Europeiska bankmyndigheten EBA BS 2011 116 slutlig

27 september 2011

Europeiska bankmyndighetens riktlinjer för intern styrning

(GL 44)

London den 27 september 2011

Europeiska bankmyndighetens riktlinjer för intern styrning

Riktlinjernas status

1. Riktlinjerna i detta dokument har utfärdats på grundval av artikel 16 i Europaparlamentets och rådets förordning (EU) nr 1093/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska bankmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/78/EG (”EBA-förordningen”). Enligt artikel 16.3 i EBA-förordningen ska behöriga myndigheter och aktörer på den finansiella marknaden med alla tillgängliga medel söka följa riktlinjerna.

2. Riktlinjerna visar vad EBA anser vara lämplig tillsynspraxis inom det europeiska systemet för finansiell tillsyn och hur EU-lagstiftningen bör tillämpas inom ett visst område. Om inte annat anges förväntar sig EBA därför att alla behöriga myndigheter och finansmarknadsaktörer som berörs av riktlinjerna också följer dessa. Behöriga myndigheter som berörs av riktlinjerna bör följa dem genom att på lämpligt sätt införliva dem med sin tillsynspraxis (till exempel genom att ändra sin legala ram eller sina tillsynsbestämmelser och/eller vägledningss- eller tillsynsprocesser), även när särskilda riktlinjer i första hand riktas till finansinstitut.

Rapporteringskrav

3. De behöriga myndigheterna ska meddela EBA om de följer eller har för avsikt att följa dessa riktlinjer, eller av vilka skäl de inte avser att följa dem, senast den 28 november 2011. Informationen bör lämnas till compliance@eba.europa.eu av personer med befogenhet att rapportera regelefterlevnad för sina behöriga myndigheters räkning.

4. De behöriga myndigheternas anmälningar ska offentliggöras på EBA:s webbplats i enlighet med artikel 16 i EBA-förordningen.

På vissa ställen i den text som följer har vi lagt in kommentarer till riktlinjerna, antingen för att exemplifiera eller för att förklara vad som ligger bakom olika bestämmelser. Denna förklarande text visas då i inramade textrutor.

Innehåll

Europeiska bankmyndighetens riktlinjer för intern styrning 2

Kapitel I – Syfte, tillämpningsområde och definitioner 6

1. Syfte 6

2. Tillämpningsområde och tillämpningsnivå 6

3. Definitioner 6

Kapitel II – Krav på institutens interna styrning 6

A. Företagets struktur och organisation 6

4. Organisatoriskt ramverk 6

5. Kontroller och maktfördelning i en koncernstruktur 7

6. Kunskap om strukturen 8

7. Verksamhet som inte är standardmässig eller som inte medger insyn 9

B. Ledningsorgan 11

B.1 Ledningsorganets uppgifter och ansvarsområden 11

8. Ledningsorganets ansvarsområden 11

9. Bedömning av ramverket för den interna styrningen 12

10. Ledningsorganets övervakande och ledande funktioner 12

B.2 Ledningsorganets sammansättning och arbetssätt 13

11. Ledningsorganets sammansättning samt utnämning av ledamöter och efterträdare för dessa 13

12. Åtaganden, oberoende och hantering av intressekonflikter i ledningsorganet 14

13. Ledamöternas kvalifikationer 15

14. Ledningsorganets arbetssätt 16

Bedömning av ledningsorganets funktionssätt 16

Ordförandens roll 16

Ledningsorganets kommittéer 17

Revisionskommitté 18

Riskkommittén 18
B.3 Ramverk för uppförande 19
15. Företags värderingar och uppförandekod 19
16. Intressekonflikter på institutsnivå 19
17. Interna rutiner för uppgiftslämning 20
B.4 Policyer om uppdragsavtal och ersättningar 20
18. Uppdragsavtal 20
19. Styrning av ersättningspolicyn 21
C. Riskhantering 22
20. Riskkultur 22
21. Överensstämmelse mellan ersättningspolicyn och riskprofilen 23
22. Ramverk för riskhanteringen 24
23. Nya produkter 26
D. Internkontroll 26
24. Ramverk för internkontroll 26
25. Riskkontrollfunktionen 28
26. Riskkontrollfunktionens roll 28
Riskkontrollfunktionens roll i fråga om strategi och beslutsfattande .. 29
Riskkontrollfunktionens roll i fråga om transaktioner med närstående parter 29
Riskkontrollfunktionens roll i fråga om den legala strukturens komplexitetsgrad 29
Riskkontrollfunktionens roll i fråga om väsentliga förändringar 29
Riskkontrollfunktionens roll i fråga om mätningar och bedömningar . 30
Riskkontrollfunktionens roll i fråga om övervakningen 30
Riskkontrollfunktionens roll i fråga om icke godkända exponeringar . 31
27. Riskchefen 31
28. Regelefterlevnadsfunktionen 32
29. Internrevisionsfunktionen 33

E. Informationssystem och kontinuitetsplanering 34
30. Informationssystem och kommunikation 34
31. Kontinuitetshantering 35
F. Insyn 36
32. Delaktighet 36
33. Insyn i den interna styrningen 36
Kapitel III – Slutbestämmelser och genomförande 37
34. Upphävanden 37
35. Ikraftträdande 37

Kapitel I – Syfte, tillämpningsområde och definitioner

1. Syfte

Syftet med dessa riktlinjer är att harmonisera förväntningarna på tillsynen och underlätta tillämpningen av sunda interna styrformer i linje med artikel 22 och bilaga V i direktiv 2006/48/EG och de nationella bolagslagarna.

2. Tillämpningsområde och tillämpningsnivå

1. De behöriga myndigheterna bör kräva att finansinstituten följer bestämmelserna i dessa riktlinjer om intern styrning.
2. Tillämpningen av riktlinjerna bör granskas av behöriga myndigheter som en del av deras gransknings- och utvärderingsprocess.

Förklarande not:
CEBS/EBA har utarbetat riktlinjer för tillsynsmyndigheternas granskning. Dessa finns på EBA:s webbplats.

3. Om inte annat anges gäller riktlinjerna för fristående institut liksom för moderbolag och dotterbolag på konsoliderad eller underkonsoliderad nivå.
4. Den proportionalitet som avses i direktiven 2006/48 och 2006/49 (i dess ändrade lydelse) är tillämplig på alla bestämmelser i riktlinjerna. Ett institut kan visa hur det med hänsyn till verksamhetens art, omfattning och komplexitet, uppfyller kraven i riktlinjerna.

3. Definitioner

1. I dessa riktlinjer avses med *ledningsorgan* det eller de organ som har en övervakande och ledande funktion inom ett institut, som är det högsta beslutande organet och som har befogenheter att fastställa institutets strategi, mål och övergripande inriktning. Personer som leder ett instituts verksamhet anses ingå i ledningsorganet.
2. I dessa riktlinjer avses med *institut* kreditinstitut och värdepappersföretag, i enlighet med direktiven 2006/48/EG och 2006/49/EG.

Kapitel II – Krav på institutens interna styrning

A. Företagets struktur och organisation

4. Organisatoriskt ramverk

1. Ett instituts ledningsorgan bör se till att institutet har en lämplig och transparent företagsstruktur. Strukturen bör främja och visa att institutet leds på ett ändamålsenligt och ansvarsfullt sätt både på företags- och koncernnivå. Rapporteringsvägarna och fördelningen av

ansvar och befogenheter inom ett institut bör vara tydliga, väl definierade och konsekventa, och tillämpningen ska kontrolleras.

2. Ledningsorganet bör se till att institutets och, i tillämpliga fall koncernens, struktur är tydlig och transparent både för den egna personalen och för tillsynsmyndigheterna.
3. Ledningsorganet bör göra en bedömning av hur de olika delarna i företagets struktur kompletterar och interagerar med varandra. Strukturen bör inte vara sådan att den hindrar ledningsorganet från att övervaka och hantera de risker som institutet eller koncernen ställs inför på ett ändamålsenligt sätt.
4. Ledningsorganet bör göra en bedömning av hur förändringar av koncernens struktur påverkar dess sundhet. Ledningsorganet bör skyndsamt genomföra nödvändiga justeringar.

Förklarande not:
Förändringar kan till exempel bero på att nya dotterbolag bildas, fusioner och förvärv, att delar av koncernen säljs eller avvecklas, eller externa faktorer.

5. Kontroller och maktfördelning i en koncernstruktur

1. I en koncernstruktur bör ledningsorganet för institutets moderbolag ha det övergripande ansvaret för att den interna styrningen i hela koncernen är tillräcklig och för att se till att det finns ett ramverk för styrning som lämpar sig för koncernens och koncernföretagens struktur, verksamhet och risker.
2. Ledningsorgan för dotterbolag i en koncern som står under tillsyn bör tillämpa samma värderingar och policyer för intern styrning på bolagsnivå som moderbolaget, om inte annat följer av legala eller tillsynsmässiga krav eller proportionalitetshänsyn. Således bör ledningsorgan för dotterbolag som står under tillsyn fastställa egna policyer inom ramen för sina skyldigheter i fråga om den interna styrningen, och analysera beslut och metoder på koncernnivå i syfte att kontrollera att de inte leder till att dotterbolaget bryter mot tillämpliga bestämmelser i lagar och författningar eller mot tillsynsregler. Ledningsorgan för dotterbolag som står under tillsyn bör också kontrollera att sådana beslut eller metoder inte inverkar negativt på

   a. den sunda och ansvarsfulla ledningen av dotterbolaget,

   b. dotterbolagets finansiella situation,

   c. dotterbolagets intressenters legala intressen.

3. Ledningsorganen för både moderbolaget och dotterbolagen bör tillämpa och ta hänsyn till nedanstående punkter, med beaktande av hur koncerndimensionen påverkar deras interna styrning.

4. När ledningsorganet för ett instituts moderbolag fullgör sina skyldigheter i fråga om den interna styrningen bör det vara medvetet om alla de risker och problem av betydelse som kan beröra koncernen, moderinstitutet självt och dess dotterbolag. Därför bör det utöva en tillräcklig övervakning av dotterbolagen, samtidigt som det respekterar de särskilda legala skyldigheter i fråga om den interna styrningen som ledningsorgan för dotterbolag som står under tillsyn har.
5. För att fullgöra sina skyldigheter i fråga om den interna styrningen bör ledningsorgan för instituts moderbolag

    a. upprätta en ledningsstruktur som bidrar till effektiv övervakning av dotterbolagen och tar hänsyn till de olika risker – deras art, omfattning och komplexitet – som koncernen och dotterbolagen är exponerade för,

    b. fastställa en policy för den interna styrningen på koncernnivå för dotterbolagen, vilken inkluderar ett åtagande att uppfylla alla tillämpliga krav på styrningen,

    c. se till att alla dotterbolag har tillräckliga resurser för att kunna leva upp till såväl koncernens standarder som lokala standarder för bolagsstyrningen,

    d. ha de resurser som krävs för att övervaka att alla dotterbolag uppfyller alla tillämpliga krav på den interna styrningen och

    e. se till att koncernens rapporteringsvägar är tydliga och transparenta, i synnerhet när verksamhetsområdena inte överensstämmer med koncernens legala struktur.

6. Dotterbolag som står under tillsyn bör överväga att förstärka sin styrning med ett tillräckligt antal oberoende medlemmar av ledningsorganet. Oberoende medlemmar av ledningsorgan är icke verkställande direktörer som inte har några beroenden till moderbolaget och koncernen, eller till den kontrollerande aktieägaren.

6. Kunskap om strukturen

1. Ledningsorganet bör vara ordentligt insatt i och förstå institutets operativa struktur och se till att den överensstämmer med den fastställda affärsstrategin och riskprofilen.

Förklarande not:
Det är mycket viktigt att ledningsorganet är ordentligt insatt i och förstår institutets operativa struktur. När ett institut skapar många juridiska personer inom sin koncern kan deras antal och i synnerhet förbindelserna och transaktionerna mellan dem ställa till med problem när det gäller utformningen av den interna styrningen och hanteringen och övervakningen av riskerna i koncernen som helhet, vilket i sig utgör en risk.

2. Ledningsorganet bör styra och förstå institutets struktur, hur den förändras och vilka begränsningar den har. Det bör också se till att strukturen är motiverad och inte onödigt eller obefogat komplicerad. Det ansvarar också för att sunda strategier och policyer för inrättandet av nya strukturer fastställs. Ledningsorganet bör också vara medvetet om de risker som komplexitetsgraden hos den juridiska personens struktur som sådan utgör, och se till att institutet skyndsamt kan ta fram information om alla juridiska personers art, stadgar, ägarförhållanden och verksamheter.
3. Ledningsorganet för ett instituts moderbolag bör inte bara förstå koncernens företagsstruktur, utan också syftet med dess olika enheter och beroenden och förbindelserna mellan dem. Detta inbegriper förståelse av koncernspecifika operativa risker, exponeringar inom koncernen och hur koncernens finansiering, kapital och riskprofiler kan påverkas under normala och ogynnsamma omständigheter.
4. Ledningsorganet för ett instituts moderbolag bör se till att de olika enheterna i koncernen (inklusive institutet självt) får tillräcklig information för att ha en tydlig bild av koncernens allmänna målsättningar och risker. Alla flöden av viktig information mellan enheterna som är relevanta för koncernens operativa verksamhet bör dokumenteras och på begäran skyndsamt göras tillgänglig för ledningsorganet, kontrollfunktionerna och/eller tillsynsmyndigheterna, beroende på omständigheterna.
5. Ledningsorganet för ett instituts moderbolag bör hålla sig informerat om de risker som koncernens struktur medför. Detta inbegriper

    a. information om viktiga riskfaktorer och

    b. regelbundna rapporter med granskningar av institutets övergripande struktur och utvärderingar av hur enskilda enheters verksamhet överensstämmer med den fastställda strategin.

7. Verksamhet som inte är standardmässig eller som inte medger insyn

1. Ledningsorgan för institut som verkar genom bolag som bildats för särskilda ändamål eller därmed förknippade bolag eller i jurisdiktioner som förhindrar insyn eller inte lever upp till internationella standarder för bankverksamhet bör vara medvetna om dessa strukturers syfte och uppbyggnad, liksom om de särskilda risker de medför. Ledningsorganet bör endast godkänna sådan verksamhet om det är övertygat om att riskerna kommer att hanteras på lämpligt sätt.

Förklarande not: Vid sidan av denna princip kan de behöriga myndigheterna också tillämpa *”Core Principles for Effective Banking Supervision”*, som har utarbetats av Baselkommittén för banktillsyn, när de bedömer företags verksamhet i jurisdiktioner där full insyn saknas eller där internationella bankstandarder inte efterlevs.

Institut kan ha legitima skäl att verka i vissa jurisdiktioner (eller ha samarbetspartner eller motparter som verkar i dessa) eller att skapa särskilda strukturer (till exempel bolag för särskilda ändamål eller företagsstiftelser). Men att verka i jurisdiktioner där full insyn saknas eller där internationella bankstandarder inte efterlevs (till exempel i fråga om tillsyn, skatter, penningtvätt och finansiering av terrorism) eller genom komplicerade strukturer eller strukturer som inte medger insyn kan medföra särskilda legala och finansiella risker samt ryktesrisker. Det kan också innebära att ledningsorganet inte kan övervaka företagets verksamhet ordentligt och förhindra en effektiv banktillsyn. Sådana strukturer bör därför endast införas och upprätthållas om syftet har fastställts och förstås, om effektiv övervakning finns och om alla väsentliga risker som dessa strukturer kan generera kan hanteras på lämpligt sätt.

Därför bör ledningsorganen uppmärksamma alla dessa situationer särskilt, eftersom de gör det svårt att få en klar bild av koncernens struktur.

2. Ledningsorganen bör fastställa och upprätthålla lämpliga strategier, policyer och rutiner för införande och upprätthållande av sådana strukturer och verksamheter och se över dem fortlöpande för att se till att de överensstämmer med det avsedda syftet.
3. Ledningsorganen bör se till att lämpliga åtgärder vidtas för att eliminera eller mildra riskerna av sådan verksamhet. Det innebär att

    a. institutet har lämpliga policyer och rutiner och dokumenterade processer (till exempel tillämpliga limiter, informationskrav) för bedömning och godkännande av sådan verksamhet och riskhantering i samband med den, med hänsyn tagen till följderna för koncernens operativa struktur,

    b. information om denna verksamhet och dess risker ska vara tillgänglig för institutets huvudkontor och revisorer och redovisas för ledningsorganet och tillsynsmyndigheterna samt att

    c. institutet med jämna mellanrum ska utvärdera om det finns ett fortsatt behov av att bedriva verksamhet som hindrar insyn.

4. Samma åtgärder bör vidtas när institut bedriver verksamhet för kunders räkning som inte är standardmässig eller som inte medger insyn.

Förklarande not:

Verksamhet för kunders räkning som inte är standardmässig eller som inte medger insyn (till exempel att bilda bolag i utländska jurisdiktioner, skapa komplicerade strukturer och finansiera transaktioner för dessa eller tillhandahålla förvaltartjänster) innebär att man ställs inför liknande utmaningar för den interna styrningen, och kan medföra betydande

operativa risker och ryktesrisker. Därför måste samma riskhanteringsåtgärder vidtas som när det gäller institutens egen verksamhet.

5. Alla dessa strukturer och all verksamhet bör vara föremål för regelbunden granskning av interna och externa revisorer.

B. Ledningsorgan

B.1 Ledningsorganets uppgifter och ansvarsområden

8. Ledningsorganets ansvarsområden

1. Ledningsorganet bör ha det övergripande ansvaret för institutet och fastställa dess strategi. Ledningsorganets ansvarsområden bör vara tydligt definierade i ett skriftligt dokument och godkända.

Förklarande not:

Att ledningsorganet fullgör sina skyldigheter på ett korrekt sätt är förutsättningen för en sund och ansvarsfull ledning av institutet. De dokumenterade ansvarsområdena måste också överensstämma med den nationella bolagslagstiftningen.

2. Några av ledningsorganets viktigaste uppgifter bör vara att fastställa och övervaka

    a. institutets övergripande affärsstrategi inom det tillämpliga legala regelverket, med hänsyn tagen till institutets långsiktiga ekonomiska intressen och solvens,

    b. institutets övergripande riskstrategi och riskpolicy, inklusive dess risktolerans/riskaptit och ramverket för dess riskhantering,

    c. hur mycket internt kapital och egna medel, och av vilket slag, som krävs för att täcka institutets risker, och hur detta ska vara fördelat,

    d. en stabil och transparent organisatorisk struktur med effektiva kommunikations- och rapporteringskanaler,

    e. en policy för tillsättning av personer på nyckelbefattningar inom institutet och utnämning av efterträdare,

    f. ett system för ersättningar som överensstämmer med institutets riskstrategier,

    g. institutets styrningsprinciper och värderingar, däribland en uppförandekod eller ett jämförbart dokument och

h. ett lämpligt och ändamålsenligt ramverk för intern kontroll, som inkluderar väl fungerande funktioner för riskkontroll, regelefterlevnad och intern revision, samt ett lämpligt ramverk för finansiell rapportering och redovisning.

3. Ledningsorganet bör också se över och modifiera dessa policyer och strategier med jämna mellanrum. Ledningsorganet ska se till att det finns en god kommunikation med tillsynsmyndigheter och andra berörda parter.

9. Bedömning av ramverket för den interna styrningen

1. Ledningsorganet bör övervaka institutets ramverk för den interna styrningen och regelbundet bedöma hur ändamålsenlig den är.
2. Ramverket för den interna styrningen och tillämpningen av det bör ses över minst en gång om året. Denna översyn bör inrikta sig på eventuella förändringar av interna och externa faktorer som påverkar institutet.

10. Ledningsorganets övervakande och ledande funktioner

1. Det bör finnas en ändamålsenlig samverkan mellan ledningsorganets övervakande och ledande funktioner.

Förklarande not:

Vanligen använder medlemsstaterna en **styrningsstruktur** med antingen en enda styrelse eller dubbla styrelser. I båda fallen har ledningsorganets ledningsfunktion och dess övervakande funktion separata roller inom institutets ledning, direkt eller via kommittéer.

Ledningsfunktionen anger vilken inriktning institutet ska ha, ser till att strategin tillämpas och ansvarar för institutets löpande verksamhet.

Den övervakande funktionen granskar ledningsfunktionen och ger den råd. Arbetet innebär att konstruktivt bidra till en väl underbyggd strategi för institutet, övervaka ledningsfunktionen och kontrollera i vilken utsträckning fastställda mål och målsättningar uppnås, samt se till att den finansiella informationen är fullständig och att riskhanteringen och den interna kontrollen är ändamålsenliga.

För att uppnå en god styrning bör institutets ledningsfunktion och dess övervakande funktion samverka på ett effektivt sätt för att genomföra institutets fastställda strategi och i synnerhet för att hantera de risker som institutet exponeras för. Det kan finnas stora skillnader mellan olika länders lagstiftning och regelverk, men detta bör inte hindra att dessa båda funktioner samverkar på ett ändamålsenligt sätt, oavsett om ledningsorganet består av en eller flera styrelser.

2. För att fullgöra sin övervakande funktion bör ledningsorganet

a. vara berett att ifrågasätta och genomföra kritiska och konstruktiva granskningar av förslag, förklaringar och information från medlemmarna av ledningsorganets ledningsfunktion,

b. övervaka att institutets strategi, risktolerans/riskaptit och policyer tillämpas konsekvent och att prestationsstandarder upprätthålls i linje med dess långsiktiga ekonomiska intressen och solvens, samt

c. övervaka hur medlemmarna av ledningsfunktionen fullgör sina uppdrag i förhållande till dessa standarder.

3. Ledningsorganets ledningsfunktion bör samordna institutets verksamhet och riskstrategier med den övervakande funktionen och regelbundet diskutera med den övervakande funktionen hur dessa strategier tillämpas.
4. Båda funktionerna bör informera varandra i tillräcklig utsträckning. Ledningsfunktionen bör regelbundet och utan dröjsmål vid behov lämna heltäckande information till övervakningsfunktionen om faktorer som inverkar på bedömningen av en specifik situation, ledningen av institutet och bibehållandet av dess finansiella stabilitet.

B.2 Ledningsorganets sammansättning och arbetssätt

11. Ledningsorganets sammansättning samt utnämning av ledamöter och efterträdare för dessa

1. Ledningsorganet bör bestå av ett tillräckligt antal ledamöter och ha en lämplig sammansättning. Det bör ha policyer för utnämning och övervakning av ledamöterna samt för successionsplanering.
2. Institutet bör fastställa ledningsorganets storlek och sammansättning med hänsyn tagen till institutets storlek och komplexitetsgrad samt verksamhetens art och omfattning. Ledamöterna bör väljas på ett sådant sätt att ledningsorganet som kollektiv besitter tillräcklig expertis.
3. Ledningsorganet bör söka och välja kvalificerade och erfarna kandidater och se till att det finns en god successionsplanering, med vederbörlig hänsyn till eventuella andra legala krav på sammansättning, utnämningar eller efterträdande.
4. Ledningsorganet bör se till att institutet har policyer för tillsättning och omval av ledamöter. Dessa policyer bör inkludera upprättandet av beskrivningar av den kompetens och de färdigheter som krävs för att säkra att ledningsorganet besitter tillräcklig sakkunskap.
5. Ledamöternas mandatperioder bör ha en lämplig längd. Nomineringar för omval bör basera sig på den ovan angivna profilen och endast göras efter ingående granskningar av hur ledamöterna i fråga har fullgjort sina uppgifter under den innevarande mandatperioden.
6. När ledningsorganet upprättar successionsplaner för ledamöterna bör det beakta när varje ledamots avtal eller mandat upphör, för att om möjligt förhindra att alltför många ledamöter måste ersättas samtidigt.

12. Åtaganden, oberoende och hantering av intressekonflikter i ledningsorganet

1. Ledningsorganets medlemmar bör aktivt delta i institutets verksamhet och kunna göra egna sunda, objektiva och självständiga avgöranden och bedömningar.
2. Tillsättningen av ledamöter bör ske på ett sådant sätt att ledningsorganet kännetecknas av tillräcklig expertis och oberoende. Institutet bör se till att ledningsorganets medlemmar kan lägga ned tillräckligt med tid och arbete för att kunna fullgöra sina skyldigheter.
3. Ledningsorganets medlemmar bör bara ha ett begränsat antal uppdrag eller andra yrkesmässiga åtaganden som kräver mycket tid. Ledamöterna bör också informera institutet om yrkesmässiga bisysslor (till exempel uppdrag för andra företag). Ordföranden har större ansvar och fler uppgifter, och därför bör han eller hon förväntas lägga ned mer tid än övriga.
4. Den tid som alla ledningsorganets medlemmar minst förväntas lägga ned bör anges i ett skriftligt dokument. När ledningsorganets medlemmar ska utse en ny ledamot eller får information om att en befintlig ledamot har fått ett nytt uppdrag bör de kritiskt granska om denna person förväntas kunna lägga ned tillräckligt med tid på att fullgöra sina skyldigheter gentemot institutet. Närvarostatistiken för medlemmarna av ledningsorganets övervakande funktion bör vara offentlig. Institutet bör också överväga att offentliggöra långvarig frånvaro för medlemmar av ledningsorganets ledningsfunktion.
5. Ledningsorganets medlemmar bör kunna agera objektivt, kritiskt och självständigt. För att förbättra förmågan att göra objektiva och självständiga bedömningar bör man bland annat se till att ha ett tillräckligt stort urval av kandidater att rekrytera ledamöter från och ha ett tillräckligt stort antal ledamöter utan verkställande funktioner.

Förklarande not:
Ledningsorganets övervakande funktion är formellt separerad från dess ledningsfunktion, men det är ändå viktigt att se till att den övervakande funktionen kännetecknas av objektivitet och oberoende genom att tillsätta självständiga ledamöter.

6. Ledningsorganet bör ha en skriftlig policy för hantering av ledamöters intressekonflikter. Denna policy bör ange

    a. att ledamöterna är skyldiga redovisa intressekonflikter till ledningsorganet för godkännande och att i övrigt se till att intressekonflikter hanteras på lämpligt sätt,

    b. ett gransknings- eller godkännandeförfarande som ledamöterna ska följa innan de tar på sig vissa uppdrag (till exempel i andra

ledningsorgan), för att se till att sådana nya åtaganden inte skapar intressekonflikter,

c. att ledamöterna är skyldiga att informera institutet om allt som kan resultera eller har resulterat i en intressekonflikt,

d. att ledamöterna är skyldiga att avstå ifrån att delta i beslutsfattande eller omröstningar om ärenden där intressekonflikter kan föreligga eller om deras objektivitet eller förmåga att fullgöra sina skyldigheter gentemot institutet på annat sätt kan ifrågasättas,

e. lämpliga rutiner för transaktioner med närstående parter på affärsmässiga grunder och

f. hur ledningsorganet hanterar bristande efterlevnad av policyn.

13. Ledamöternas kvalifikationer

1. Ledningsorganets medlemmar bör ha de kvalifikationer som krävs för deras befattningar, och bland annat genom fortbildning se till att upprätthålla sin kompetens. De bör ha en tydlig bild av institutets styrelseformer och sin egen roll.
2. De enskilda ledamöterna och ledningsorganet som kollektiv bör besitta den expertkunskap, de erfarenheter, den kompetens, den förståelse och de personliga kvaliteter, däribland professionalitet och personlig integritet, som krävs för att fullgöra uppgifterna.
3. Ledningsorganets medlemmar bör ha aktuella kunskaper om institutets verksamhet på en nivå som motsvarar deras skyldigheter. Detta innefattar en tillräcklig insyn i de områden som de inte har något direkt ansvar för som individer, bara som medlemmar av kollektivet.
4. Som kollektiv bör de ha fullständiga kunskaper om verksamhetens art och därmed förknippade risker samt tillräcklig sakkunskap och erfarenhet som är relevant för alla institutets väsentliga verksamhetsområden, för att styrningen och övervakningen ska bli ändamålsenlig.
5. Institutet bör ha sunda processer som säkrar att ledningsorganets medlemmar har tillräckliga kvalifikationer, både som individer och kollektiv.
6. Ledningsorganets medlemmar bör inhämta, upprätthålla och fördjupa de kunskaper och färdigheter som erfordras för deras uppgifter. Instituten bör se till att ledamöterna har tillgång till individuellt utformade utbildningsprogram som tar hänsyn till eventuella luckor i institutets kunskapsprofil som behöver fyllas och ledamöternas befintliga kunskaper. Några exempel på områden är institutets verktyg och modeller för riskhantering, ny utveckling, organisatoriska förändringar, komplicerade produkter, nya produkter eller marknader samt fusioner. Utbildningen bör också omfatta affärsområden som de enskilda ledamöterna inte har något direkt ansvar för. Ledningsorganet bör avsätta tillräckligt med tid, budgetresurser och andra resurser för utbildning.

14. Ledningsorganets arbetssätt

1. Ledningsorganet bör fastställa lämpliga metoder och rutiner för den interna styrningen av sin egen organisation och sitt eget funktionssätt samt ha verktyg för att se till att dessa följs och med jämna mellanrum ses över och förbättras.

Förklarande not: Sunda metoder och rutiner för ledningsorganets interna styrning sänder ut viktiga signaler internt och externt om institutets policy och mål med styrningen. Dessa metoder och rutiner kan till exempel gälla hur ofta sammanträden hålls, hur de genomförs och hur protokollen ska vara utformade, ordförandens roll och kommittéernas funktion.

2. Ledningsorganet bör sammanträda regelbundet för att kunna fullgöra sina skyldigheter på ett korrekt och effektivt sätt. Ledamöterna bör avsätta tillräckligt med tid för att förbereda sammanträdena. I dessa förberedelser ingår att fastställa dagordningarna. Protokollen bör tydligt utvisa vilka beslut som har fattats och vilka åtgärder som har vidtagits i fråga om de ärenden som har behandlats. Ledningsorganet bör dokumentera och med jämna mellanrum se över dessa metoder och rutiner, och även ledningsorganets rättigheter, skyldigheter och huvudsakliga verksamhetsområden.

Bedömning av ledningsorganets funktionssätt

3. Ledningsorganet bör göra regelbundna bedömningar av hur effektiva och ändamålsenliga dess enskilda och sammantagna verksamheter, metoder och rutiner för den interna styrningen är samt hur väl dess kommittéer fungerar. Externa konsulter kan anlitas för dessa bedömningar.

Ordförandens roll

4. Ordföranden bör se till att ledningsorganets beslut fattas på goda grunder och är väl underbyggda. Han eller hon bör främja en öppen diskussion och en kritisk granskning och se till att olika åsikter kommer fram och diskuteras under beslutsprocessen.

Förklarande not: Ledningsorganets ordförande spelar en viktig roll när det gäller att se till att ledningsorganet fungerar på avsett sätt. Han eller hon leder ledningsorganet och ansvarar för att det fungerar effektivt.

5. I styrningsstrukturer med endast en styrelse bör ledningsorganets ordförande och institutets verkställande direktör inte vara samma person. Om ledningsorganets ordförande också är institutets verkställande direktör bör institutet ha verktyg för att minimera risken för förskjutningar i maktbalansen.

Förklarande not:
Denna maktbalans kan till exempel innebära att en oberoende erfaren ledamot av ledningsorganet ingår i den övervakande funktionen eller liknande.

Ledningsorganets kommittéer

6. Den övervakande funktionen bör, med beaktande av institutets storlek och komplexitetsgrad, överväga att tillsätta specialiserade kommittéer bestående av ledningsorganets medlemmar (andra personer kan bjudas in för att bistå med specifik expertis eller rådgivning i en viss fråga). Exempel på sådana kommittéer kan vara en revisionskommitté, en riskkommitté, en ersättningskommitté, en nominerings- eller personalkommitté och/eller en styrnings-, etik- eller regelefterlevnadskommitté.

Förklarande not:
Att ledningsorganet delegerar uppgifter till sådana kommittéer innebär inte att dess övervakande funktion på något sätt befrias från ansvar för att fullgöra sina skyldigheter, men förfarandet kan stödja ledningsorganet inom vissa specifika områden om det underlättar utvecklingen och införandet av bra styrningsmetoder och beslut.

7. Specialiserade kommittéer bör besitta en optimal blandning av expertis, kompetens och erfarenhet, så att de till fullo kan sätta sig in i de aktuella frågorna, göra objektiva bedömningar och föra in nya tankegångar. De bör bestå av ett tillräckligt antal oberoende ledamöter. Alla kommittéer bör ha dokumenterade mandat (med definierad omfattning) från den övervakande funktionen och fastställda arbetsordningar. Det kan vara lämpligt att emellanåt byta ut ledamöterna och ordföranden.

Förklarande not:
Genom att ledamöterna och ordföranden byts ut motverkar man en olämplig maktkoncentration och främjar nya perspektiv.

8. Kommittéernas ordförande bör regelbundet rapportera till ledningsorganet. De specialiserade kommittéerna bör samverka med varandra för att skapa konsekvens och undvika att luckor uppstår. Detta kan till exempel ske

genom att ordföranden för eller en ledamot av en specialiserad kommitté också är ledamot av en annan kommitté.

Revisionskommitté

9. En revisionskommitté (eller motsvarande) bör bland annat granska hur ändamålsenliga företagets system för intern kontroll, internrevision och riskhantering är, övervaka institutets externa revisorer, göra rekommendationer till ledningsorganet om att anlita och sluta anlita externa revisorer samt ersättningen till dessa, granska och godkänna revisionens omfattning och frekvens, granska revisionsrapporter och kontrollera att ledningsorganets övervakande funktion skyndsamt vidtar nödvändiga korrigerande åtgärder för att komma till rätta med brister i kontrollen, bristande efterlevnad av lagar, förordningar och riktlinjer samt andra problem som revisorerna upptäcker. Dessutom bör revisionskommittén se till att institutet utarbetar en redovisningspolicy.

Förklarande not: Se även artikel 41 i direktiv 2006/43/EG om lagstadgad revision av årsbokslut och sammanställd redovisning.

10. Kommittéernas ordförande bör vara oberoende. Om en person som tidigare har tillhört institutets ledningsfunktion ska utses till ordförande bör en lämplig tid förflyta innan tillsättningen sker.
11. Alla ledamöterna i revisionskommittén bör ha aktuell och relevant praktisk erfarenhet av finansiella marknader eller ha inhämtat tillräcklig yrkeserfarenhet med direkt koppling till finansiella marknader genom sin yrkesbakgrund. Revisionskommitténs ordförande bör ha specialistkunskaper om och erfarenhet av tillämpning av redovisningsprinciper och internkontrollprocesser.

Riskkommittén

12. En riskkommitté (eller motsvarande) bör ansvara för att ge ledningsorganet råd om institutets övergripande aktuella och framtida risktolerans/riskaptit och strategi samt för att övervaka hur denna strategi tillämpas. För att riskkommitténs arbete ska bli mer effektivt bör kommittén regelbundet kommunicera med institutets funktion för riskkontroll och dess riskchef, och när så är lämpligt ha tillgång till externa experter, i synnerhet när det gäller föreslagna strategiska transaktioner såsom fusioner och förvärv.

B.3 Ramverk för uppförande

15. Företags värderingar och uppförandekod

1. Ledningsorganet bör utarbeta och främja höga standarder för etiskt och professionellt uppträdande.

> Förklarande not:
>
> Om ett instituts rykte ifrågasätts kan detta få återverkningar på hela marknaden, och det kan vara svårt att bygga upp det förlorade förtroendet igen.
>
> Genom att införa lämpliga standarder (till exempel en uppförandekod) för professionellt och ansvarsfullt uppträdande i hela institutet kan man mildra de risker det är exponerat för. Om dessa standarder ges hög prioritet och tillämpas på ett sunt sätt minskar i synnerhet den operativa risken och ryktesrisken.

2. Ledningsorganet bör ha en tydlig policy för hur dessa standarder ska upprätthållas.
3. Hur standarderna tillämpas och efterlevs bör vara föremål för en fortlöpande översyn. Resultaten bör regelbundet rapporteras till ledningsorganet.

16. Intressekonflikter på institutsnivå

1. Ledningsorganet bör fastställa, införa och upprätthålla ändamålsenliga riktlinjer för att urskilja faktiska och potentiella intressekonflikter. Intressekonflikter som har rapporterats till och godkänts av ledningsorganet bör hanteras på lämpligt sätt.
2. De förbindelser, tjänster, aktiviteter och transaktioner som kan ge upphov till intressekonflikter inom ett institut bör beskrivas i en skriftlig policy. Av denna ska också framgå hur konflikterna bör hanteras. Denna policy bör omfatta förbindelser och transaktioner mellan institutets olika kunder samt mellan institutet och
   a. dess kunder (till följd av den affärsmodell och/eller de olika tjänster och verksamheter som institutet tillhandahåller),
   b. dess aktieägare,
   c. ledningsorganets medlemmar,
   d. personalen,
   e. viktiga leverantörer och affärspartner samt
   f. andra närstående parter (till exempel dess moderbolag eller dotterbolag).

3. Moderbolag bör beakta alla sina dotterbolags intressen och skapa balans mellan dem samt ta hänsyn till hur dessa intressen bidrar till det gemensamma målet och koncernens övergripande intressen på lång sikt.
4. Policyn om intressekonflikter bör innehålla åtgärder som ska vidtas för att förhindra och hantera intressekonflikter. Några exempel på sådana åtgärder:

   a. Åtskillnad mellan ansvarsområden, till exempel genom att anförtro verksamheter inom transaktionskedjan eller i fråga om tjänster som kan innebära en intressekonflikt till olika personer eller genom att anförtro övervakningen och rapporteringen om sådana verksamheter till olika personer.

   b. Skapa informationsbarriärer genom att till exempel separera vissa avdelningar fysiskt.

   c. Förhindra människor som också har sysslor utanför institutet att utöva ett otillbörligt inflytande på dessa områden inom institutet.

17. Interna rutiner för uppgiftslämning

1. Ledningsorganet bör införa lämpliga interna rutiner som gör att personalen kan slå larm om interna missförhållanden.
2. Institutet bör införa lämpliga interna rutiner som gör att personalen kan påtala missförhållanden i den interna styrningen som de upplever som väsentliga och känner en legitim oro för. Dessa rutiner bör vara sådana att den som påtalar sådana missförhållanden kan göra det konfidentiellt. För att undvika intressekonflikter bör det finnas möjlighet att ta upp sådana missförhållanden vid sidan av de vanliga rapporteringsvägarna (till exempel genom regelefterlevnadsfunktionen, internrevisionen eller ett internt uppgiftslämnarsystem). Rutinen för uppgiftslämning bör kunna användas av all personal vid institutet. De uppgifter som personalen lämnar med hjälp av rutinen för uppgiftslämning bör när så är lämpligt göras tillgängliga för ledningsorganet.

Förklarande not: I vissa medlemsstater kan det vid sidan om en intern rutin för uppgiftslämning inom ett institut också finnas möjlighet för personalen att informera tillsynsmyndigheten om problem av detta slag.

B.4 Policyer om uppdragsavtal och ersättningar

18. Uppdragsavtal

1. Ledningsorganet bör anta en policy om uppdragsavtal för institutet och regelbundet se över denna.

Förklarande not:

Dessa riktlinjer avser endast policyn om uppdragsavtal. Specifika frågor som har med uppdragsavtal att göra diskuteras i CEBS riktlinjer om uppdragsavtal, som finns att tillgå på EBA:s webbplats.

Instituten förväntas följa båda dessa riktlinjer. I händelse av skillnader bör CEBS riktlinjer om uppdragsavtal gälla, eftersom de är mer detaljerade. Om en fråga inte omfattas av CEBS riktlinjer bör den allmänna princip som kommer till uttryck i dessa riktlinjer gälla.

2. Policyn om uppdragsavtal bör beakta hur uppdragsavtal påverkar institutets verksamhet och de risker det exponeras för (såsom operativa risker, ryktesrisker och koncentrationsrisker). Policyn bör inkludera de rapporterings- och övervakningsprocesser som ska tillämpas i alla steg vid uppdragsavtal (såsom att sammanställa projektbeskrivningar som motiverar ett uppdragsavtal, ingå avtal, fullfölja avtalet under hela avtalstiden och upprätta beredskapsplaner och utträdesstrategier). Policyn bör regelbundet ses över och uppdateras och ändringar bör genomföras i god tid.
3. Institutet har det fulla ansvaret för alla tjänster och all verksamhet som läggs ut som uppdragsavtal samt de ledningsbeslut de ger upphov till. Följaktligen bör policyn för uppdragsavtal göra det klart att uppdragsavtalet inte innebär att institutet befrias från sina skyldigheter enligt lag eller sitt ansvar gentemot kunderna.
4. Policyn bör ange att uppdragsavtal inte får hindra en ändamålsenlig tillsyn på plats eller utanför institutet och att den inte får strida mot några begränsningar av tjänster eller verksamhet som följer av tillsynsreglerna. Policyn bör också omfatta interna uppdragsavtal (till exempel av en separat juridisk person i koncernen) och andra specifika omständigheter för koncernen som bör beaktas.

19. Styrning av ersättningspolicyn

1. Institutets ledningsorgan bör ha det yttersta ansvaret för ersättningspolicyn.

Förklarande not:

Dessa riktlinjer ger ett *allmänt* ramverk som är tillämpligt på den interna styrningen av ersättningspolicyn. *Specifika* aspekter på ersättningsfrågor behandlas i CEBS riktlinjer om ersättning från december 2010. Instituten förväntas följa båda dessa riktlinjer.

2. Den övervakande funktionen bör upprätthålla, godkänna och övervaka principerna bakom institutets övergripande ersättningspolicy. Institutets

rutiner för fastställande av ersättningar bör vara tydliga, väl dokumenterade och internt transparenta.

3. Vid sidan av ledningsorganets generella ansvar för den övergripande ersättningspolicyn och översynen av den krävs aktiv medverkan från kontrollfunktionernas sida. Ledningsorganets och ersättningskommitténs medlemmar samt annan personal som är delaktig i ersättningspolicyns utformning och tillämpning bör ha relevant sakkunskap och självständigt kunna bedöma ersättningspolicyns lämplighet, inbegripet dess påverkan på riskhanteringen.
4. Ersättningspolicyn bör också syfta till att förebygga intressekonflikter. Den övervakande funktionen bör inte fastställa sin egen ersättning. För att undvika en sådan situation kan ledningsorganet till exempel tillsätta en oberoende ersättningskommitté. En affärsenhet bör inte få fastställa ersättningen till sina kontrollfunktioner.
5. Ledningsorganet bör upprätthålla en tillsyn över hur ersättningspolicyn tillämpas för att se till att den fungerar på avsett sätt. Tillämpningen av ersättningspolicyn bör också vara föremål för oberoende granskning på central nivå.

C. Riskhantering

20. Riskkultur

1. Institutet bör utforma en integrerad riskkultur som omfattar hela institutet och som bygger på full kunskap om de risker det exponeras för och hur de hanteras, med hänsyn tagen till risktoleransen/riskaptiten.

Förklarande not: Eftersom en stor del av institutets verksamhet är förknippad med risker är det mycket viktigt att riskerna hanteras på lämpligt sätt. En sund och konsekvent riskkultur inom hela institutet är en central del av en effektiv riskhantering.

2. Institutet bör utveckla sin riskkultur med hjälp av policyer, exempel, kommunikation och utbildning av medarbetarna om deras ansvar för hantering av risker.
3. Alla medarbetare bör vara fullt medvetna om vilket ansvar de har för riskhanteringen. Riskhanteringen bör inte överlåtas enbart till riskspecialister eller kontrollfunktioner. Affärsenheterna bör ha det primära ansvaret för den dagliga riskhanteringen, under övervakning av ledningsorganet, med hänsyn tagen till institutets risktolerans/riskaptit och i linje med dess policyer, rutiner och kontroller.
4. Institutet bör ha ett heltäckande ramverk för riskhanteringen som omfattar alla affärs-, stöd- och kontrollenheter och alla relevanta risker (till exempel finansiella och icke-finansiella, i och utanför balansräkningen, och oavsett

om de är potentiella eller följer av avtal) och till fullo återspeglar den ekonomiska innebörden av dess riskexponering. Detta ramverk bör inte bara omfatta risker som är förknippade med kredit-, marknads- och likviditetsrisker och operativa risker, utan också inkludera koncentrationsrisker, ryktesrisker, regelefterlevnadsrisker och strategiska risker.

5. Ramverket för riskhantering bör göra det möjligt för institutet att fatta underbyggda beslut. Dessa bör basera sig på information som härleds från identifiering, mätning eller bedömning och övervakning av risker. Riskerna bör bedömas nedifrån och upp och uppifrån och ned, i hela ledningskedjan och för alla verksamhetsområden, med användning av en konsekvent terminologi och enhetliga metoder i hela institutet och koncernen.
6. Ramverket för riskhantering bör vara föremål för oberoende intern eller extern granskning och regelbundet bedömas i förhållande till institutets risktolerans/riskaptit, med hänsyn tagen till information från funktionen för riskkontroll och, när så erfordras, riskkommittén. Exempel på faktorer som bör beaktas är den interna och externa utvecklingen, däribland ökad balansomslutning och ökade intäkter, ökad komplexitetsgrad för institutets verksamhet, riskprofil och verksamhetsstruktur, geografisk expansion, fusioner och förvärv samt införandet av nya produkter eller verksamhetsområden.

21. Överensstämmelse mellan ersättningspolicyn och riskprofilen

1. Institutets policy och metoder i fråga om ersättningar bör överensstämma med dess riskprofil och främja en sund och ändamålsenlig riskhantering.

Förklarande not:
Dessa riktlinjer ger ett *allmänt* ramverk som är tillämpligt på anpassningen av ersättningspolicyn till institutets riskprofil. *Specifika* aspekter på ersättningsfrågor behandlas i CEBS riktlinjer om ersättning från december 2010. Instituten förväntas följa båda dessa riktlinjer.

2. Institutets övergripande ersättningspolicy bör överensstämma med dess värderingar, affärsstrategi, risktolerans/riskaptit och långsiktiga intressen. Den bör inte uppmuntra till ett överdrivet risktagande. Garanterad rörlig ersättning eller avgångsvederlag som får till följd att misslyckanden belönas är inte förenliga med en sund riskhantering eller principen om resultatlön och bör som regel vara förbjudna.
3. När det gäller personalkategorier som i tjänsten utövar ett väsentligt inflytande på institutets riskprofil (till exempel ledningsorganets medlemmar, högre chefer, risktagare i affärsenheter, personal med ansvar för intern kontroll och medarbetare som får en sammantagen ersättning som innebär att de hamnar på samma ersättningsnivå som företagsledningen och risktagarna) bör ersättningspolicyn innehålla

särskilda bestämmelser för att se till att deras ersättning är förenlig med en sund och ändamålsenlig riskhantering.

4. Personal inom kontrollfunktioner bör ha ersättning som är relaterad till deras mål och resultat, inte resultaten för de affärsenheter de kontrollerar.
5. Om lönerna är resultatrelaterade bör ersättningen basera sig på en kombination av individuella och kollektiva resultat. Vid bedömningen av individuella prestationer bör andra faktorer än ekonomiska resultat beaktas. Resultatmått som används för bonustilldelning bör justeras för alla slags risker, kapitalkostnad och likviditet.
6. Grundlönen bör stå i proportion till bonusen. En betydande bonus bör inte bara utbetalas direkt i kontanter, utan innehålla en flexibel och uppskjuten riskjusterad komponent. Bonusutbetalningen bör ta hänsyn till hur den underliggande risken utvecklas.

22. Ramverk för riskhanteringen

1. Institutets ramverk för riskhantering bör innehålla policyer, rutiner, risklimiter och kontroller som gör att man korrekt, i rätt tid och kontinuerligt kan identifiera, mäta eller bedöma, övervaka, mildra och rapportera de risker som verksamheten inom affärsområdet och i hela institutet medför.
2. Institutets ramverk för riskhantering bör ge särskild vägledning för tillämpningen av dess strategier. Det bör när så är lämpligt fastställa och upprätthålla interna risklimiter som överensstämmer med dess risktolerans/riskaptit och är förenliga med en god förvaltning, finansiell styrka och institutets strategiska mål. Institutets riskprofil (det vill säga summan av dess faktiska och potentiella riskexponeringar) bör hållas inom dessa risklimiter. Ramverket för riskhantering bör säkra att överträdelser av dessa risklimiter rapporteras och följs upp på lämpligt sätt.
3. När institutet identifierar och mäter risker bör det utveckla framåtsyftande och bakåtblickande verktyg som komplement till arbetet med de aktuella exponeringarna. Dessa verktyg bör göra det möjligt att aggregera riskexponeringen för olika verksamhetsområden och stödja identifieringen av riskkoncentrationer.
4. Framåtsyftande verktyg (såsom analyser av scenarier och stresstest) bör identifiera potentiella riskexponeringar under olika negativa omständigheter. Bakåtblickande verktyg bör bidra till en översyn av den faktiska riskprofilen i förhållande till institutets risktolerans/riskaptit och dess ramverk för riskhantering samt ge underlag för eventuella justeringar.

Förklarande not: Riktlinjer för stresstest finns på EBA:s webbplats.

5. Det är institutet som har det yttersta ansvaret för riskbedömningen. Således bör det göra en kritisk granskning av sina risker och inte enbart förlita sig på externa bedömningar.

Förklarande not:
Institutet bör till exempel utvärdera en färdigköpt riskmodell och anpassa den till sina egna omständigheter för att se till att riskerna fångas upp och analyseras på ett korrekt och heltäckande sätt. Externa riskbedömningar (till exempel externa kreditbetyg och riskmodeller som köps av externa aktörer) kan bidra till en mer heltäckande uppskattning av riskerna. Instituten bör vara medvetna om syftet med sådana bedömningar.

6. Vilken risknivå som ska tillämpas bör inte endast avgöras på basis av kvantitativ information eller modellresultat, utan också med hänsyn tagen till de praktiska och konceptuella begränsningar som olika mått och modeller har, genom en kvalitativ analys (med expertutlåtanden och kritisk analys). Relevanta makroekonomiska trender och data bör uppmärksammas särskilt, så att deras potentiella påverkan på exponeringar och portföljer kan fastställas. Sådana bedömningar bör formellt integreras med viktiga riskbeslut.

Förklarande not:
Institutet bör tänka på att resultaten av framåtblickande kvantitativa bedömningar och stresstest till stor del beror på modellernas begränsningar och de antaganden som görs (till exempel om den extrema situationens allvar och varaktighet och de underliggande riskerna). Att en modell visar en mycket hög avkastning på ekonomiskt kapital kan till exempel bero på att modellen har en svaghet (till exempel att vissa relevanta risker inte tas med i beräkningen), och inte på att institutet har en bättre strategi eller genomför den bättre.

7. Mekanismer för regelbunden och öppen rapportering bör finnas, så att ledningsorganet och alla relevanta enheter inom ett institut får korrekta, koncisa, begripliga och meningsfulla rapporter i rätt tid och kan utbyta relevant information om identifiering, mätning eller bedömning och övervakning av risker. Rapporteringsramverket bör vara väl definierat, dokumenterat och godkänt av ledningsorganet.
8. Om en riskkommitté finns bör den regelbundet erhålla formella rapporter och informell information från funktionen för riskkontroll och riskchefen.

Förklarande not:

En effektiv spridning av riskinformation är avgörande för hela riskhanteringen, underlättar granskningen och beslutsfattandet och bidrar till att förhindra beslut som omedvetet kan öka riskerna. En effektiv riskrapportering inbegriper en sund behandling och intern kommunikation av riskstrategin och relevanta riskdata (till exempel exponeringar och viktiga riskindikatorer) både horisontellt inom institutet och i ledningskedjan.

23. Nya produkter

1. Institutet bör ha en väl dokumenterad policy för godkännande av nya produkter. Denna ska vara godkänd av ledningsorganet och behandla frågor som har med utvecklingen av nya marknader, produkter och tjänster samt betydande förändringar av befintliga sådana att göra.
2. Institutets policy för godkännande av nya produkter bör omfatta allt man bör ta med i beräkningen innan man beslutar sig för att gå in på nya marknader, hantera nya produkter, lansera nya tjänster eller göra betydande förändringar av befintliga produkter eller tjänster. Policyn för godkännande av nya produkter bör också slå fast den definition av ”ny produkt/marknad/verksamhet” som ska användas i organisationen, och vilka interna funktioner som ska vara delaktiga i beslutsprocessen.
3. Policyn för godkännande av nya produkter bör ange de viktigaste frågorna som ska beaktas innan ett beslut fattas. Exempel på sådana frågor är regelefterlevnad, prissättningsmodeller, påverkan på riskprofilen, kapitalkrav och lönsamhet samt tillgång på tillräckliga front-, back- och middle office-resurser samt interna verktyg och expertis som gör att man kan förstå och övervaka riskerna. Vilken affärsenhet och vilka personer som ansvarar för att lansera en ny verksamhet bör klart framgå av lanseringsbeslutet. Ingen ny verksamhet bör införas förrän det finns resurser att förstå och hantera de risker den medför.
4. Funktionen för riskkontroll bör medverka till att godkänna nya produkter eller betydande förändringar av befintliga produkter. Den bör bland annat göra en fullständig och objektiv bedömning av riskerna med ny verksamhet i en mängd olika scenarier, av potentiella brister i institutets riskhantering och interna kontroll och av institutets förmåga att hantera nya risker på ett effektivt sätt. Funktionen för riskkontroll bör också ha en god bild av införandet av nya produkter (eller betydande förändringar av befintliga produkter) på olika verksamhetsområden och i olika portföljer, och befogenhet att kräva att förändringar av befintliga produkter genomförs enligt den formella policyn för godkännande av nya produkter.

D. Internkontroll

24. Ramverk för internkontroll

1. Institutet bör utarbeta och upprätthålla ett starkt och heltäckande ramverk för internkontroll med särskilda oberoende kontrollfunktioner som har den ställning som krävs för att fullgöra uppdraget.
2. Institutets ramverk för internkontroll bör säkerställa att dess verksamhet är effektiv och ändamålsenlig, att riskkontrollen fungerar, att verksamheten bedrivs på ett ansvarsfullt sätt, att den finansiella och icke-finansiella information som rapporteras internt och externt är tillförlitlig samt att lagar, bestämmelser, tillsynskrav och institutets interna regler och beslut efterlevs. Ramverket för internkontroll bör omfatta hela organisationen, inklusive alla affärs-, stöd- och kontrollenheters verksamhet. Ramverket för internkontroll bör vara anpassat till institutets verksamhet och innehålla sunda administrativa rutiner och redovisningsrutiner.
3. När institutet utvecklar sitt ramverk för internkontroll bör det se till att beslutsprocessen är tydlig, transparent och dokumenterad och att fördelningen av ansvar och befogenheter är tydlig, så att interna regler och beslut efterlevs. Affärs- och stödenheterna bör ha det främsta ansvaret för att fastställa och upprätthålla lämpliga policyer och rutiner för den interna kontrollen, så att ett starkt ramverk för internkontrollen skapas på alla institutets verksamhetsområden.
4. Det är också viktigt att oberoende kontrollfunktioner kontrollerar att dessa policyer och rutiner följs. Kontrollfunktionerna bör bestå av en riskkontrollfunktion, en regelefterlevnadsfunktion och en internrevisionsfunktion.
5. Kontrollfunktionerna bör återfinnas på en lämplig hierarkisk nivå och rapportera direkt till ledningsorganet. De bör vara oberoende av de affärs- och stödenheter de övervakar och kontrollerar samt organisatoriskt oberoende av varandra (eftersom de har olika uppgifter). I institut som är mindre till storleken eller mindre komplicerade kan dock riskkontrollfunktionen och regelefterlevnadsfunktionen slås samman. Koncernens kontrollfunktioner bör granska dotterbolagens kontrollfunktioner.
6. För att kontrollfunktionen ska betraktas som oberoende bör följande villkor vara uppfyllda:

    a. Dess personal ska inte utföra några uppgifter som rör den verksamhet som kontrollfunktionen ska övervaka och kontrollera.

    b. Kontrollfunktionen ska organisatoriskt vara åtskild från den verksamhet den ska övervaka och kontrollera.

    c. Kontrollfunktionens chef ska rapportera till en person som inte har något ansvar för den verksamhet som kontrollfunktionen ska övervaka och kontrollera. Kontrollfunktionens chef bör i allmänhet rapportera direkt till ledningsorganet och eventuella relevanta kommittéer, och bör regelbundet delta i deras möten.

d. Ersättningen till kontrollfunktionens personal bör inte vara relaterad till den verksamhet som kontrollfunktionen ska övervaka och kontrollera och inte heller på annat sätt kunna antas äventyra dess objektivitet.

7. Kontrollfunktionen bör ha ett lämpligt antal kvalificerade medarbetare (både på moderbolagsnivå och på dotterbolagsnivå i koncerner). Personalen bör erhålla lämplig utbildning och löpande fortbildning. Den bör ha tillgång till lämpliga datasystem och stödtjänster samt den interna och externa information som krävs för att utföra arbetsuppgifterna.
8. Kontrollfunktionerna bör regelbundet överlämna formella rapporter om väsentliga brister som har upptäckts till ledningsorganet. Dessa rapporter bör innehålla uppföljningar av tidigare rapporterade brister och en redovisning av risker förknippade med nyupptäckta väsentliga brister, konsekvensbedömningar och rekommendationer. Ledningsorganet bör agera skyndsamt och effektivt, och kräva att lämpliga korrigerande åtgärder vidtas med anledning av kontrollfunktionernas rapporter.

25. Riskkontrollfunktionen

1. Institutet bör inrätta en heltäckande och oberoende funktion för riskkontroll.
2. Riskkontrollfunktionen bör se till att alla väsentliga risker som institutet exponeras för identifieras och hanteras på lämpligt sätt av institutets berörda enheter samt att heltäckande beskrivningar av alla relevanta risker tillställs ledningsorganet. Riskkontrollfunktionen bör tillhandahålla relevant och oberoende information, analyser och expertutlåtanden om riskexponeringar, samt i samband med att ledningsorganet och affärs- och stödenheterna lägger fram förslag och fattar riskbeslut uttala sig om huruvida dessa är förenliga med institutets risktolerans/riskaptit. Riskkontrollfunktionen kan rekommendera förbättringar av ramverket för riskhantering och olika sätt att komma till rätta med överträdelser av riskpolicyer, rutiner och risklimiter.
3. Riskkontrollfunktionen bör vara en central del av institutets organisation och strukturerad så att den kan genomföra riskpolicyer och kontrollera ramverket för riskhantering. Stora, komplicerade och sofistikerade institut kan överväga att inrätta särskilda funktioner för riskkontroll för alla större affärsområden. Det bör dock finnas en central riskkontrollfunktion inom institutet (och när så är lämpligt en riskkontrollfunktion hos moderbolag i koncerner), så att man får en heltäckande bild av alla risker.
4. Riskkontrollfunktionen bör vara oberoende av de affärs- och stödenheter vilkas risker den kontrollerar, men inte isolerad från dem. Den bör ha tillräckliga kunskaper om riskhanteringstekniker och -rutiner för att hantera risker samt om marknader och produkter. De operativa funktionerna och riskkontrollfunktionen bör samverka med målet att hela institutets personal ska ta ansvar för riskhanteringen.

26. Riskkontrollfunktionens roll

1. Riskkontrollfunktionen bör på ett tidigt stadium vara aktivt delaktig i utarbetandet av institutets riskstrategi och alla väsentliga beslut som har med riskhanteringen att göra. Riskkontrollfunktionen bör spela en viktig roll när det gäller att se till att institutet har effektiva riskhanteringsprocesser.

Riskkontrollfunktionens roll i fråga om strategi och beslutsfattande

2. Riskkontrollfunktionen bör förse ledningsorganet med all relevant riskrelaterad information (till exempel genom tekniska analyser av riskexponeringen), så att det kan fastställa institutets risktolerans/riskaptit.
3. Riskkontrollfunktionen bör också bedöma riskstrategin, inklusive de mål som affärsenheterna föreslår, och ge ledningsorganet råd innan beslut fattas. Målen, som inkluderar kreditbetyg och avkastning på eget kapital, bör vara rimliga och konsekventa.
4. Riskkontrollfunktionen bör ta en del av ansvaret för att genomföra institutets riskstrategi och riskpolicy i alla institutets affärsenheter. Affärsenheterna bör tillämpa de relevanta risklimiterna, men riskkontrollfunktionen bör ansvara för att se till att risklimiterna är i linje med institutets övergripande risktolerans/riskaptit och löpande övervaka att institutet inte tar för stora risker.
5. Riskkontrollfunktionen bör vara delaktig i beslutsprocessen för att säkra att riskerna beaktas i tillräcklig omfattning. Ansvaret för de fattade besluten bör dock ligga hos affärs- och stödenheterna, och ytterst hos ledningsorganet.

Riskkontrollfunktionens roll i fråga om transaktioner med närstående parter

6. Riskkontrollfunktionen bör se till att transaktioner med närstående parter granskas och att de risker de medför för institutet identifieras och bedöms tillräckligt.

Riskkontrollfunktionens roll i fråga om den legala strukturens komplexitetsgrad

7. Riskkontrollfunktionen bör sträva efter att identifiera väsentliga risker som härrör från komplexitetsgraden i institutets legala struktur.

Förklarande not:

Sådana risker kan vara brist på insyn i styrningen, operativa risker som orsakas av inbördes beroende och komplicerade finansieringsstrukturer, exponeringar inom koncernen, ej realiserbara säkerheter och motpartsrisker.

Riskkontrollfunktionens roll i fråga om väsentliga förändringar

8. Riskkontrollfunktionen bör bedöma hur identifierade väsentliga risker kan påverka institutets eller koncernens förmåga att hantera sin riskprofil och fördela finansiering och kapital under normala och negativa omständigheter.
9. Riskkontrollfunktionen bör delta i bedömningen av vilka konsekvenser väsentliga förändringar och exceptionella transaktioner får för institutets och koncernens totala risk innan beslut om sådana förändringar och transaktioner fattas.

Förklarande not:

Några exempel på väsentliga förändringar och exceptionella transaktioner är fusioner och förvärv, bildande eller försäljning av dotterbolag och s.k. ”Special Purpose Vehicles” (SPV), nya produkter, förändringar av system, ramverket för riskhantering och rutiner och förändringar av institutets organisation.

Se de gemensamma riktlinjerna från de tre tidigare nivå 3-kommittéerna (de europeiska finanstillsynsorganen CEBS, CESR och CEIOPS) från 2008 om bedömning av förvärv och ökning av innehav inom finanssektorn. Dessa finns att tillgå på EBA:s webbplats. Riskkontrollfunktionen bör på ett tidigt stadium aktivt medverka till att identifiera relevanta risker (inklusive potentiella konsekvenser av bristfällig s.k. ”due diligence” som inte påvisar risker som uppstår efter fusioner) som har med förändringar av koncernens struktur att göra (däribland fusioner och förvärv) och bör redovisa resultaten direkt till ledningsorganet.

Riskkontrollfunktionens roll i fråga om mätningar och bedömningar

10. Riskkontrollfunktionen bör se till att institutets interna mätningar och bedömningar av risker omfattar en lämplig uppsättning scenarier och bygger på tillräckligt konservativa antaganden om beroenden och korrelationer. I detta bör ingå kvalitativa översikter av sambanden mellan hela institutets risker och lönsamhet och dess externa miljö (också med expertutlåtanden).

Riskkontrollfunktionens roll i fråga om övervakningen

11. Riskkontrollfunktionen bör se till att affärsenheterna kan övervaka alla identifierade risker på ett effektivt sätt. Riskkontrollfunktionen bör regelbundet övervaka institutets faktiska riskprofil och granska den i förhållande till institutets strategiska mål och risktolerans/riskaptit så att ledningsorganets ledningsfunktion kan fatta beslut och dess övervakande funktion kan göra kritiska granskningar.
12. Riskkontrollfunktionen bör analysera trender och urskilja nya och framväxande risker som följer av förändrade omständigheter och villkor. Den bör också regelbundet granska de faktiska riskerna i förhållande till

tidigare uppskattningar (göra utfallstest) för att bedöma hur korrekt och ändamålsenlig riskhanteringen är och förbättra den.

13. Koncernens riskkontrollfunktion bör övervaka de risker som dotterbolagen tar. Bristande överensstämmelse med den antagna koncernstrategin bör rapporteras till relevant ledningsorgan.

Riskkontrollfunktionens roll i fråga om icke godkända exponeringar

14. Riskkontrollfunktionen bör vara delaktig i alla förändringar av institutets strategi och dess godkända risktolerans/riskaptit och risklimiter.
15. Riskkontrollfunktionen bör göra självständiga bedömningar av brott mot eller överträdelser av dem (inklusive orsaker och legal och ekonomisk analys av de faktiska kostnaderna för att eliminera, reducera eller säkra exponeringen i förhållande till de potentiella kostnaderna för att behålla den). Riskkontrollfunktionen bör när så är lämpligt informera de berörda affärsenheterna och rekommendera korrigerande åtgärder.

Förklarande not: Några exempel på orsaker till brott mot eller överträdelser av strategier, risktolerans/riskaptit och risklimiter är nya transaktioner, förändrade marknadsförhållanden eller att institutets strategi, policyer eller rutiner har utvecklats utan att limiterna eller risktoleransen/riskaptiten har anpassats till detta.

16. Riskkontrollfunktionen bör spela en viktig roll när det gäller att se till att beslut om dess rekommendationer fattas på lämplig nivå, följs av berörda affärsenheter och rapporteras till ledningsorganet, riskkommittén och affärs- eller stödenheten.
17. Institutet bör vidta lämpliga åtgärder mot bedrägliga handlingar och bristande disciplin inom och utanför institutet (till exempel brott mot interna rutiner eller överträdelser av risklimiter).

Förklarande not: I dessa riktlinjer avses med ”bedrägeri” både interna och externa bedrägerier enligt definitionen i direktiv 2006/48/EG, bilaga X, del 5. Detta innefattar förluster till följd av handlingar som är avsedda att bedra, tillskansa sig egendom eller kringgå bestämmelser, lagstiftning eller företagets policy, med undantag för förluster som orsakats av diskriminering eller som sammanhänger med social eller kulturell mångfald, och som involverar åtminstone en intern part (interna bedrägerier) samt förluster till följd av tredje mans handlingar i syfte att undanhålla, tillskansa sig egendom eller kringgå lagstiftningen (externa bedrägerier).

27. Riskchefen

1. Institutet ska utse en riskchef, som ska ha det fulla ansvaret för riskkontrollfunktionen och för att övervaka institutets ramverk för riskhantering i hela organisationen.
2. Riskchefen (eller motsvarande) bör ansvara för att tillhandahålla heltäckande och begriplig information om risker, så att ledningsorganet förstår institutets övergripande riskprofil. Riskchefen i ett moderbolag har samma ansvar på koncernnivå.
3. Riskchefen bör ha den sakkunskap, operativa erfarenhet, självständighet och pondus som krävs för att ifrågasätta beslut som påverkar institutets exponering för risker. Institutet bör överväga att ge riskchefen vetorätt. Riskchefen och ledningsorganet eller berörda kommittéer bör kunna kommunicera direkt med varandra om viktiga riskrelaterade frågor och utveckling som kan vara oförenlig med institutets risktolerans/riskaptit och strategi.
4. Om institutet vill ge riskchefen vetorätt mot beslut bör dess riskpolicyer innehålla bestämmelser om under vilka omständigheter riskchefen får åberopa detta och avseende vilka beslut (till exempel kredit- eller investeringsbeslut eller fastställande av risklimiter). Policyerna bör innehålla beskrivningar av hur ärenden ska kunna föras upp på högre nivåer i företaget eller överklagas och av hur ledningsorganet informeras.
5. Om ett institut inte är så beskaffat – främst till följd av sin storlek, organisation eller verksamhets art – att det är motiverat att ha en särskild person med detta ansvar kan en annan högre tjänsteman fylla denna funktion, under förutsättning att det inte finns några intressekonflikter.
6. Institutet bör ha dokumenterade processer för hur tillsättningen av riskchefen ska gå till och för hur dennes uppdrag upphävs. Om riskchefen ska ersättas bör ledningsorganets övervakande funktion godkänna detta i förväg. Generellt sett bör av- eller tillsättning av en riskchef offentliggöras och tillsynsmyndigheten informeras om skälen.

28. Regelefterlevnadsfunktionen

1. Institutet bör inrätta en regelefterlevnadsfunktion med uppgift att hantera dess regelefterlevnadsrisk.
2. Institutet bör anta och tillämpa en regelefterlevnadspolicy, som bör spridas till all personal.

Förklarande not:

Regelefterlevnadsrisk (vilken definieras som den aktuella eller potentiella risken för påverkan på intäkter och kapital som uppstår till följd av överträdelser eller bristande efterlevnad av lagar, bestämmelser, avtal, föreskrivna rutiner eller etiska standarder) kan leda till böter, skadestånd och/eller annullering av avtal och kan skada institutets rykte.

3. Institutet bör inrätta en permanent och effektiv regelefterlevnadsfunktion och utse en ansvarig för denna funktion för hela institutet och koncernen (en regelefterlevnadsansvarig eller regelefterlevnadschef). I mindre och inte så komplicerade institut kan denna funktion kombineras med eller bistås av riskkontroll- eller stödfunktioner (till exempel personalavdelningen, den juridiska avdelningen etc.).
4. Regelefterlevnadsfunktionen bör se till att regelefterlevnadspolicyn följs och rapportera till ledningsorganet och i tillämpliga fall riskkontrollfunktionen om institutets hantering av regelefterlevnadsrisker. Regelefterlevnadsfunktionens slutsatser bör beaktas av ledningsorganet och riskkontrollfunktionen i beslutsprocessen.
5. Regelefterlevnadsfunktionen bör ge ledningsorganet råd om lagar, regler, bestämmelser och standarder som institutet måste följa och bedöma vilka konsekvenser förändringar av den legala och tillsynsmässiga miljön kan få på institutets verksamhet.
6. Regelefterlevnadsfunktionen bör också kontrollera att nya produkter och rutiner är anpassade till den aktuella legala miljön och kända kommande förändringar av lagstiftning, bestämmelser och tillsynskrav.

Förklarande not: Särskild försiktighet bör iakttas när institutet utför vissa tjänster eller inrättar strukturer för kunders räkning (till exempel fungerar som agent för bildandet av bolag eller partnerskap, tillhandahåller förvaltningstjänster eller utvecklar komplicerade finansiella transaktioner åt kunderna) som kan ge upphov till särskilda utmaningar för den interna styrningen och tillsynsmässiga problem.

29. Internrevisionsfunktionen

1. Internrevisionsfunktionen bör bedöma om institutets ramverk för internkontroll är effektiv och ändamålsenlig.
2. Internrevisionsfunktionen bör ha obegränsad tillgång till relevanta dokument och information hos alla operativa enheter och kontrollenheter.
3. Internrevisionsfunktionen bör granska om institutets verksamhet och enheter (inklusive riskkontrollfunktionen och regelefterlevnadsfunktionen) är förenliga med dess policyer och rutiner. Därför bör internrevisionsfunktionen inte kombineras med någon annan funktion. Internrevisionsfunktionen bör också granska om befintliga policyer och rutiner är fortsatt lämpliga och förenliga med legala och tillsynsmässiga krav.
4. Internrevisionsfunktionen bör särskilt granska processer som ska säkra att institutets metoder och tekniker, dess antaganden och de informationskällor som används i dess interna modeller (till exempel riskmodeller och redovisningsberäkningar) är tillförlitliga. Den bör också bedöma kvaliteten hos verktyg för identifiering och bedömning av kvalitativa risker och hur de

används. För att stärka internrevisionsfunktionens oberoende bör den emellertid inte direkt medverka till att utforma eller välja modeller eller andra verktyg för riskhantering.

5. Ledningsorganet bör uppmuntra internrevisorerna att följa nationella och internationella branschstandarder. Den interna revisionen bör genomföras i enlighet med en revisionsplan och detaljerade revisionsprogram med en riskbaserad strategi. Revisionsplanen bör godkännas av revisionskommittén och/eller ledningsorganet.

Förklarande not:
Ett exempel på sådan branschstandard är den som fastställs av *Institute of Internal Auditors*.

6. Internrevisionsfunktionen bör rapportera sina resultat direkt till ledningsorganet och/eller dess revisionskommitté (om sådan finns) och framföra förslag till förbättringar av den interna kontrollen. Alla rekommendationer från revisorerna bör bli föremål för formella uppföljningar på respektive ledningsnivå, för att säkra att de beaktas och att resultaten rapporteras.

E. Informationssystem och kontinuitetsplanering

30. Informationssystem och kommunikation

1. Institutet bör ha effektiva och tillförlitliga informations- och kommunikationssystem för all väsentlig verksamhet.

Förklarande not:
Företagsledningens beslutsfattande kan påverkas negativt av otillförlitlig eller vilseledande information från dåligt utformade och kontrollerade system. Därför är ett väsentligt inslag i ett instituts verksamhet att skapa och upprätthålla informations- och kommunikationssystem som omfattar hela dess verksamhet. Informationen tillhandahålls vanligen på både elektronisk och icke-elektronisk väg. Institutet bör särskilt vara medvetet om de krav som ställs på organisationen och internkontrollen när det gäller behandling av information i elektronisk form och vikten av att ha en tillfredsställande verifieringskedja. Detta gäller också om IT-system läggs ut genom uppdragsavtal på IT-tjänsteleverantörer.

2. Informationssystemen, däribland de som innehåller och använder data i elektronisk form, bör vara säkra, stå under oberoende övervakning och

stödjas av lämpliga beredskapsåtgärder. Institutet bör följa allmänt accepterade IT-standarder när IT-system införs.

31. Kontinuitetshantering

1. Ett institut ska etablera en god kontinuitetshantering för att säkerställa institutets förmåga att upprätthålla verksamheten och begränsa förlusterna vid en allvarlig störning i verksamheten.

> Förklarande not:
>
> Institutets verksamhet är beroende av många olika viktiga resurser (till exempel IT-system, kommunikationssystem och byggnader). Syftet med kontinuitetsplaneringen är att mildra operativa, finansiella, legala och andra konsekvenser samt påverkan på institutets rykte av ett haveri eller långvarigt avbrott i tillgången till dessa resurser som stör institutets normala verksamhet. Andra riskhanteringsåtgärder kan vara att minska sannolikheten för sådana händelser eller överföra de ekonomiska konsekvenserna till tredje parter (till exempel genom försäkringar).

2. För att ha en god kontinuitetshantering bör institutet noggrant analysera sin exponering för allvarliga verksamhetsstörningar och göra (kvantitativa och kvalitativa) bedömningar av deras potentiella påverkan med hjälp av interna och/eller externa data och scenarieanalyser. Dessa analyser bör omfatta alla affärs- och stödenheter samt riskkontrollfunktionen och ta hänsyn till deras beroende av varandra. Dessutom bör en särskild oberoende kontinuitetsfunktion, riskkontrollfunktionen eller funktionen för hantering av operativa risker aktivt medverka. Resultaten av analyserna bör ligga till grund för fastställandet av institutets prioriteringar och mål under återställningsskedet.

> Förklarande not:
>
> Se också direktiv 2006/48/EG, bilaga X, del 3, punkt 3, enligt vilken institut som använder en internmätningsmetod för operativa risker måste ha en oberoende riskhanteringsfunktion för operativa risker. Denna funktions uppgifter beskrivs i punkterna 615–620 i riktlinjerna om validering (som publicerades 2006) som finns på EBA:s webbplats.

3. Baserat på ovanstående analyser bör institutet utarbeta

    a. beredskaps- och kontinuitetsplaner som säkerställer att det reagerar på nödsituationer på lämpligt sätt och kan upprätthålla sin viktigaste verksamhet om de vanliga rutinerna störs och

    b. återställningsplaner för viktiga resurser, så att det kan återgå till sina vanliga rutiner inom rimlig tid. Eventuella återstående risker till

följd av verksamhetsstörningar bör vara förenliga med institutets risktolerans/riskaptit.

4. Beredskaps-, kontinuitets- och återställningsplaner bör vara dokumenterade och genomföras omsorgsfullt. Dokumentationen bör finnas tillgänglig hos affärs- och stödenheterna samt hos riskkontrollfunktionen och lagras i system som är fysiskt åtskilda från övriga och lätt tillgängliga i en nödsituation. Lämplig utbildning bör tillhandahållas. Planerna bör testas och uppdateras regelbundet. Problem eller misslyckanden under testerna bör dokumenteras och analyseras och ligga till grund för översyner av planerna.

F. Insyn

32. Delaktighet

1. Strategier och policyer bör kommuniceras till all berörd personal vid institutet.
2. Institutets personal bör förstå och följa policyer och rutiner som har med deras uppgifter och ansvarsområden att göra.
3. Följaktligen bör ledningsorganet informera den berörda personalen och hålla den uppdaterad om institutets strategier och policyer på ett tydligt och konsekvent sätt, åtminstone i den utsträckning som krävs för att de ska kunna utföra sina uppgifter. Detta kan göras med hjälp av skriftliga riktlinjer, manualer eller annat.

33. Insyn i den interna styrningen

1. Ramverket för institutets interna styrning bör vara transparent. Institutet bör presentera sin aktuella ställning och framtidsutsikter i god tid på ett tydligt, balanserat och korrekt sätt.

Förklarande not:

Syftet med insynen i den interna styrningen är att ge alla institutets relevanta intressenter (däribland aktieägare, anställda, kunder och allmänheten) viktig information som de behöver för att kunna bedöma hur väl ledningsorganet styr institutet.

I enlighet med artikel 72 i direktiv 2006/48/EG och artikel 2 i direktiv 2006/49/EG bör moderkreditinstitut inom EU och institut som kontrolleras av ett finansiellt moderholdingföretag inom EU lämna heltäckande och meningsfull information som beskriver dess interna styrning på konsoliderad nivå. Det är god praxis att institut lämnar proportionerliga uppgifter om sin interna styrning på bolagsnivå.

2. Institutet bör åtminstone offentliggöra

a. sina strukturer och policyer för styrningen, inklusive sina mål, sin organisationsstruktur, sina interna styrmedel, ledningsorganets struktur och organisation, inklusive närvaro, samt institutets incitaments- och ersättningssystem,

b. art, omfattning, syfte med och ekonomisk substans hos transaktioner med närstående bolag och parter om dessa har väsentlig påverkan på institutet,

c. hur dess affärs- och riskstrategi fastställs (inklusive ledningsorganets delaktighet) och förutsebara riskfaktorer,

d. vilka kommittéer det har, deras mandat och sammansättning,

e. sitt ramverk för internkontroll och hur dess kontrollfunktioner är organiserade, deras huvudsakliga uppgifter, hur deras resultat övervakas av ledningsorganet och eventuella planerade väsentliga förändringar av dessa funktioner, samt

f. väsentlig information om sina finansiella resultat och rörelseresultat.

3. Informationen om institutets aktuella ställning bör överensstämma med eventuella lagkrav på offentliggörande. Informationen bör vara tydlig, korrekt, relevant och tillgänglig och lämnas i rätt tid.
4. I fall där offentliggörandet av tidskänslig information skulle försenas om en hög grad av korrekthet måste säkras bör institutet göra en bedömning av vad som är en lämplig balans mellan tidsaspekten och korrektheten, med hänsyn tagen till kravet att ge en sann och rättvisande bild av dess situation och tillfredsställande förklaringar till eventuella dröjsmål. Denna förklaring bör inte användas för att försena uppfyllandet av normala rapporteringskrav.

Kapitel III – Slutbestämmelser och genomförande

34. Upphävanden

Genom antagandet och publiceringen av dessa riktlinjer för intern styrning upphävs följande riktlinjer: avsnitt 2.1 i CEBS *Guidelines on the Application of the Supervisory Review Process* (från den 25 januari 2006) med rubriken *”Guidelines on Internal Governance”*, *”High Level Principles for Remuneration Policies”* (från den 20 april 2009) och *”High Level Principles for Risk Management”* (från den 16 februari 2010).

35. Ikraftträdande

De behöriga myndigheterna bör tillämpa riktlinjerna för intern styrning genom att införliva dem i sin tillsynsverksamhet senast den 31 mars 2012. Efter detta datum bör de behöriga myndigheterna se till att instituten följer dem.