

Dokumentnamn	Policy för intern styrning och kontroll		
Dokumentägare	Fastställd av	Datum	Ersätter dok. daterad
<i>Head of CEO Office</i>	<i>Styrelsen</i>	<i>2023-12-06</i>	<i>2023-09-13</i>
INFORMATIONSKLASS	Relaterade styrdokument		Publ. Intranät/webb
ALLMÄN	<i>VD-instruktion för intern styrning och kontroll</i>		<i>Ja</i>

## Innehåll

1. Inledning .....	3
1.1 Bakgrund och syfte .....	3
1.2 Rättslig grund .....	3
2. Övergripande principer för intern styrning och kontroll .....	3
3. Principer för beslutsfattande .....	4
4. Organisation och styrningsmodell.....	4
4.1 Bolagstämman .....	4
4.2 Valberedning .....	5
4.3 Styrelsen och styrelseutskott.....	5
4.3.1 Revisionsutskottet.....	6
4.3.2 Ersättningsutskott.....	6
4.3.3 Kreditutskott.....	6
4.3.4 Risk- och Complianceutskottet.....	6
4.4 VD6	
4.4.1 Kommittéer.....	7
4.4.2. Ledningsgruppen.....	7
4.4.3. Kreditkommitté Företag.....	7
4.4.4. Riskkommitté.....	7

4.4.5. Kommitté för icke-finansiella risker .....	7
4.4.6. Asset Liability Committee .....	8
4.5 Enhetsansvariga/affärsansvariga .....	8
4.6 Kontrollfunktioner.....	8
4.6.1 Allmänt om kontrollfunktioner .....	8
4.6.2 Riskkontrollfunktionen .....	9
4.6.3 Compliancefunktionen.....	9
4.6.4 Internrevisionsfunktionen .....	10
4.6.5 Information till kontrollfunktioner.....	10
5. Kontrollmiljö .....	10
5.1 De tre försvarslinjerna .....	10
5.2 Första försvarslinjen.....	11
5.3 Andra försvarslinjen.....	11
5.4 Tredje försvarslinjen .....	11
6. Internt regelverk.....	11
7. Process för regelverksbevakning .....	12
8. Riskhanteringsramverk.....	12
8.1 Allmänt.....	12
8.2 Riskkultur .....	12
8.3 Riskhanteringsprocess.....	13
8.4 Riskstrategier och riskaptit .....	13
9. Övriga processer för intern styrning i banken .....	13
10. Etiska frågor.....	14
11. Förmedling av låneskyddsförsäkringar .....	14
12. Dokumentationsrutiner.....	15
13. Uppföljning och fastställande .....	15
13.1 Efterlevnad och uppföljning.....	15
13.2 Uppdatering och fastställande.....	15

## 1. Inledning

### 1.1 Bakgrund och syfte

Denna policy gäller för Norion Bank AB, dess dotterbolag och dess filialer ("Norion Bank", "banken"). Policyn omfattar bankens verksamhet och medarbetare och gäller även i förhållande till såväl kunder som leverantörer och andra samarbetspartners.

I syfte att säkerställa en väl fungerande intern styrning och kontroll har Norion Bank etablerat ett ramverk bestående av interna regler och processer. Ramverket syftar till en effektiv och ändamålsenlig organisation av verksamheten beträffande förmågan att identifiera, mäta, styra, rapportera samt i övrigt hantera risker och regelefterlevnaden i verksamheten.

I denna policy beskrivs det övergripande ramverket för intern styrning och kontroll och policyn utgör styrelsens övergripande styrdokument för att etablera en sund kultur av styrning och kontroll av risker och regler som är anpassade till den verksamhet som bedrivs i Norion Bank. Styrelsen delegerar ansvaret för den löpande verksamheten till verkställande direktör ("**VD**") och denne har att utfärda en instruktion för att i detalj beskriva den interna styrningen och kontrollen som möjliggörs i banken genom det mandat som styrelsen tilldelat VD ("VD-instruktion för intern styrning och kontroll").

### 1.2 Rättslig grund

Regelverk till grund för denna policy:

- Lag (2004:297) om bank- och finansieringsrörelse,
- Finansinspektionens föreskrifter och allmänna råd (2014:1) om styrning, riskhantering och kontroll i kreditinstitut,
- Finansinspektionens föreskrifter FFFS 2018:10
- EBA:s riktlinjer för intern styrning (EBA/GL/2021/05)
- Svensk kod för bolagsstyrning ("Bolagsstyrningskoden")
- Nasdaq regelverk
- Lag (2018:1219) om försäkringsdistribution,
- Förordning (2018:1231) om försäkringsdistribution samt
- EBA:s riktlinjer för lämplighetsbedömning av styrelse, VD och ledande befattningshavare (EBA/GL/2021/06)

## 2. Övergripande principer för intern styrning och kontroll

Den interna styrningen och kontrollen konkretiseras genom följande principer:

- Intresset och medvetenheten för regler och risker i organisationen ska löpande främjas.
- Norion Banks organisation ska vara transparent och ändamålsenlig med tydligt angivna och dokumenterade ansvarsområden.
- Ledande befattningshavare, som direktrapporterar till VD, ska ha individuella mandatbeskrivningar.
- Norion Bank ska ha tydliga och dokumenterade beslutsprocesser.

- Norion Banks fora för beslutsfattande ska ha tydliga ramar och dokumenterade beslut, när relevant.
- Norion Bank ska ha tydliga och dokumenterade rapporteringsvägar.
- Norion Banks verksamhet ska gynna en god och välfungerande kontrollmiljö.
- Vid beslutsfattande ska hållbarhet tas i beaktande i den utsträckning det är relevant och möjligt.
- Norion Bank ska ha tydliga processer för att hantera etablering och avveckling på nya marknader. Processerna ska omfatta underrättelse till tillsynsmyndigheter samt hantering av lokala regelverk.
- Norion Banks huvudsakliga geografiska marknad ska vara Norden och Tyskland, och därtill drivs verksamhet i vissa delar av Europa. VD äger rätt att fatta beslut om verksamhet inom EU.
- Norion Banks huvudsakliga geografiska marknad ska vara Norden och Tyskland, och därtill drivs verksamhet i vissa delar av Europa.

### **3. Principer för beslutsfattande**

- Vid strategiska beslut ska alltid konsekvenserna och påverkan med avseende på regler (compliance) och risker beaktas. Även vid samtliga övriga affärsbeslut ska alltid interna och externa regelverk beaktas.
- Alla väsentliga beslut ska vara spårbara så att grunderna för beslutet förblir kända.
- Transparens och tydlighet har särskild betydelse för beslut inom områden som rapporteringslinjer, roller och ansvar.
- Vid beslutsfattande ska hållbarhet tas i beaktande i den utsträckning det är relevant och möjligt.

## **4. Organisation och styrningsmodell**

### **4.1 Bolagstämman**

Norion Banks högsta beslutande organ är bolagsstämman.

Årsstämman väljer styrelse och revisorer, fastställer räkenskaper, beslutar om eventuell utdelning och andra dispositioner av resultatet samt beslutar om ansvarsfrihet för styrelsen och VD. Därutöver beslutar bolagsstämman bland annat om eventuella nyemissioner, efter bemyndigande, införande av aktierelaterade incitamentsprogram, förfarandet vid tillsättning av valberedning samt riktlinjer för ersättning till ledande befattningshavare. Ordinarie årsstämma ska hållas inom sex månader från räkenskapsårets utgång.

Samtliga aktieägare som är registrerade i aktieboken per avstämningsdagen och är anmälda i enlighet med bolagsordningens föreskrifter har rätt att delta vid bolagsstämman. Kallelse till bolagsstämma ska ske i enlighet med bestämmelser i aktiebolagslag (2005:551) och bolagsordningen. Varje aktie ger aktieägare rätt till en röst.

Norion Bank ska förse aktieägare och finansmarknad med information i enlighet med tillämpliga regelverk.

## 4.2 Valberedning

Årsstämman fastställer principer för valberedningens tillsättning. Valberedningen har att lämna förslag till årsstämman om;

- val av ordförande vid årsstämma,
- val av antal stämموvalda styrelseledamöter,
- val av styrelsens ordförande,
- arvode och annan ersättning till var och en av de stämموvalda styrelseledamöterna och till ledamöter av styrelsens utskott,
- val av revisorer och arvode till revisorer, samt
- val av valberedning alternativt principer för tillsättande av valberedning, instruktion för valberedning samt ersättning till valberedningens ledamöter.

Valberedningen har i övrigt att utföra de uppgifter som ankommer på valberedningen i enlighet med Bolagsstyrningskoden.

## 4.3 Styrelsen och styrelseutskott

Styrelsen har det yttersta ansvaret för Norion Banks verksamhet och organisation samt ansvarar för att det finns en ändamålsenlig struktur för intern styrning och kontroll. Det innebär att styrelsen är ytterst ansvarig för att fatta beslut om Norion Banks verksamhet och för att kontrollera och följa upp verksamheten. Detta ansvar uppfyller styrelsen genom att dels vara väl insatta i Norion Banks verksamhet och därmed kunna fatta välgrundade beslut, dels genom att löpande övervaka och utmana verksamheten. Till stöd i sitt arbete med att övervaka verksamheten har styrelsen kontrollfunktionerna. Styrelsen ska därtill verka för en företagskultur som främjar god intern styrning och kontroll i verksamheten samt verkar för en god och effektiv kontrollmiljö. Vidare ska styrelsen säkerställa att Norion Banks styrsystem, kontrollmiljö och resursallokering är effektiv och lämplig med hänsyn till den verksamheten som banken bedriver.

Som ett led i att fullgöra sitt ansvar ska styrelsen fastställa interna regler i syfte att styra verksamheten samt säkerställa att tillförlitlig, aktuell och fullständig information rapporteras till styrelsen av verksamheten. Styrelsen ska regelbundet, dock minst årligen, utvärdera om de interna reglerna behöver ändras eller uppdateras, för att på så sätt säkerställa att intern styrning och kontroll vid var tid är uppdaterad samt effektiv och anpassad till verksamheten, Norion Banks affärsstrategier och gällande externa regelverk. Styrelsen ska vidare regelbundet bedöma effektiviteten i Norion Banks ramverk för intern styrning och kontroll med avseende på regelefterlevnad och riskhantering.

Styrelsens organisation, ansvar och uppgifter regleras närmare i *Arbetsordning för styrelsen Norion Bank AB*.

För beredning av styrelsens arbete finns fyra av styrelsen särskilt inrättade utskott. Dessa utskott utgörs av Revisionsutskottet, Ersättningsutskottet, Risk- och Complianceutskottet och Kreditutskottet. Samtliga möten i utskotten protokollförs.

#### 4.3.1 Revisionsutskottet

För att bistå styrelsen i dess övervakande roll över revisionsfrågor har styrelsen för Norion Bank inrättat ett särskilt Revisionsutskott. Utskottet är beredande och styrelsen fattar samtliga beslut.

Styrelsen har fastställt en särskild arbetsordning för utskottet, se *Arbetsordning för styrelsens revisionsutskott*. Där i anges revisionsutskottets uppdrag och sammansättning mer detaljerat.

#### 4.3.2 Ersättningsutskott

För att bistå styrelsen i bankens ersättningsfrågor har styrelsen för Norion Bank inrättat ett Ersättningsutskott. Utskottet är beredande och styrelsen fattar samtliga beslut.

Styrelsen har fastställt en särskild arbetsordning för utskottet, se *Arbetsordning för styrelsens ersättningsutskott*. Där i anges ersättningsutskottets uppdrag och sammansättning mer detaljerat.

#### 4.3.3 Kreditutskott

För att säkerställa att bankens kreditprocess är i enlighet med av styrelsen antagen *Kreditpolicy* har styrelsen för Norion Bank inrättat ett Kreditutskott. Kreditutskottet har som huvudregel, att fatta beslut om krediter i de jurisdiktioner och uppgående till det belopp som vid var tid fastställs av styrelsen i *Kreditpolicy*n. Kreditbesluten fattas i enlighet med bankens principer för beslutsfattande enligt avsnitt 3.

Styrelsen har fastställt en särskild arbetsordning för utskottet, se *Arbetsordning för styrelsens kreditutskott*. Där i anges kreditutskottets sammansättning och uppdrag mer detaljerat.

#### 4.3.4 Risk- och Complianceutskottet

För att bistå styrelsen i Norion Bank i frågor rörande risk- och compliancefrågor har styrelsen i Norion Bank inrättat ett Risk- och Complianceutskott. Utskottet är beredande och styrelsen fattar samtliga beslut.

Styrelsen har fastställt en särskild arbetsordning för utskottet, se *Arbetsordning för styrelsens Risk- och complianceutskott*. Där i anges risk- och complianceutskottets uppdrag och sammansättning mer detaljerat.

### 4.4 VD

Styrelsen delegerar ansvaret för den löpande verksamheten till VD. Till stöd i affärsbeslut har VD ledningsgruppen, se avsnitt 4.4.2 nedan, samt ett antal kommittéer, se avsnitt 4.4.3-4.4.7 nedan. Till stöd i sitt arbete med att kontrollera verksamheten har VD även Riskkontrollfunktionen och Compliancefunktionen, se avsnitt 4.6 nedan.

Norion Banks VD ansvarar för den löpande förvaltningen enligt styrelsens riktlinjer och anvisningar samt för sådana skyldigheter som ligger inom ramen för VD:s uppgifter i enlighet med externa regelverk. VD har även ansvar för att styrelsens anvisningar om intern styrning och kontroll implementeras och efterlevs av verksamheten.

VD ska regelbundet, minst årligen, utvärdera de interna regelverk som VD beslutat om och se över om dessa behöver uppdateras. VD ska vidare främja förståelsen för det interna regelverket och verka för en företagskultur inbegripet en god och effektiv kontrollmiljö.

VD ska tillse att styrelsen får tillförlitlig, aktuell och fullständig information för att kunna fatta väl underbyggda beslut. VD ska även tillse att styrelsen löpande får information om hur Norion Banks verksamhet utvecklas. VD ska dessutom säkerställa och verka för att samtliga anställda i Norion Bank har kunskap och information om hur de ska arbeta för och bidra till att uppnå en effektiv och god intern styrning och kontroll.

VD har att besluta i väsentliga frågor rörande verksamheten och eskalering av VD-beslut ska ske av verksamheten i enlighet med de mandatbeskrivningar som upprättats åt bankens ledande befattningshavare och med stöd av, i tillämpliga fall, erforderligt beslutsunderlag, se VD-instruktionen för intern styrning och kontroll.

VD:s ansvar och uppgifter fastställs mer i detalj enligt styrelsens riktlinjer och anvisningar, däribland *Instruktion för VD*.

#### **4.4.1 Kommittéer**

VD:s samlade forum ska tillsammans utgöra det stöd som VD finner erforderligt för att kunna utföra sina arbetsuppgifter såsom beskrivna i avsnitt 4.4. Upprättade ramar till respektive fora ska biläggas VD-instruktionen för intern styrning och kontroll, förutom ramen avseende de två kreditkommittéerna Företag och Konsument som ska biläggas kreditpolicyn då det ytterst är forum inrättade av styrelsen. Beslut fattade inom ramen för ett fora protokollförs och följer de principer för beslutsfattande som beskrivits ovan i avsnitt 3.

#### **4.4.2. Ledningsgruppen**

Ledningsgruppen i Norion Bank utses av VD och sammansättning framgår av VD-instruktionen för intern styrning och kontroll.

#### **4.4.3. Kreditkommitté Företag**

För att fatta kreditbeslut i enlighet med av styrelsen antagen *Kreditpolicy* har styrelsen inrättat Kreditkommittén Företag. Kommittén har som huvudregel att fatta beslut om de företagskrediter i de jurisdiktioner och uppgående till det belopp som vid var tid fastställs av styrelsen i *Kreditpolicyn*. Sammansättning och formen i övrigt för denna kommitté finns såsom bilaga till kreditpolicyn.

#### **4.4.4. Riskkommitté**

VD har i syfte att säkerställa en effektiv riskhantering inrättat en riskkommitté. Riskkommitténs arbete består i att regelbundet följa upp de mest väsentliga riskerna i banken och skaffa sig en djupare förståelse för dessa. Sammansättning och formen i övrigt för denna kommitté finns såsom bilaga till VD-instruktionen för intern styrning och kontroll.

#### **4.4.5. Kommitté för icke-finansiella risker**

VD har i syfte att säkerställa en effektiv hantering av icke-finansiella risker inrättat en kommitté för icke-finansiella risker. Denna kommitté har till syfte att följa upp de mest väsentliga icke-finansiella riskerna i banken och skaffa sig en djupare förståelse för detta. Sammansättning och formen i övrigt för denna kommitté finns såsom bilaga till VD-instruktionen för intern styrning och kontroll.

#### 4.4.6. Asset Liability Committee

Asset Liability Committee ("**ALCO**") ska hantera frågor som berör Bankens finansieringsstrategi, likviditetsreserv samt likviditets- och marknadsrisker. Sammansättning och formen i övrigt för denna kommitté finns såsom bilaga till VD-instruktionen för intern styrning och kontroll.

#### 4.4.7 Etiska kommittén

VD har inrättat en Etisk Kommitté ("**EK**") som har till uppgift att lämna rekommendationer och fatta beslut i etiska frågeställningar, däribland hållbarhetsfrågor. Sammansättning och formen i övrigt för denna kommitté finns såsom bilaga till VD-instruktionen för intern styrning och kontroll.

#### 4.4.8 Kreditkommitté Konsument

Styrelsen har i enlighet med antagen kreditpolicy inrättat kreditkommittén Konsument för löpande monitorering av konsumentkrediter. Kommittén har till uppgift att löpande vidta nödvändiga åtgärder i syfte att säkerställa god regelefterlevnad och acceptabel risk. Sammansättning och formen i övrigt för denna kommitté finns såsom bilaga till kreditpolicyn.

### 4.5 Enhetsansvariga/affärsansvariga

Enhetsansvarig/affärsområdesansvarig är den person som är anställd i Norion Bank med ansvar för en organisatorisk enhet. Denna person har det övergripande operativa ansvaret för att hantera samtliga risker inom enheten/affärsområdet.

En väsentlig förutsättning för en god intern styrning och kontroll är att tillämpliga regler följs. Samtliga anställda i Norion Bank, och i förekommande fall uppdragstagare, har därför ett eget ansvar och en skyldighet för att följa såväl externa som interna regelverk.

Enhetsansvariga/affärsområdesansvariga ska, inom sitt respektive ansvarsområde, säkerställa och verka för att samtliga anställda i Norion Bank har kunskap och information om hur de ska arbeta för och bidra till att uppnå en effektiv och god intern styrning och kontroll.

### 4.6 Kontrollfunktioner

#### 4.6.1 Allmänt om kontrollfunktioner

Norion Bank har tre kontrollfunktioner: Internrevisionen, Riskkontrollfunktionen och Compliancefunktionen.

Kontrollfunktionerna ska vara permanenta, ha de resurser som krävs för att kunna fullgöra sina arbetsuppgifter samt vara oberoende. Med oberoende i detta sammanhang avses att:

- medarbetare i kontrollfunktionerna inte utför uppgifter som ingår i verksamhet de övervakar och kontrollerar,
- funktionerna är organisatoriskt separerade från de funktioner och områden de ska kontrollera,
- ansvarig för respektive kontrollfunktion rapporterar direkt till styrelsen och är regelbundet föredragande vid styrelsens sammanträden, och



- metoden för att fastställa ersättning till personal i kontrollfunktionerna inte äventyrar eller kan komma att äventyra deras objektivitet.

Kontrollfunktionernas arbete ska regleras i, av styrelsen fastställda, styrdokument och årsplaner för respektive funktion. Norion Bank ska även tillse att personalen i en kontrollfunktion löpande utbildas för att hålla kunskapen aktuell samt att kontrollfunktionerna har ändamålsenliga IT-system och stöd till sitt förfogande.

Kontrollfunktionerna ska regelbundet och löpande, åtminstone kvartalsvis, rapportera om väsentliga brister och risker som identifierats till styrelse och VD.

#### 4.6.2 Riskkontrollfunktionen

Riskkontrollfunktionen är Norion Banks funktion för riskkontroll och är direkt underställd VD och rapporterar även direkt till styrelsen.

Riskkontrollfunktionen ansvarar för att kontrollera att alla väsentliga risker som Norion Bank exponeras för identifieras och hanteras av berörda funktioner i affärsverksamheten. Vidare ska Riskkontrollfunktionen kontrollera att Norion Banks interna regelverk avseende riskhantering och riskramverk i övrigt är lämpligt och effektivt samt vid behov föreslå förändringar i regelverket. Riskkontrollfunktionen ska vidare bistå affärsverksamheten med råd och stöd vid implementation av de krav som uppställs genom externa regelverk samt löpande verka för och bidra till att det finns en god riskmedvetenhet inom organisationen.

Riskkontrollfunktionen ska tillse att information om Norion Banks risker regelbundet lämnas till styrelsen och VD. Funktionen ska minst kvartalsvis rapportera till styrelsen om Norion Banks samlade risker och bland annat då redogöra för hur riskexponeringen förhåller sig till fastställd riskaptit. Funktionen ska vidare ge råd och stöd till styrelse eller VD i riskrelaterade frågeställningar samt minst årligen utvärdera tillvägagångssättet och resultatet av genomförd intern kapital- och likviditetsutvärdering.

Riskkontrollfunktionens ansvarsområden och uppgifter är fastställda i *Instruktion för Riskkontrollfunktionen*.

#### 4.6.3 Compliancefunktionen

Compliancefunktionen är Norion Banks funktion för regelefterlevnad och är direkt underställd VD och rapporterar även direkt till styrelsen.

Compliancefunktionen ska identifiera vilka risker det finns för bristande regelefterlevnad i Norion Banks verksamhet och övervaka att dessa risker hanteras av berörda funktioner i affärsverksamheten. Compliancefunktionen ska vidare ansvara för att kontrollera efterlevnaden av de externa och interna regelverk som avser Norion Banks tillståndspliktiga verksamhet samt regelbundet bedöma om Norion Banks rutiner och åtgärder för regelefterlevnad är lämpliga och effektiva. Compliancefunktionen ska vidare bistå affärsverksamheten med råd och stöd vid implementation av de krav som uppställs genom externa regelverk samt löpande verka för och bidra till att det finns en god riskmedvetenhet inom organisationen.

Funktionen ska vidare utvärdera de åtgärder som verksamheten vidtagit för att avhjälpa brister i regelefterlevnaden, ge råd och stöd till anställda, VD och styrelse avseende externa regelverk som avser Norion Banks tillståndspliktiga verksamhet, interna regelverk samt informera och

utbilda berörda anställda i Norion Bank om nya eller ändrade regler. Compliancefunktionen ska minst kvartalsvis rapportera till styrelsen och löpande till VD om regelefterlevnaden i Norion Bank.

Compliancefunktionens ansvarsområden och uppgifter är fastställda i *Instruktion för Compliancefunktionen*.

#### **4.6.4 Internrevisionsfunktionen**

Internrevisionen är Norion Banks funktion för internrevision och är direkt underställd styrelsen. Internrevisionen i Norion Bank är utlagd till en extern uppdragstagare.

Internrevisionen utgör styrelsens redskap för att uppfylla kraven på en god och effektiv intern styrning och kontroll. Internrevisionen ska mot bakgrund av detta vara helt organisatoriskt skild från Norion Banks övriga funktioner och verksamhet.

Internrevisionen ska granska och regelbundet utvärdera om den interna styrningen och kontrollen i Norion Bank är effektiv och ändamålsenlig. Inom ramen för detta ska funktionen bland annat granska och regelbundet utvärdera Norion Banks riskhantering, efterlevnad av externa och interna regelverk samt de andra två kontrollfunktionerna.

Funktionen ska regelbundet och minst årligen avlägga rapport till styrelsen som omfattar planering, granskning, rapportering samt förslag till åtgärder.

Internrevisionens ansvarsområden och uppgifter är fastställda i *Instruktion för internrevision*.

#### **4.6.5 Information till kontrollfunktioner**

I syfte att främja och upprätthålla en god intern kontrollmiljö ska samtliga funktioner och anställda underrätta Riskkontrollfunktionen respektive Compliancefunktionen om förhållanden som negativt påverkar den interna kontrollen i Norion Bank i enlighet med Norion Banks interna regler. Kontrollfunktionerna ska ha rätt att få tillgång till samtlig information som behövs för att kontrollfunktionerna ska kunna fullgöra sina uppdrag. Kontrollfunktionerna ska i sin tur hantera denna information med den varsamhet som krävs i varje enskilt fall.

## **5. Kontrollmiljö**

### **5.1 De tre försvarslinjerna**

För att kunna hantera risker på ett tillfredsställande sätt är det viktigt att det finns en genomtänkt och tydlig intern styrning och kontroll som genomsyrar organisationen. Styrelsen i Norion Bank har det yttersta ansvaret för att se till att Norion Bank har en god kontrollmiljö.

För att uppnå en god kontrollmiljö ska Norion Bank tillämpa den s.k. principen om tre försvarslinjer, där de olika försvarslinjerna har olika ansvarsområden men med ett gemensamt ansvar för att uppnå en god intern styrning och kontroll. Norion Banks hela organisation är delaktig i denna kontrollmiljö.

Modellen beskrivs nedan tillsammans med den organisatoriska ansvarsfördelningen.

## 5.2 Första försvarslinjen

Den första försvarslinjen består av hela verksamheten och samtliga anställda utom de som tillhör kontrollfunktionerna, dvs. andra och tredje försvarslinjen. Första försvarslinjen leds av VD och består av den affärsdrivande och operativa verksamheten. I den första linjen innefattas även stödjande enheter.

Den första försvarslinjen är den del av verksamheten som är risktagande och ska därför hantera de dagliga risker som uppkommer, bl.a. genom att efterleva både interna och externa regelverk.

## 5.3 Andra försvarslinjen

Den andra försvarslinjen består av Riskkontrollfunktionen och Compliancefunktionen som utgör oberoende kontrollfunktioner, se avsnitt 4.6 ovan. Funktionerna i den andra linjen ansvarar för att kontrollera att den första linjen följer interna och externa regelverk. Vidare ska den andra linjen vara ett stöd till den första linjen avseende arbetet med intern styrning och kontroll och att arbeta proaktivt för att skapa en bra och effektiv kontrollmiljö i Norion Bank. Även Bankens DPO-funktion ingår i den andra försvarslinjen, liksom bankens CFA. Den andra försvarslinjen ansvarar även för att analysera, följa upp samt rapportera arbetet till styrelse och VD.

## 5.4 Tredje försvarslinjen

Den tredje försvarslinjen består av Internrevisionen som är en, från verksamheten, helt oberoende granskningsfunktion, se avsnitt 4.6 ovan. Internrevisionen ansvarar för att, bland annat, granska det arbete som utförs av den första och andra försvarslinjen, och rapporterar direkt till styrelsen.

## 6. Internt regelverk

Norion Bank har ett internt regelverk, bestående av policyer, VD-instruktioner och riktlinjer samt andra skriftliga dokument och som fastställts av Norion Banks styrelse, VD och/eller enhetsansvariga/affärsområdesansvariga och genom vilka verksamheten i Norion Bank styrs. Processen och hierarkin för bankens interna regelverk beskrivs närmare i instruktionen "Process för Styrdokument".

Övergripande gäller att det genom externa regelverk framgår i regel vilken funktion, styrelse eller VD, som ska fastställa ett specifikt internt regelverk. Norion Bank kan därför besluta om att styrdokument ska fastställas på en högre nivå än vad som regleras i externa regelverk, dock aldrig på en lägre beslutsnivå.

<i>Nivå</i>	<i>Typ av dokument</i>	<i>Innehåll</i>	<i>Beslutas av</i>
1	Policy/styrelsens och dess utskotts arbetsordningar	Övergripande principer och ansvarsområden	Styrelsen
2	Instruktion	Tydliggör vad som ska göras och hur detta kontrolleras	VD (dock styrelsen avseende instruktioner för kontrollfunktionerna och VD)
3	Riktlinjer	Beskriver i detalj hur arbete ska utföras	Enhetsansvariga inom sitt respektive ansvarsområde

Det interna regelverket ska tillgängliggöras dels i tillämpliga delar för Norion Banks anställda i icke-redigerbar form på bankens intranät, dels i den mån det är lämpligt även på bankens webb-sida. Det är VD som ytterst fattar beslut om spridning av internt regelverk.

Den funktion som ansvarar för samordning vid årlig revidering av styrdokument på nivå 1-2 är CEO Office.

## 7. Process för regelverksbevakning

För att skapa förutsättningar för ett proaktivt arbete med nya och förändrade externa regler ska Norion Bank ha en etablerad process för regelverksbevakning och den beskrivs närmare i VD-instruktionen Process för regelverksbevakning.

Övergripande säkerställer bankens process efterlevnad av gällande externa regler och implementering av dessa regelkrav i Norion Banks interna regler och verksamhet.

Compliancefunktionen har det huvudsakliga ansvaret för processen som inbegriper identifikation av nya regelverk, tilldelande av ägarskap, analys samt fördelning av implementationsansvar. I funktionens ansvar ingår även att till styrelsen rapportera regelverksförändringar, för den tillståndspliktiga verksamheten. Rapporteringen ska bl.a. innehålla information om hur och i vilken utsträckning förändringen påverkar Norion Bank och status vad gäller implementeringen. Implementering av nya regler i första linjen ska ombesörjas av första linjen med stöd av Juridik och Compliance.

## 8. Riskhanteringsramverk

### 8.1 Allmänt

Styrelsen har det yttersta ansvaret för Norion Banks riskhanteringsramverk, inom vilket Norion Banks riskhanteringsprocesser inryms. Norion Banks ramverk för riskhantering innefattar alla de strategier, processer, rutiner, interna regler, limiter, kontroller och rapporteringsrutiner som utgör en ram för riskhanteringen. Ramverket formas bland annat, men inte uteslutande, av *Riskpolicy*, *Policy för intern styrning och kontroll*, *Finanspolicy*, *Kreditpolicy* och *Policy för Operativa risker*, samt även de interna instruktioner och rutiner som underordnas dessa policydokument.

Nedan följer en översiktlig beskrivning av riskhanteringsramverket. Ramverket beskrivs mer utförligt i främst Bankens *Riskpolicy* men även i övriga riskrelaterade interna regelverk.

### 8.2 Riskkultur

Norion Bank eftersträvar att ha en organisation med hög riskmedvetenhet kombinerat med ett balanserat risktagande. Att ha en hög riskmedvetenhet innebär bland annat att varje anställd förstår vilka potentiella risker dennes arbetsuppgifter är förknippade med för Norion Bank, den nivå på risktagande som är acceptabel och hur den anställda ska agera för att inte överskrida

den accepterade risknivån. Ett balanserat risktagande uppnås genom förankring i styrelsen, hög riskmedvetenhet och en tydlig beslutsordning för anställda.

Att ta kalkylerade risker är en grundläggande del av den verksamhet som Banken bedriver vilket innebär att risken alltid ska ställas i relation till förväntad avkastning. Medarbetare på alla nivåer bör ha en hög riskmedvetenhet och förstå Norion Banks värderingar som ligger till grund för en sund riskkultur samt principen med de tre försvarslinjerna. För att skapa en god förståelse för de risker som verksamheten exponeras för samt säkerställa en sund och bra hantering av dessa har Banken i Riskpolicyn ställt upp följande grundläggande principer avseende riskkultur:

- Ansvar för riskhantering
- Genomlysning, ifrågasättande och öppenhet
- Ersättningssystem
- Ledningen som förebild – "Tone from the Top"

### 8.3 Riskhanteringsprocess

Riskhanteringsprocessens syfte är att möjliggöra en effektiv identifiering, bedömning och kontroll av de risker som uppstår i verksamheten i Norion Bank. Processen ska vara väl integrerad i Norion Bank eftersom dess effektivitet är avgörande för Norion Banks långsiktiga lönsamhet och stabilitet. Att kunna identifiera, bedöma och kontrollera de risker som uppstår i verksamheten gör det möjligt att medvetet acceptera önskvärda risker och prissätta dem korrekt.

En löpande uppföljning och rapportering av Norion Banks riskprofil från både första och andra försvarslinjen gör det möjligt för styrelse och VD att förstå om risktagandet ligger inom de fastställda riskkaptiterna och inte utvecklas i en riktning så att riskkaptiterna riskerar brytas framgent.

### 8.4 Riskstrategier och riskkaptit

Riskstrategier fastställda av styrelsen beskriver hur Norion Bank ska ta på sig, styra och ha kontroll över de huvudsakliga riskerna Norion Bank är eller kan bli exponerad för. Norion Banks riskstrategier, vilka beskrivs i *Riskpolicyn*, beskriver hur de huvudsakliga riskerna uppstår i verksamheten samt styrningen av dessa.

Norion Bank ska generellt ha en balanserad riskprofil med en diversifierad kreditportfölj och samtidigt begränsa exponeringen mot de valuta- och ränterisker som uppstår till följd av verksamheten. Andra risker av till exempel operativ art ska, om det bedöms vara kostnadseffektivt, minimeras genom förebyggande åtgärder och kontroller.

Riskkaptiterna i Norion Bank utgörs av kvalitativa och mätbara kvantitativa mått med nivå och inriktning för den risk som kan accepteras för att de strategiska målen ska uppfyllas.

Styrelsens beslutade riskkaptitmått för de huvudsakliga riskkategorierna framgår av *Riskpolicyn*.

## 9. Övriga processer för intern styrning i banken

Banken ska upprätthålla ett flertal andra väsentliga, utöver ovan nämnda process för regelverksbevakning, processer såsom led i bankens interna styrning. Varje process ska ägas

av en ledande befattningshavare och finnas med i dennes mandatbeskrivning. Styrelsen ansvarar ytterst för att årligen uppdatera respektive policy som hanterar processen. Dessa är:

- Utläggning av arbete eller funktioner ("outsourcing")
- Process för visseblåsning
- Process för ersättningsregelverket
- NPAP
- Kontinuitetsprocessen
- Process för IKT-regelverket

## 10. Etiska frågor

Norion Bank ska ha interna regler för att säkerställa att verksamheten bedrivs på ett sunt och etiskt försvarbart sätt. Rutinerna ska stödja medarbetare, styrelse och övriga inom Norion Bank i hur man ska handla i etiska frågor eller där rättsreglerna på området inte ger tillräcklig vägledning. Rutinerna beskrivs i Norion Banks *Code of Conduct*.

Norion Bank ska ha ett särskilt inrättat rapporteringssystem för anställda som vill göra anmälningar om misstänkta allvarliga fall av överträdelser av externa och interna regelverk av ledande befattningshavare som gäller för verksamheten när de normala rapporteringsvägarna inte bedöms vara lämpliga (s.k. visseblåsning).

Norion Banks rapporteringssystem är beskrivet i *Policy för visseblåsning*.

Norion Bank ska ha dokumenterade interna regelverk kring rutiner för att identifiera, dokumentera och hantera faktiska och potentiella intressekonflikter i verksamheten. Processer och rutiner för identifiering och hantering av intressekonflikter beskrivs i Norion Banks *Policy för hantering av intressekonflikter*.

Hållbarhet regleras i bankens *Hållbarhetspolicy* och bankens *Miljöpolicy* beskriver bankens interna arbete med egen miljöpåverkan. Instruktionen "*Röda Listan*" ger hänvisning i fråga om kreditgivning sektorsvis och utifrån bankens strategiska hållbarhetsram.

AML regleras i bankens AML-policy och underliggande styrdokument. Policyn beskriver bankens strategi och åtgärder för att motverka penningtvätt och finansiering av terrorism liksom för att säkra efterlevnaden av internationella sanktioner. I Norion Banks policy återfinns bland annat de interna regler som gäller för särskild utsedd befattningshavare (SUB), den centralt funktionsansvariga (CFA) och den oberoende granskningsfunktionen.

## 11. Förmedling av låneskyddsförsäkringar

Banken har interna regler för kontroll av kunskap och kompetens hos berörda anställda i enlighet med de externa krav som ställs på banken såsom försäkringsdistributör. Detta för att säkerställa anställdas kompetens, insikt och erfarenhet samt skötsamhet i ekonomiska angelägenheter inom försäkringsdistribution. VD eller den VD utser, ska ha ansvaret för att dessa interna regler regelbundet, minst årligen, utvärderas och uppdateras om så behövs.

De interna reglerna ska ha en ändamålsenlig och överblickbar organisationsstruktur. Krav som gäller i förhållande till ledningspersoners insikt och erfarenhet av försäkringsdistribution, samt skötsamhet i ekonomiska angelägenheter, regleras i Norion Banks övergripande Policy för

lämplighetsbedömning.

Norion ska bedriva sin verksamhet enligt god försäkringsdistributionssed och med tillbörlig omsorg ta tillvara kundens intressen. Därtill ska banken handla hederligt, rättvist och professionellt.

Banken ska anpassa sin rådgivning efter kundens önskemål samt behov och endast rekommendera lösningar som är lämpliga för kunden. Informationen ska presenteras på ett tydligt och enkelt sätt för att kunden ska kunna fatta ett välgrundat beslut innan ett eventuellt avtal ingås. Banken ska avråda en kund från att vidta åtgärder som inte kan anses lämpliga med hänsyn till kundens behov, ekonomiska förhållanden eller andra omständigheter. Banken ska erbjuda låneskyddsförsäkringen med en reservationsanslutning såsom beskriven i bankens instruktion för försäkringsförmedling.

Bankens interna regler återfinns i Instruktionen samt riktlinjer för försäkringsdistribution.

## **12. Dokumentationsrutiner**

För att säkerställa god intern styrning, kontroll och spårbarhet krävs etablerade dokumentationsrutiner. Norion Banks styrelse, kontrollfunktioner samt externa parter ska kunna följa verksamhetens regelefterlevnad, och i förekommande fall, de brister som rapporteras och vilka åtgärder som vidtagits för att hantera dessa. Norion Bank ska bevara relevanta uppgifter som avser verksamheten och den interna organisationen i minst fem år.

## **13. Uppföljning och fastställande**

### **13.1 Efterlevnad och uppföljning**

Styrelsen är ytterst ansvarig för Norion Banks verksamhet och därmed även ytterst ansvarig för att verksamheten bedrivs i enlighet med denna policy. Var och en som omfattas av denna policy är även ansvarig för att efterleva policyn.

Styrelsen ansvarar för att säkerställa att uppföljning och kontroll av efterlevnaden av denna policy sker.

### **13.2 Uppdatering och fastställande**

Policyn ska uppdateras och fastställas av Styrelsen när det föranleds av nya eller förändrade externa regelverk samt av relevanta förändringar i Norion Banks organisation och verksamhet. Policyn ska dock fastställas av Styrelsen minst årligen även om inga förändringar är påkallade.

Head of CEO Office ansvarar för att föreslå ändringar i policyn och att den är uppdaterad i enlighet med gällande lagar och regler. Head of CEO Office ska se över och eventuellt revidera policyn inför Styrelsens beslut.