Compliance Risk Assessment – få en inblick i hur man gör

Fredrik Styrlander, 20 januari 2026

BG Institute
EN DEL AV BLENDOW GROUP

Årets samhälls-insats 2025
SVENSKA UTBILDNINGSPRISET

Agenda

- Kort introduktion om Compliance
- Det riskbaserade arbetssättet
- Vad är en Compliancerisk?
- Metod för identifiering och utvärdering av risker
- Sammanfattning och praktiska tips

BG Institute
EN DEL AV BLENDOW GROUP

Fredrik Styrlander

- Jurist
- Head of Risk & Compliance Mangold Fondkommission
- Bakgrund från Finansinspektionen och andra tillsynsmyndigheter

BG Institute
EN DEL AV BLENDOW GROUP

Vad är Compliance?

- Kontrollant och intern polis?
- Övervakare?
- Ansvarig för regelefterlevnad?
- Skydd för aktieägarnas intressen?
- Regulatorisk rådgivare och kvalitetssäkrare?
- Moralisk kompass?
- Samvete?
- Detektiv?
- Författare av interna regler?
- Utbildningsansvarig?
- Process och affärsutvecklare?

BG Institute
EN DEL AV BLENDOW GROUP

Exempel från lagtext

Artikel 22.2 Kommissionens delegerade förordning (EU) 2017/565 (MiFID II)

Värdepappersföretag ska införa och upprätthålla en permanent och effektiv avdelning för regelefterlevnad som fungerar oberoende och som ansvarar för följande:

Övervaka, ge rådgivning, rapportera till styrelsen

FFFS 2014:1

Finansinspektionens föreskrifter och allmänna råd om styrning, riskhantering och kontroll i kreditinstitut

8 kap 3 § - Funktionen för regelefterlevnad ska identifiera, **övervaka och kontrollera, ge råd och stöd, utbilda**, kontrollera att nya tjänster följer relevanta regler

6 kap 7 § - **Rapportera** regelbundet och minst årligen **till Styrelsen**, **risk&compliance utskott, VD** och **följa upp rapporterade brister, åtgärder och konsekvenser**.

EBA/GL/2021/05 Guidelines om intern styrning och kontroll

Ge ledningsorganet råd om åtgärder som kan vidtas för att säkerställa efterlevnaden av tillämpliga lagar, regler, förordningar och standarder.

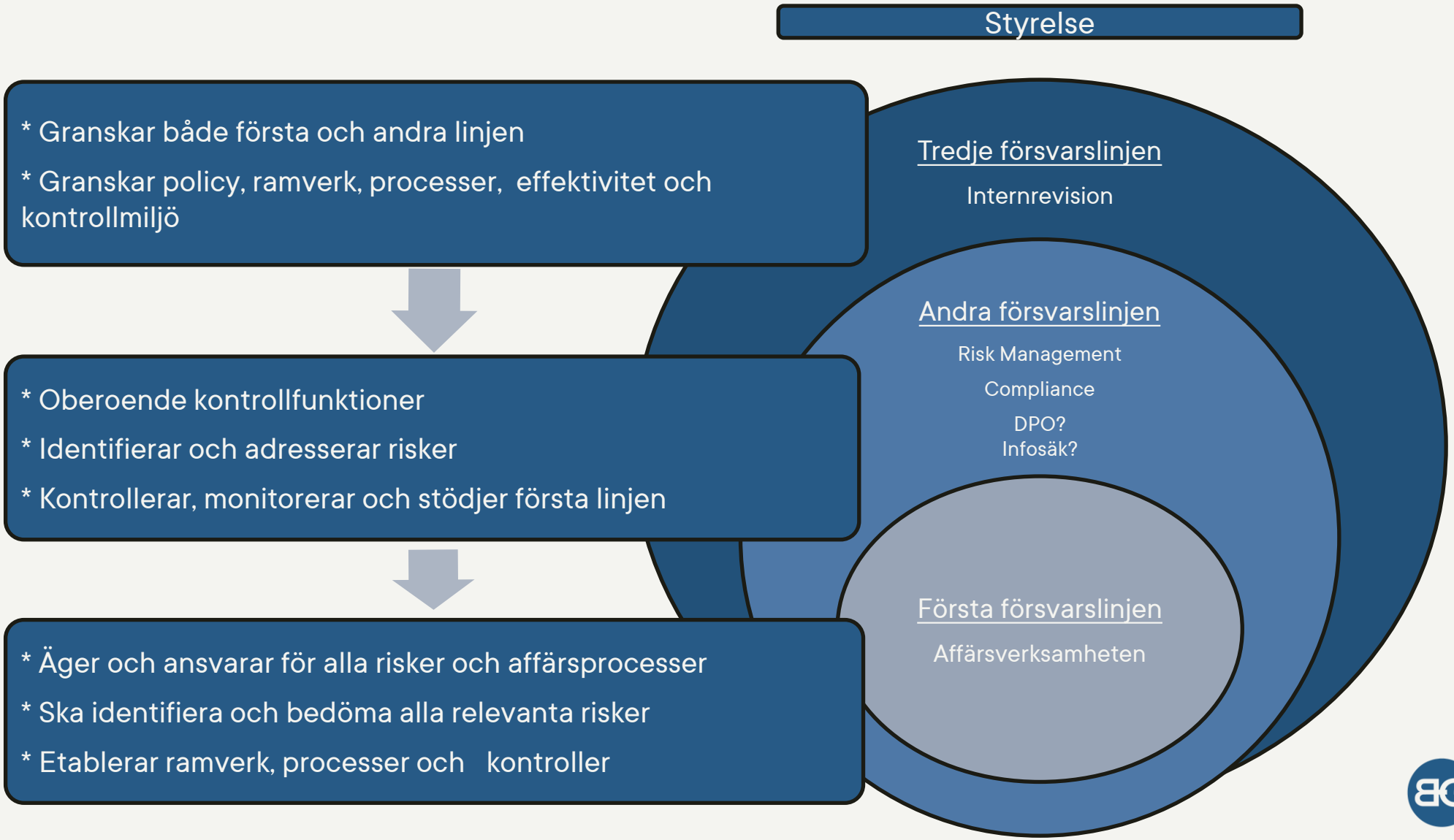
Bedöma hur **ändringar i lagstiftningen** eller regelverket kan komma att **påverka institutets verksamhet och ramverk** för efterlevnad.

Övervaka regelefterlevnad med hjälp av ett strukturerat och väldefinierat program

Rapportera till ledningsorganet

BG Institute
EN DEL AV BLENDOW GROUP

Principen om de tre försvarslinjerna



BG Institute
EN DEL AV BLENDOW GROUP

Compliance roll och funktion

- Kontrollfunktion
- Oberoende från verksamheten
- Rapporterar till Styrelse och VD/Ledning
- Granskar, monitorerar och stödjer verksamheten
- Scoope: Efterlevnad av interna och externa regler

Det riskbaserade arbetssättet

- Resursfördelning och attention utifrån risknivå
- Fokusera och lägga resurserna på de områden där de väsentligaste riskerna finns och som kräver starkare intern kontrollmiljö
- Utgångspunkt för planering och prioritering av kontrollfunktionernas arbete
- Underlag för styrelsen vid beslut av aktivitetsplan för kontrollfunktionerna

Riskbaserat arbetssätt

Från lagtext och vägledning

Kommissionens delegerade förordning (EU) 2017/565 (MiFID II) Artikel 22.2

*"**Funktionen för regelefterlevnad ska upprätta ett riskbaserat övervakningsprogram** som tar hänsyn till värdepappersföretagets alla områden av investeringstjänster, verksamheter och alla relevanta sidotjänster, inbegripet relevant information som inhämtats i samband med övervakningen av handläggningen av klagomål. **Övervakningsprogrammet ska fastställa prioriteringar som avgörs genom riskbedömningen** av regelefterlevnad som säkerställer övergripande övervakning av regelefterlevnaden."*

Från FFFS 2014:1 om styrning, riskhantering och kontroll i kreditinstitut

8 kap 1 §

*"Företaget ska **ha lämpliga rutiner** och vidta **lämpliga åtgärder** för att **minimera risken** för att **lagar, förordningar och andra regler** som gäller för den tillståndspliktiga verksamheten **inte följs**."*

8 kap 3 §

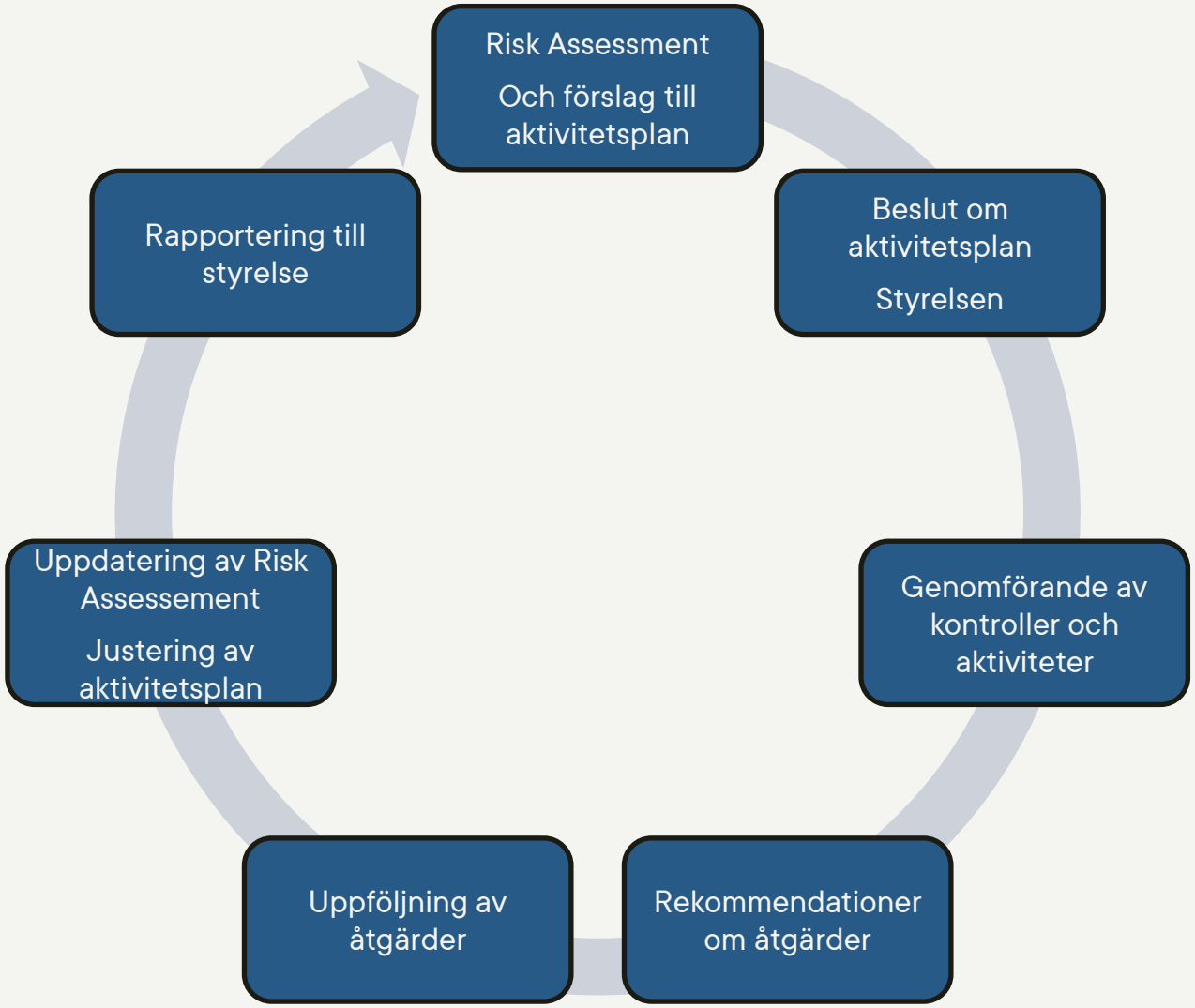
*"1. dels **identifiera vilka risker** som finns för att företaget inte fullgör sina förpliktelser enligt lagar, förordningar och andra regler som gäller **för den tillståndspliktiga verksamheten**, dels **övervaka och kontrollera att riskerna hanteras** av berörda funktioner,"*

Från FATF guidelines avseende AML

*"**The risk-based approach is central to the effective implementation** of the FATF Recommendations. **A risk-based approach means** that countries, competent authorities, and banks **identify, assess, and understand** the money laundering and terrorist financing **risk to which they are exposed**, and take the **appropriate mitigation measures in accordance with the level of risk."***

BG Institute
EN DEL AV BLENDOW GROUP

Riskbaserat arbetssätt - Compliance årshjul



Vad är en compliancerisk?

Compliancerisk – finns ingen universell definition

Möjliga perspektiv:

- Risken för att inte följa relevanta regler
- Skada på skyddsintressen för externa och interna regler (kunder, finansiellt stabilitet, samhället)
- Risk att inte leva upp till tillsynsmyndigheter krav och förväntningar (sanktion)
- Avvikelser från regler och utfästelser som skadar förtroendet hos investerare och allmänhet
- Bör inte enbart mätas i kronor och ören…

Från 9 kap 1 § Lagen om värdepappersmarknaden (2007:528) - Sundhetsbestämmelsen

”Ett värdepappersinstitut skall tillvarata sina kunders intressen när det tillhandahåller investeringstjänster eller sidotjänster till dessa ***samt handla hederligt, rättvist och professionellt.*** *Ett värdepappersinstitut skall även* ***i övrigt handla på ett sätt så att allmänhetens förtroende*** *för värdepappersmarknaden* ***upprätthålls****.”*

BG Institute
EN DEL AV BLENDOW GROUP

Inventera regeluniversum/kravbild

Vilka regler gäller för er verksamhet? Och vilka är det mest centrala?

- Tillstånd och rörelseregler
- AML, konsumentskyddsregler, jäv och intressekonflikter, anti-korruption och finansiell brottslighet, sanktioner, GDPR, MAR m.m.
- Vilka skyddsintressen finns? Vad är lagstiftningen till för att skydda?
- Standarder och certifieringar
- Leverantörskrav, kontraktuella åtaganden
- Utfästelser mot allmänheten – exempelvis inom hållbarhet

Identifiera risker

- Hur kan avvikelser från interna och externa regler materialisera sig?
- Vilken skada kan det medföra för bolaget, kunder och lagstiftningens skyddsintressen?

Exempel på riskområden för ett finansiellt institut

- Kundskydd – Hur beter vi oss mot kunder och hur iakttar vi kundskyddsregler?
- Exempel: uppvisar vi omsorg och konsumentskydd i investeringsrådgivning till konsument?

- Market conduct – Agerar vi korrekt och följer regler på värdepappersmarknaden?
- Exempel: Hanterar vi förfaranden och protokoll för marknadssonderingar korrekt?

- AML – Följer vi tillämpliga regler och har vi tillräckliga processer för att motverka, förhindra, upptäcka och rapportera penningtvätt?
- Exempel: Har vi välfungerande processer för inhämtande av kundkännedom och monitorering av transaktioner?

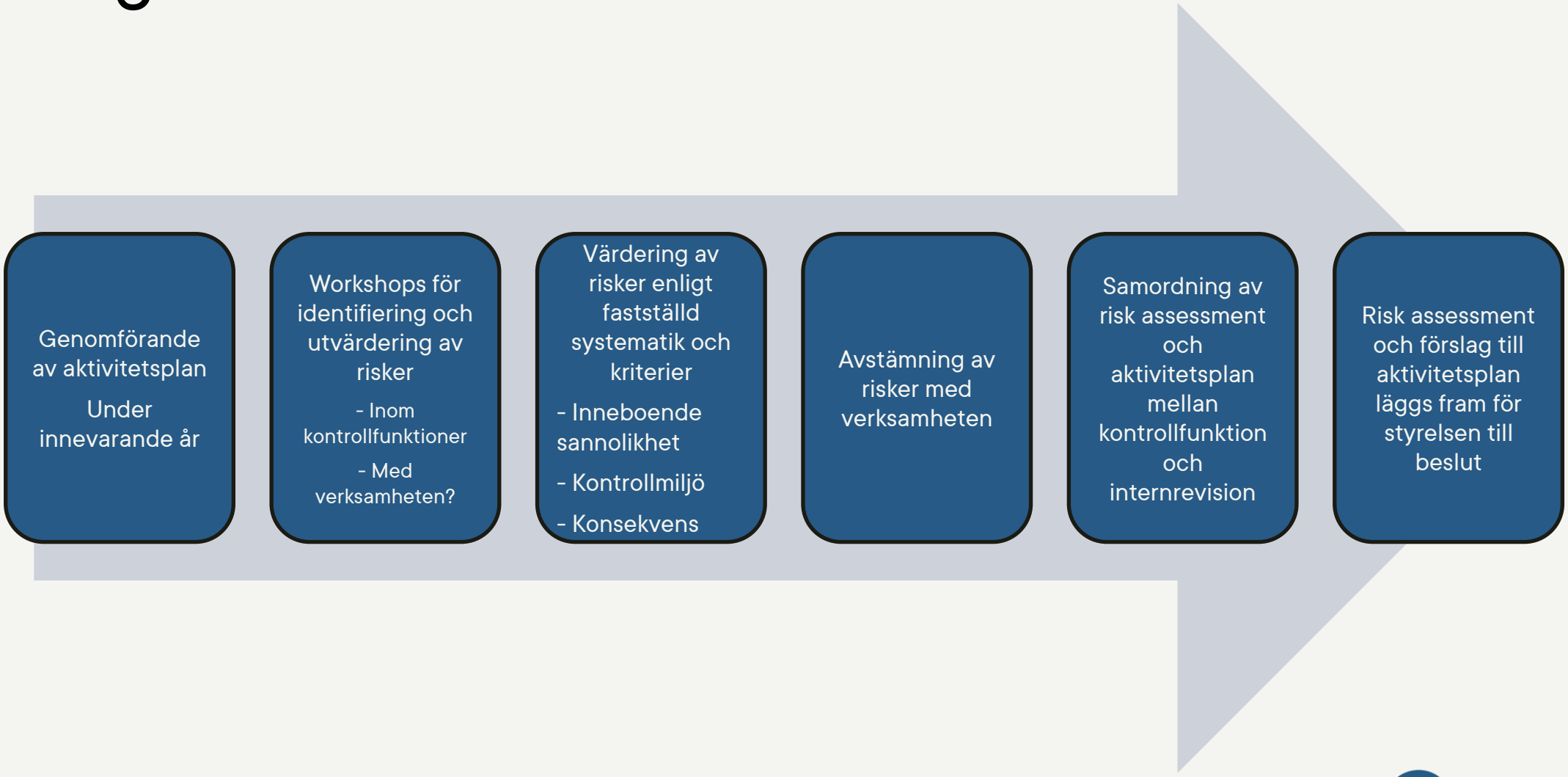
BG Institute
EN DEL AV BLENDOW GROUP

För att förstå verksamhetens risker måste man först förstå hur verksamheten fungerar

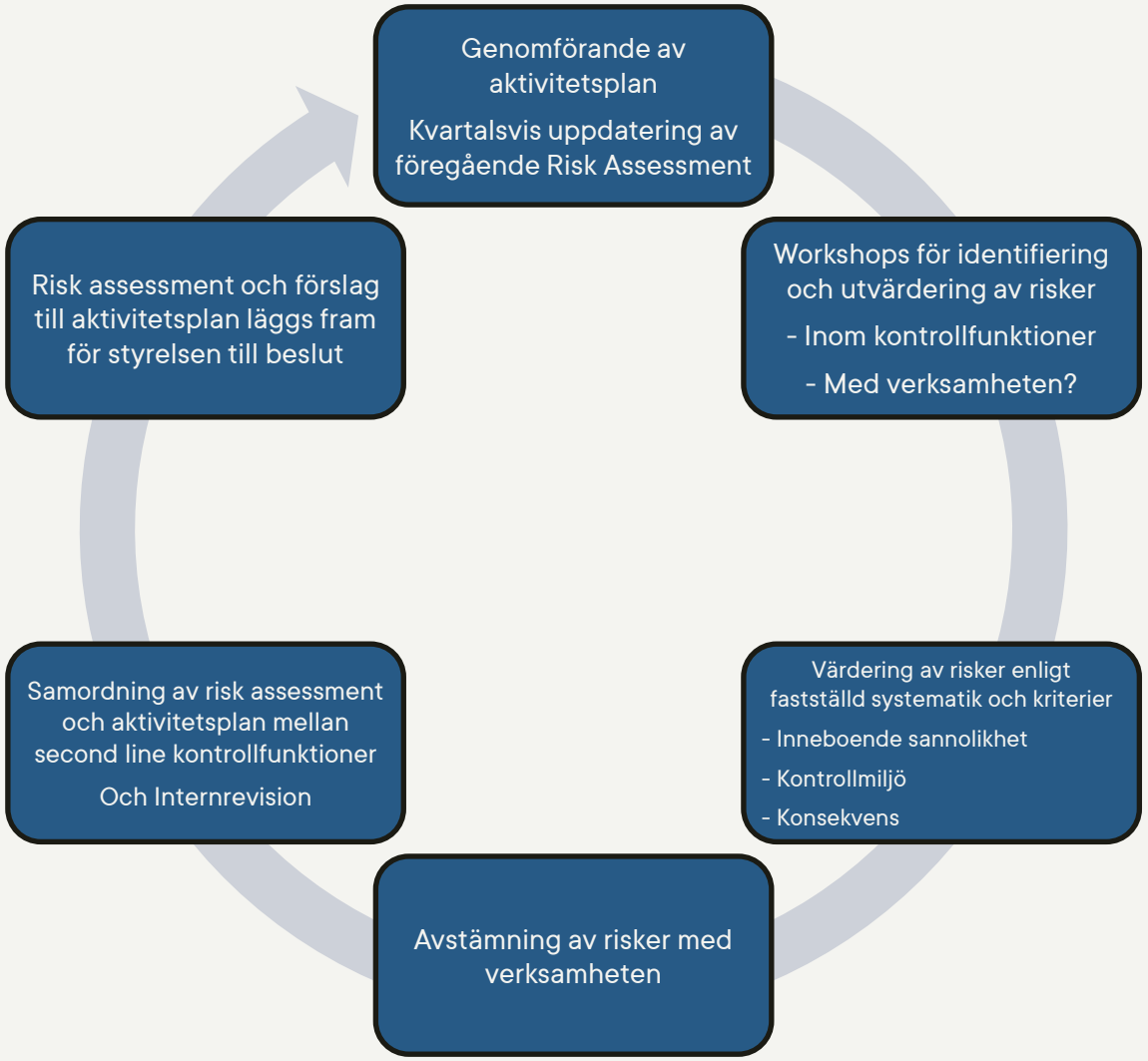
- Affärsmodell
- Intjäning
- Incitament
- Riskaptit, inställning och kultur inom verksamheten och olika affärsområden
- Processer, system och manuell hantering
- Vad funkar bra? Vad funkar dåligt?

BG Institute
EN DEL AV BLENDOW GROUP

Att göra en risk assessment



Feed in och utgångspunkter



Feed in:

- Observationer i genomförda kontroller
- Observationer i löpande verksamhet/Råd&stöd
- Observationer från andra kontrollfunktioner
- Självutvärdering av risk management inom OP-risk
- Omvärldsbevakning
- Nya sanktioner från tillsynsmyndighet
- Nya och kommande regelverk
- Respons i genomförda utbildningar
- Händelser och incidenter
- Workshops med verksamheten
- Magkänsla…

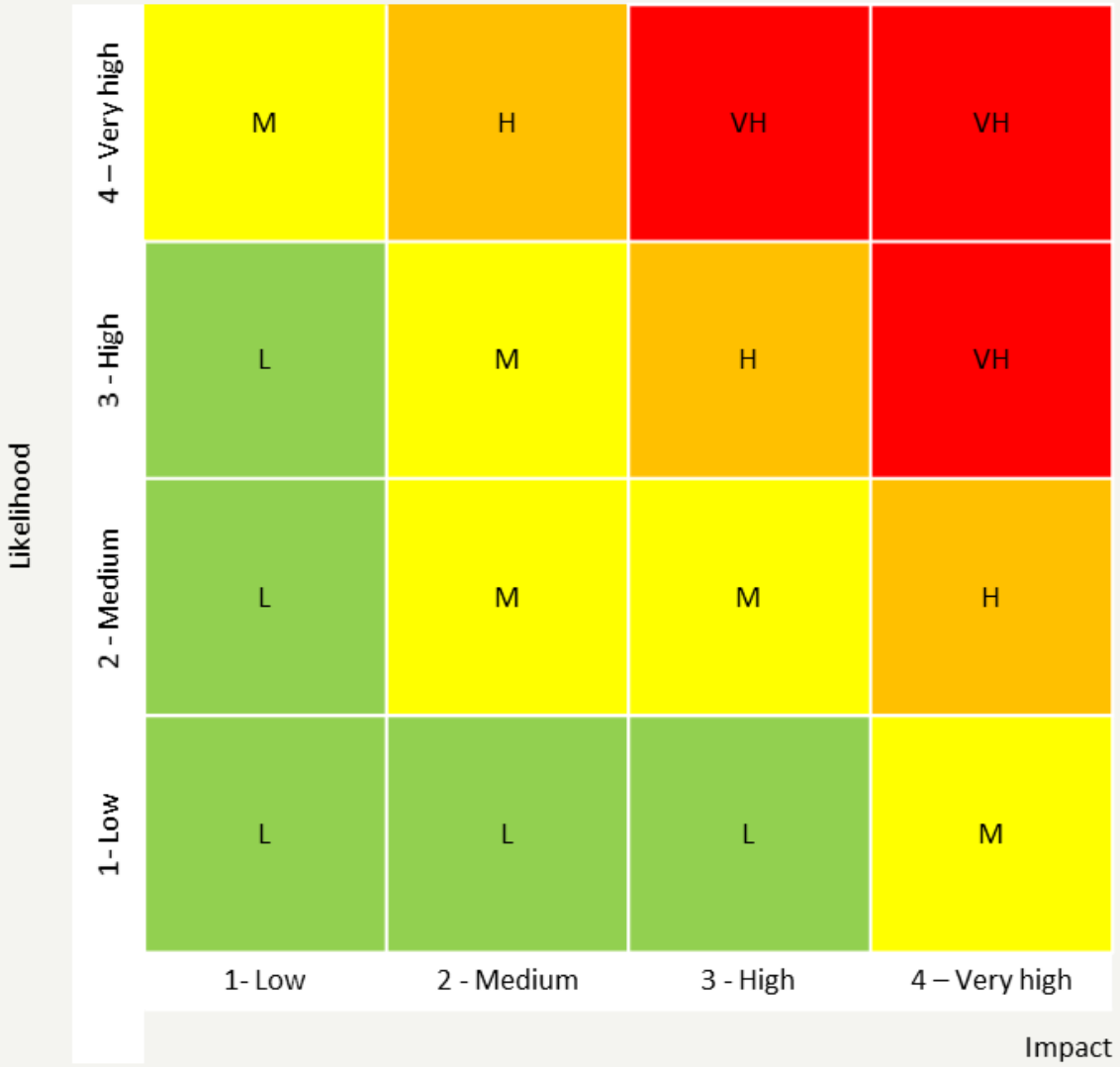
BG Institute
EN DEL AV BLENDOW GROUP

Inneboende sannolikhet

Minus kontrollmiljö = Residualrisk

Multiplicerat med Konsekvens

= Riskfaktor



BG Institute
EN DEL AV BLENDOW GROUP

Sannolikhet?

- Vad är sannolikheten att avvikelse uppstår eller att risk materialiseras?

- Utan att beakta interna kontroller

- Exempel på faktorer som påverkar sannolikheten för att en risk inträffar
  - Frekvens och volym av affär eller flöde
  - Där en hög frekvens och volym medför ökad sannolikhet för brister
  - Om hantering, processer och flöden är automatiserade eller manuella
  - Inneboende och identifierade intressekonflikter
  - Kommersiella motiv för verksamheten att frångå riktlinjer, limiter eller exponera sig för risk
  - Personliga ekonomiska intressen att frångå riktlinjer, limiter eller exponera sig för risk

BG Institute
EN DEL AV BLENDOW GROUP

Kontrollmiljö?

- Finns dokumenterade interna processer/rutiner?
- Är dessa tillfredsställande utformade och effektiva?
- Har första linjen identifierat sina risker?
- Och etablerat kontroller och interna avstämningar?
- Och adresserar kontrollerna identifierade risker i processer på ett effektivt sätt?
- Har relevanta intressekonflikter identifierats av verksamheten och finns beslutad hantering av intressekonflikter som adresserar dessa på ett adekvat sätt?

BG Institute
EN DEL AV BLENDOW GROUP

Kontrollmiljö forts

- Finns begränsningar och reglering för incitament och ersättningssystem?
- Nivå av kunskap om regler och krav i verksamheten
- Har avvikelser och brister identifierats i kontrollfunktionernas granskningar?
- Har verksamheten genomfört åtgärder för identifierade brister i kontrollfunktionernas granskningar?
- Kundklagomål?

BG Institute
EN DEL AV BLENDOW GROUP

Viktiga frågeställningar vid värdering av konsekvens

- Hur definierar man konsekvenser för överträdelser av externa och interna regler?
- Avvikelser mot kundskydd, good conduct och beteende på marknaden har större konsekvenser för bolaget än den rena regelöverträdelsen
- Går konsekvensen av en compliancerisk att mäta i kronor och ören?
- Kommersiella konsekvenser? Ryktesrisk?
- Risk för sanktion eller indraget tillstånd?

BG Institute
EN DEL AV BLENDOW GROUP

Exempel på bedömning av risk

- **Område:**

Kundskydd/good conduct

- **Delrisk:**

Risk att rådgivare brister i omsorgsplikten och inte rekommenderar finansiella produkter som är mest lämpliga för kunden

- **Bedömning inneboende sannolikhet - hög:**

Det finns skillnad i lönsamhet mellan produkter i institutets produktutbud, rådgivningen har en hög transaktionsvolym och intjäning hos enskild rådgivare påverkar bonus

- **Bedömning kontrollmiljö - god:**

Compliance har tidigare år identifierat brister i rådgivningsakter vid genomförda kontroller där kunder rekommenderats produkter i högre risknivå än vad som är lämpligt utifrån kundens profil

Verksamheten har därefter etablerat regelbunden egenkontroll vilket kombinerat med utbildning från Compliance medfört ett förbättrat resultat utan avvikelser i uppföljande kontroll

- **Bedömning konsekvens - hög:**

Kundskydd är ett centralt område inom Mifid II och är prioriterat i Finansinspektionens tillsyn där ett flertal bolag tilldelats sanktion och i vissa fall indraget tillstånd. Konsumenter är ett viktigt skyddsområde och avvikelser mot kundskyddet kan medföra förtroendeförlust och ryktesskada som kan medföra allvarliga kommersiella konsekvenser för bolaget

BG Institute
EN DEL AV BLENDOW GROUP

Exempel på hur det kan se ut

Risk ID	Affärsområde	Område	Riskägare	Risk	Konsekvens 1(låg) - 5(hög)	Innebodende sannolikhet 1(låg) - 5(hög)	Kontrollmiljö	Sannolikhet efter kontrollmiljö	Riskfaktor Residualrisk	Risknivå	Förändring 2023 vs 2024	Senast utförd granskning
1.3	A	Mutor & korruption		Beskrivning av risken…	3	4	Mycket god	2	6	Ingen väsentlig risk	Oförändrad	2020
1.4	B	Hantering av intressekonflikter		Beskrivning av risken…	5	4	Mycket god	2	10	Betydande risk	Minskad	2023
1.5	Z	Kundskydd rådgivning		Beskrivning av risken…	3	3	Medel	3	9	Mindre väsentlig risk	Ökad	2023
1.6	D	AML-risker kopplat till kunder utanför EU/EES samt Offshore-upplägg		Beskrivning av risken…	4	4	Mycket god	2	8	Mindre väsentlig risk	Oförändrad	2019
1.7	A	Hållbarhet		Beskrivning av risken…	4	4	Mycket god	2	8	Mindre väsentlig risk	Minskad	2022

BG Institute
EN DEL AV BLENDOW GROUP

Risk assessment – praktiska tips

- Redigera, gå igenom, värdera och harmonisera
- Vikta upp värdet av risker med högre konsekvens så att centrala områden får attention även om de är väl hanterade av verksamheten – for the moment..
- Erfarenheten är att där man är och petar hålls standarden uppe och där man släpper – så släpper också verksamheten efter vart efter
- Stäm av och förankra viktiga risker med berörda delar av verksamheten
- Alla risker kan inte vara viktigast – våga differentiera!
- Styrelsen ska enkelt kunna ta ställning till vilka risker som är de viktigaste

  - Vilka är topp 3?

BG Institute
EN DEL AV BLENDOW GROUP

Compliance i praktiken – grundkurs

17 mars 2026

Som kursdeltagare får du kunskap om:

- Compliancefunktionens roll och ansvar.
- Begreppet intern styrning och kontroll.
- Grunderna i det riskbaserade arbetssättet.
- Praktisk vägledning i hur du genomför en riskbedömning och utformar en effektiv aktivitetsplan.
- Hur du utformar ett effektivt kontrollarbete och rapporterar/kommunicerar dina iakttagelser och slutsatser.
- Viktiga tips för att navigera, kommunicera och skapa förtroende internt.
- Vanliga fallgropar och praktiska tips för framgångsfaktorer inom compliancearbetet.

BG Institute
EN DEL AV BLENDOW GROUP

Vad tyckte du om dagens webbinarium?

Ta gärna 30 sekunder och svara på utvärderingen!
Efter det besvaras frågor i mån av tid

BG Institute
EN DEL AV BLENDOW GROUP

Frågor?

BG Institute
EN DEL AV BLENDOW GROUP

Årets samhälls-insats 2025
SVENSKA UTBILDNINGSPRISET

Tack!

För frågor om BG Institute och våra kurser,
mejla oss på kursinformation@bginstitute.se

BG Institute
EN DEL AV BLENDOW GROUP

Årets samhälls-insats 2025
SVENSKA UTBILDNINGSPRISET