslutsfattarna i beslut kopplade till riskfrågor.

På Carnegie berättar Ola att man har avdelningar som till exempel enbart arbetar med AML-frågor, men dessa kallas inte compliance officers. Han tycker att det är fördelaktigt att delegera regelefterlevnadsfrågor till specifika personer som arbetar närmare affären. Detta tillåter i sin tur att compliancefunktionen kan arbeta närmare och mer koncentrerat med ledningen. På så sätt kan man hålla sin compliancefunktion smal, samtidigt som compliancearbetet blir mer utbrett och integrerat i organisationen.

– Jag tror att en tydlig definition av compliancefunktionen är nyckeln till att lösa många av de problem vi ser idag. Ordet compliance har en förmåga att bli väldigt generellt. Det behöver finnas en tydlig distinktion av vad som är compliancearbete, d v s regelefterlevnad, och vad som är compliancefunktionens arbete och ansvarsområden. Compliancearbete är enligt mig någonting som behöver finnas i hela organisationen, medan compliancefunktionen arbetar närmare ledning och omvärldsbevakar.

En utmaning med compliance är enligt Ola om ledningen inte helt och hållet förstår vad compliance är, eller vilka ansvarsområden som ska ligga på rollen. Då riskerar man att rollen blir för bred, vilket kan bidra till att för mycket ansvar läggs på ett fåtal personer, eller tvinga avdelningen att växa och bli enorm.

– Vi såg mycket av detta för några år sedan, när compliance blev allt viktigare att ha på plats. Då panikrekryterade man enorma avdelningar på många finansiella institut. Detta har lett till att vi har många juniora complianceofficers som ofta får för mycket ansvar på sig, samtidigt som mer erfaren kompetens är svår att rekrytera.

Personer som Ola, med lång erfarenhet av compliance, är få och svåra att rekrytera. Det leder till en brist på erfaren kompetens med ett brett och utvecklat perspektiv inom branschen. Ola menar att en god förståelse av compliance är en fingertoppskänsla som utvecklas över tid. För att kunna locka den här typen av kompetens tror han att man behöver kunna erbjuda mer än en hög lön. Det som verkligen lockar den erfarna kompetensen är ett uppdrag nära ledningen, där arbetsuppgifterna är övergripande och varierade.

På frågan om vad som utmärker en riktigt bra complianceperson ger Ola ett antal exempel. Han menar att mycket handlar om förtroende, och en god kommunikationsförmåga.

– Jag brukar säga att man behöver vara tydlig, påläst och trevlig. Som Compliance måste man ha en bra samarbetsförmåga, och tydligt kunna kommunicera risker. Man måste vara beredd att leda i dessa frågor, och inte vela för mycket fram och tillbaka. Även om compliance är ett rådgivande organ måste man helt enkelt våga peka med hela handen ibland, och vara beredd på att bli testad av ledning eller andra avdelningar. Där kommer delen om att vara påläst in. Du ska kunna motivera varför en viss åtgärd behövs, och visa att du förstår riskerna. Compliance är inte någonting för enstöringar. Utöver att vara påläst måste du också kunna vara social och trevlig, så att folk vågar vända sig till dig med frågor eller osäkerheter. Att välja sina strider är också viktigt. Vissa åtgärder är viktigare än andra, och man behöver kunna samarbeta med resten av organisationen för att hitta en lösning som är hållbar för alla. Det här är helt enkelt ett komplext yrke, där ingenting är svart eller vitt.





EU:s Due Diligence Directive:
Lättnader och företagens ansvar

Som en konsekvens av EU-kommissionens föreslagna ”omnibuspaket” har vissa lättnader föreslagits i EU:s hållbarhetsdirektiv i syfte att minska den regulatoriska bördan. Stora företags ansvar för att upptäcka, förhindra och åtgärda överträdelser av mänskliga rättigheter och internationella miljökonventioner i den egna koncernen och i leverantörers verksamhet kvarstår dock. Vissa administrativt betungande delar av regelverket och den indirekta regulatoriska bördan på mindre företag är dock tänkt att minska. skriver advokaterna Jenny Welander Wadström och Andreas Hallbeck.

I juli 2024 antogs EU-direktivet Corporate Sustainability Due Diligence Directive (ofta förkortat ”CSDDD” eller ”CS3D”). Efter en översyn av hur CS3D och andra EU-direktiv på hållbarhetsområdet ökar den regulatoriska bördan på företag, och därmed hämmar EU:s konkurrenskraft, presenterade EU-kommissionen den 26 februari sitt ”omnibuspaket” med förslag på lättnader i regelverken. Bland annat föreslogs vissa lättnader i CS3D.

CS3D har tröskelvärden som innebär att enbart stora företag träffas direkt av direktivets skyldigheter. Det handlar om företag med säte i EU med över 1000 anställda och en global nettoomsättning om minst 450 miljoner euro på koncernnivå men också företag med säte utanför EU med en nettoomsättning inom EU om minst 450 miljoner euro på koncernnivå.

Kärnan i CS3D handlar om att dessa företag ska införa processer för att upptäcka överträdelser av mänskliga rättigheter och internationell miljölagstiftning i sin egen, sina dotterbolags och sina leverantörers verksamheter. Företagen förväntas också arbeta förebyggande med att förhindra överträdelser och att ha en beredskap för att hantera och åtgärda sådana överträdelser när de upptäcks.



Företagen förväntas inte garantera att överträdelser aldrig kommer att inträffa, utan det som krävs är att det finns processer och åtgärdsplaner på plats som är anpassade utifrån risknivån för den relevanta verksamheten och de geografiska marknader där denna bedrivs eller där leverantörer finns. Bristande efterlevnad av kraven kan föranleda sanktionsavgifter och även innebära skadeståndsskyldighet mot andra parter.

Tidsplanen för implementeringen av CS3D i nationell lagstiftning ska enligt omnibusförslaget skjutas upp från 2026 till 2027 och kraven föreslås träda i kraft 2028. EU-kommissionen föreslås komma med vägledande riktlinjer för hur kraven ska kunna efterlevas redan år 2026. Dessa förslag kan sammantaget öka rättssäkerheten och förutsebarheten då företagen ges mer tid att med stöd av EU-kommissionens riktlinjer sätta korrekta processer på plats.

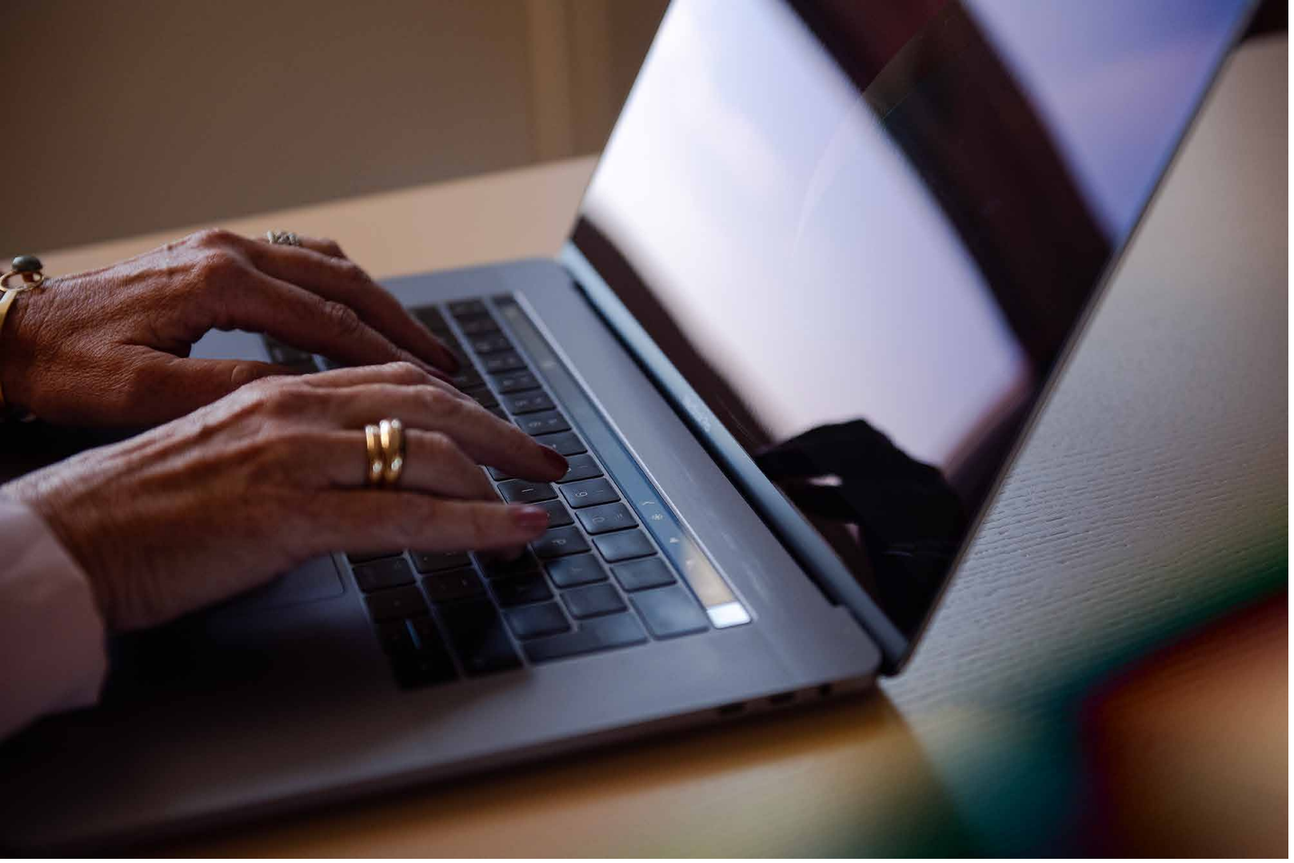
En lättnad som föreslås handlar om due diligence-kraven avseende leverantörsleden. Direktivet innebär långtgående undersökningsskyldigheter (”due diligence”) av leverantörers verksamhet. Detta kan bli särskilt utmanande att leva upp till med hänsyn till begränsade möjligheter till kontroll och insyn, särskilt vid komplexa underleverantörskedjor och leverantörer i andra länder. Enligt omnibusförslaget ska denna skyldighet som utgångspunkt enbart omfatta direkta leverantörer och inte underleverantörer. En skyldighet att granska underleverantörer ska dock, enligt omnibusförslaget, inträda så snart ett stort företag har information som gör det ”plausibelt” – en ganska låg tröskel av sannolikhet – att överträdelser av mänskliga rättigheter eller brott mot internationell miljölagstiftning sker i underleverantörsled.

En del av omnibusförslaget syftar till att begränsa administrativt betungande utvärderingar för stora företag och den indirekt ökade regulatoriska bördan för mindre företag. De stora företag som träffas av CS3D ska löpande utvärdera sina processer. Men enligt omnibusförslaget behöver detta enbart ske vart femte år istället för varje år som CS3D ursprungligen krävde. En utvärdering måste dock alltid ske när existerande processer kan bedömas vara otillräckliga eller nya omständigheter motiverar en sådan utvärdering, såsom vid företagsförvärv, ändrad affärsinriktning eller inträde på en ny marknad. Detta möjliggör för företagen att fokusera på due diligence och relevanta åtgärder istället för på årliga administrativt betungande utvärderingar av processerna.

Dessutom minskar den regulatoriska bördan på mindre företag indirekt genom att större företag inte med samma regelbundenhet som en del av sina utvärderingar behöver efterfråga information från sina leverantörer. Den minskar också genom att omnibusdirektivet inför begränsningar av hur mycket information större företag som en del av sina due diligence-processer och utvärderingar av sina processer har rätt att efterfråga från mindre företag med färre än 500 anställda.

Avslutningsvis noteras att antikorruptionsarbete sannolikt blir en viktig del i företagens arbete för att efterleva kraven i CS3D. Även om CS3D tar sikte på överträdelser av mänskliga rättigheter och miljökrav noteras i direktivet att korruption och mutor kan hänga ihop med sådana överträdelser samt att det *”kan bli nödvändigt för företag* [i sina due diligence-processer] *att ta hänsyn till dessa faktorer”*. Antikorruptionsarbete såsom due diligence av riskerna för korruption i sina leverantörsled, och interna kontroller för att förhindra mutor, kan vara avgörande för att relevanta due diligence-processer och åtgärdsplaner ska få avsedd effekt. Utan dessa delar kan uppförandekoder som leverantörer åtar sig att efterleva bli verkningslösa, ifall leverantörer låter sig mutas för att intyga och eventuellt med falska underlag bekräfta efterlevnad, eller mutar underleverantörer i syfte att undanhålla information om överträdelser. Det återstår att se om EU-kommissionens i sina vägledande riktlinjer som väntas 2026 ger några förtydliganden avseende vilket antikorruptionsarbete som kan krävas för att efterleva kraven i CS3D.

Jenny Welander Wadström, *advokat och Partner på Roschier Advokatbyrå*
Andreas Hallbeck, *advokat och Senior Associate på Roschier Advokatbyrå*



Realtidsövervakning kan vara nyckeln till att stoppa den kriminella ekonomin

Niklas Rosvall är Chief Product Officer på Trapets, ett regtech-företag som levererar övervakningssystem till banker och finansiella institutioner för att upptäcka och förebygga finansiell brottslighet. Vi träffas för att diskutera realtidsövervakning, och hur metoden kan sätta rejäla kuggar i hjulen för hur kriminella aktörer finansierar sin verksamhet.

Niklas har en lång bakgrund inom fintech- och andra SaaS-bolag som verkar under regelverk, med roller på tunga bolag som HR-portalen Benify och betalföretaget Worldline. Idag är han CPO på Trapets, och agerar länk mellan produktutveckling, marknadsföring och försäljning. Han beskriver ett skifte i synen på compliance under sin karriär - från att enbart vara en regelefterlevnadsfråga till att bli en viktig del av hur företag förebygger brottslighet.

– Mycket av det vi gör på Trapets handlar om att hjälpa våra kunder att möta både finansiella regelverk och samhällstrender, trender som idag tyvärr ökar behovet av bättre och effektivare brottsförebyggande verktyg.

Realtidsövervakning och dess betydelse

Realtidsövervakning är, som det låter, ett system som möjliggör att banker och andra finansiella institutioner kontinuerligt analyserar transaktioner i realtid. Niklas berättar att man hittills ofta har skickat in transaktionsdata för monitorering i större batcher, ibland endast en gång per dag. Detta innebar att en misstänkt transaktion ofta inte upptäcks förrän efter flera timmar, eller dagen efter att den skett, vilket är mycket tid när det kommer till bedrägerier.

– Nyckeln till att hinna stoppa ett bedrägeri är att upptäcka det i tid. Det har historiskt sett varit svårt med de äldre systemen, men realtidsövervakningen innebär ett stort genombrott på området. Det innebär att man nu kan agera direkt på misstankar, och minimera eller eliminera skadan. Vid misstänkt penningtvätt kan man till exempel frysa kundens konto medan man utreder ett misstänkt ärende. Detta möjliggör effektivare bekämpning av penningtvätt och bedrägeriförsök än den traditionella monitoreringen, där syftet främst varit att rapportera misstänkt olaglig hantering av pengar. Idag kan vi göra mer än så, och faktiskt stoppa misstänkta transaktioner innan de genomförs.



"Jag tycker att det finns fler poänger med att implementera realtidsövervakning än enbart att följa regelverk, även om det såklart är en stor del. För mig handlar det om att ta sitt samhällsansvar, gentemot samhället i stort och mot sina kunder."

- Niklas Rosvall

Hur Trapets realtidsövervakning fungerar

Trapets realtidsövervakning bygger på två fundamentala steg. Det första är en allmän riskbedömning som görs i samband med att en person eller företag blir kund till en bank eller annan finansiell institution. Man gör bland annat inhämtning av allmän kundkännedom genom frågeformulär, samt en screening av kunden mot sanktionslistor. Den andra är analysen av mönster i personens transaktioner. Utöver att etablera mönster för hur personen vanligtvis hanterar sina pengar, görs även screening av motparten för varje enskild transaktion. Skulle personens transaktioner avvika mot kundkännedom och tidigare analyser går ett larm.

– De kriminella vet ofta vad som kommer att ge utslag i en klassisk monitorering, och det är inte ovanligt att de testar nya metoder för att försöka kringgå detta. Till exempel kan de börja föra över pengar i mindre belopp, för att inte dra uppmärksamhet till transaktionen. Det är därför viktigt att man screenar varje enskild transaktion, oavsett hur obetydlig den är.

Utmaningar och framtida krav

När de kriminella försöker få ut svarta pengar från banken kan det vara för att antingen ta ut för egen vinning, eller för att skicka till sanktionerade personer eller bolag utomlands. Den ökande hastigheten och digitaliseringen av den organiserade brottsligheten innebär att övervakningen också behöver bli snabbare.

– Vi ser redan flera regulatoriska krav på horisonten som troligtvis kommer tvinga fram den här typen av monitorering. Myndigheter som EBA (European Banking Authority) har redan uppmanat till att implementera realtidsövervakning där risker identifierats. Även utvecklingen av regelverk som penningtvättsdirektiven och betaltjänstdirektiven verkar peka åt samma håll, nämligen att fördröjningar inte kommer vara acceptabla i framtiden. Finansiella institut kommer troligtvis åläggas att ta detta på allt större allvar.

Niklas lyfter även att en brett implementerad praxis av realtidsövervakning skulle kunna ha en avskräckande effekt. Man har sett att de kriminella tenderar att följa minsta motståndets lag när det gäller finansiell brottslighet, och om tillräckligt många försök att använda bankkonton i deras kriminella upplägg stoppas kommer det helt enkelt inte längre vara lönsamt för dem att fortsätta.

– Jag tycker att det finns fler poänger med att implementera realtidsövervakning än enbart att följa regelverk, även om det såklart är en stor del. För mig handlar det om att ta sitt samhällsansvar, gentemot samhället i stort och mot sina kunder. I framtiden, i ännu större utsträckning än idag, kommer kunder värdesätta en bank som tar deras säkerhet på stort allvar.

Niklas vittnar om att flera av de företag som infört en process för realtidsövervakning har lyckats stoppa en mängd misstänkt olagliga transaktioner. Ett typiskt exempel är att en transaktion stoppas då det vid screening mot sanktionslistor visar sig att mottagaren är en person eller ett företag med kopplingar till exempelvis den ryska regimen eller en terrorstämplad organisation.

Så vilka är utmaningarna?

Niklas säger att det som kan vara ett hinder för många kunder är att det kan vara komplicerat att integrera realtidsövervakningen med systemet som banken använder till sina transaktioner. Det är bland annat detta Trapets hjälper företag med. En annan utmaning är mer operativ, menar Niklas. Avdelningen som ska handlägga alla dessa larm bör få mandaten och kompetensen att kunna stå på egna ben, för att ytterligare snabba på arbetet.

– Man behöver kunna fatta snabba beslut utan att det kräver godkännande av en annan funktion. Konsumenterna kommer inte acceptera att det tar dagar innan en transaktion eller kontoansökan godkänns, så handläggningen av ärenden måste ske inom minuter. I förlängningen innebär det att det behövs en mer autonom AML-avdelning, som kan strategiska avvägningar och fatta policybeslut själva. Om de effektivt ska kunna bidra till bekämpningen av den accelererande finansiella brottsligheten, så behövs en kompetensutveckling och en självständighet som ger compliance-teamen den status som detta viktiga yrke förtjänar, avslutar Niklas.



Compliancefunktionens roll i arbetet med DORA

Dora-förordningen (DORA) började att tillämpas den 17 januari i år och omfattar nästan alla finansiella företag som står under Finansinspektionens tillsyn. DORA ställer höga krav på att dessa företag har kontroll över sina IKT-risker. Det innebär bland annat att företagen måste ha tillräckliga processer, system och styrdokument på plats för att kunna hantera IKT-risker i verksamheten. Vid implementeringen av nya och så omfattande regelverk som DORA har compliancefunktionen hos finansiella företag ofta en stor roll i att kvalitetssäkra implementeringen. Utöver det kan funktionen även ha en stöttande roll för verksamheten vid efterlevnaden av DORA.

Vad bör compliancefunktionen hantera i förhållande till DORA?

För många finansiella företag är det en självklarhet att compliancefunktionen ska arbeta med DORA på ett eller annat sätt. Hur arbetet ska se ut är däremot inte alltid lika självklart. Det finns därmed en del frågor som företagen behöver ta ställning till för att compliancefunktionen ska kunna göra som mest nytta på det här området.

DORA-regelverket är stort och omfattande och det är inte rimligt att utgå från att en av kontrollfunktionerna i företaget, till exempel compliance eller risk, ensamt ska ta sig an det. En bra utgångpunkt är därför att reda ut vilka avgränsningar som behöver göras mellan compliancefunktionen och övriga kontrollfunktioner inom företaget på det här området. Ett naturligt led i compliancefunktionens uppdrag kan vara att inkludera de delar av DORA som rör företagsstyrning inom IKT-området. Compliance kan då ansvara för regelefterlevnadsrisker kopplade till exempelvis styrdokument, outsourcing och hantering av IKT-tjänsteleverantörer, som regleras i DORA. Vilka specifika delar av DORA som compliancefunktionen ska ta ansvar för kan naturligtvis hanteras på olika sätt, beroende på hur verksamheten är organiserad och hur omfattande den är. En utgångspunkt i det sammanhanget bör vara att verksamheten åtminstone har en tydlig linje mellan operativa risker och regelefterlevnadsrisker.





Författare: Johannes Spansk och Johanna Borg, Kompass Advokat.

Många företag har redan gjort liknande avvägningar i samband med sitt arbete med till exempel GDPR och Eiopas IKT-riktlinjer. Om dessa avvägningar har lett till ett väl fungerande resultat kan företaget ta med sig det i arbetet även med DORA.

I arbetet med granskningar och kontrollaktiviteter med anledning av DORA kan det vara klokt att överväga ett samarbete mellan compliance och övriga kontrollfunktioner i företaget (s k combined assurances). Ta i sådant fall hjälp av övriga kontrollfunktioner och diskutera vilken funktion som tittar på vad, för att få med hela regelverket och för att undvika överlappningar i funktionernas granskningar. På så sätt blir även gränsdragningen mellan kontrollfunktionernas arbete tydlig. För compliancefunktionen kan det innebära att tillsammans med internrevisionsfunktionen, som har ett utpekat ansvar enligt DORA, göra upp en plan för kommande DORA-granskningar eller andra aktiviteter. Eftersom DORA-regelverket är nytt kan det hos verksamheten finnas ett behov av, och vara välkommet att, kontrollfunktionerna gör kontroller och granskningar av hur regelverket har implementerats och efterlevs. Trots det är det även viktigt att ta hänsyn till eventuellt kvarvarande och pågående implementeringsarbete vid de granskningar som görs. Det är inte alltid som mest effektivt för compliancefunktionen att genomföra en granskning under en pågående implementeringsprocess. Det kan i vissa fall leda till att verksamheten behöver lägga fokus på granskningen i stället för att arbeta vidare med implementeringen och att compliance inte får ut några resultat som kan leda till förbättringar. Ibland kan det därför vara en bra lösning att sprida ut granskningsaktiviteterna över en längre period på ett till två år, om vissa delar av implementeringen eller organisationen inte är mogna för kontroller.

Compliancefunktionen har även en viktig roll i att ge råd och stöd till verksamheten samt till VD och styrelse. Denna del av compliancefunktionens uppdrag får extra betydelse i arbetet med DORA, då det finns uttryckliga krav på att bland andra styrelsen ska ha tillräcklig kunskap om regelverket och då det följer ett särskilt ansvar för styrelsen vid överträdelser av förordningen. Informationsinsatser och utbildning inom det här området kan därför behöva prioriteras av compliancefunktionen under de närmsta åren.

Det är också viktigt att compliancefunktionen redan nu arbetar för att få tillräckligt med resurser från ledningen, det vill säga både från VD och från styrelsen. DORA har nu börjat att tillämpas och flera delar av reglerna kommer att ha en märkbar effekt på verksamheten redan i år. Här kan compliancefunktionen redan nu se över om det till exempel planeras för DORA-granskningar framöver som kommer att ta mycket tid i anspråk, för att utvärdera behovet av resurser eller omprioriteringar.

Varför är DORA-compliance viktigt?

Att inte följa DORA kan bli kostsamt för företaget på flera sätt. Det kan dels leda till sanktionsavgifter både för företaget och för enskilda styrelseledamöter, dels innebära att det faktiskt finns säkerhetsbrister i verksamheten och ut mot företagets kunder, som kunde ha undvikits om regelverket hade efterlevts. Vi får inte glömma att DORA i första hand syftar till att i så stor utsträckning som möjligt höja cybersäkerheten och motverka att risker kopplade till IKT förverkligas. Om det uppstår stora störningar eller andra problem kopplade till IKT kan det naturligtvis, utöver praktiska problem, i sin tur leda till ett förlorat förtroende avseende företagens digitala miljö och en risk för kundflykt. DORA-compliance handlar därför inte bara om att uppfylla de krav som förordningen ställer och att checka av boxar, utan även om att se till att skydda verksamheten och kunderna från reella cyberhot och IKT-risker. Det viktiga är därför att arbeta för att säkerställa att verksamheten har en god IKT-riskhantering i samtliga led.

Compliancefunktionen spelar alltså en viktig roll i egenskap av kontrollfunktion, men också som rådgivande funktion. Det viktiga är att fundera över hur företagets verksamhet ser ut, att kartlägga företagets IKT-risker och att göra en bedömning av hur man vill använda sig av compliancefunktionen i arbetet med DORA. Involvera compliancefunktionen tydligt i DORA arbetet för att optimera möjligheterna och affärsnyttan med funktionen.

”God styrning saktar inte ner – den snabbar upp genom att minska osäkerhet och bygga tillit.”

- Julia Haglind & Anna Romberg



Styrning som gör skillnad – när byråkratin blir en framgångsfaktor

Även om bolagsstyrning ofta ses som en självklarhet för att driva en organisation, misstas det inte sällan för att vara en formalitet att bocka av innan man ”går tillbaka till att göra affärer”. Det väcker bilder av styrelsesammanträden, långa styrdokument och komplexa attest- och delegationsmatriser. Vissa ser styrning som en hyllvara – något för bolagsjuristen eller den externa advokatbyrån att hantera. Men det underskattar styrningens verkliga kraft som organisationens dolda motor.

Vi som har upplevt havererad styrning vet att när motorn stannar i ett högriskläge, kan konsekvenserna bli ödesdigra. Precis som en bilmotor måste vara konstruerad för sitt ändamål och bilens kapacitet, bör bolagsstyrningen anpassas efter organisationens syfte och förutsättningar. Goda intentioner väger inte upp för dålig design.

I denna artikel delar vi tre konkreta angreppssätt för att lyfta fram byråkratins styrkor:
Tänk i system – inte silos, designa för verkligheten – inte bara för regelverken, och följ beteenden – inte byråkratin.

1. Tänk i system – inte silos

En välfungerande styrmodell knyter ihop helheten i organisationen. I stället för att hantera styrning i stuprör – per avdelning eller bolag – bör man tänka systemiskt.

God styrning ger tydlighet kring hur information flödar, hur ansvar fördelas och hur beslut fattas. Det handlar om att rätt personer får rätt information i rätt tid, att organisationen har en tydlig rytm och att ledare på alla nivåer både har mandat och ansvar.

Det innebär också att koppla styrning till strategi, verksamhet och kultur. När styrning lever i ett vakuum blir den snabbt förlegad eller ignorerad. Men när den integreras i strategiska beslut, budgetering, projektplanering och uppföljning – då blir den en kraftmultiplikator.

Praktiskt tips: Kartlägg era viktigaste styrdokument, beslutsmandat och rapporteringslinjer över olika bolag och enheter. Identifiera överlapp, luckor och inkonsekvenser. Inför ett centralt styrregister eller en digital plattform för att skapa synlighet och spårbarhet i era policyer och ansvarsförhållanden.

2. Designa för verkligheten – inte bara för regelverken

En av de största utmaningarna i större organisationer är att hantera balansen mellan kontroll och flexibilitet. Behovet av enhetlighet och styrning inom koncernen krockar ofta med verkligheten – där dotterbolag, affärsenheter eller portföljbolag måste förhålla sig till lokala regler, kulturer och förutsättningar. Utmaningen är att undvika överkonstruktion men ändå skapa en ryggrad – en struktur utan stelhet.

Att designa för människor innebär också att tänka på olika användare: från styrelsemedlemmar till medarbetare i första linjen. Det betyder att förenkla språk, förtydliga roller och förklara varför reglerna finns – inte bara vad de säger. Juridikavdelningen kanske behöver exakta referenser – men affärschefen behöver tydlighet, relevans och användbarhet.

I större organisationsstrukturer är styrning också motgiftet mot fragmentering. Den hjälper till att samordna prioriteringar, minska risker och möjliggöra samarbete över gränser – geografiska, kulturella och organisatoriska. När det misslyckas är det ofta för att styrningen blivit för abstrakt eller för långt ifrån vardagen.

Praktiskt tips: Genomför workshops med olika team för att stresstesta styrningen. Fråga: Vet medarbetarna vad som förväntas av dem? Vet de var de hittar det de behöver? Känner de sig trygga i att hantera osäkra beslut? Om inte – förenkla, visualisera eller berätta.

3. Följ beteenden – inte byråkratin

Även det mest sofistikerade styrsystem kan fallera om kulturen motverkar det. När människor känner sig bortkopplade från beslutsprocesser, när tempo värderas över transparens, eller när ledare kringgår strukturer för bekvämlighetens skull – då eroderar styrningen.

Kulturen är det yttersta sammanhanget för styrning. Om medarbetare tror att det inte lönar sig att lyfta problem, eller att policyer bara finns ”för att uppfylla krav” men inte för verkligheten, så tappar de engagemanget. Men om de ser styrningen som ett verktyg som skyddar, ger klarhet och främjar rättvisa – då kommer de att använda det.

Praktiskt tips: Lyssna noga på vad människor säger om era styrmodeller. Är de betrodda eller fruktade? Möjliggör de handling – eller försenar de? Använd pulsmätningar, möten över nivågränser och scenariobaserade övningar för att skapa en öppen dialog.

God styrning saktar inte ner – den snabbar upp genom att minska osäkerhet och bygga tillit. I en allt mer komplex värld hjälper den företag att växa med integritet, fatta snabbare beslut och möta osäkerhet med självförtroende.



A leading governance, risk and compliance powerhouse, offering best-in-class services and tech solutions to the European industry

advisense.com