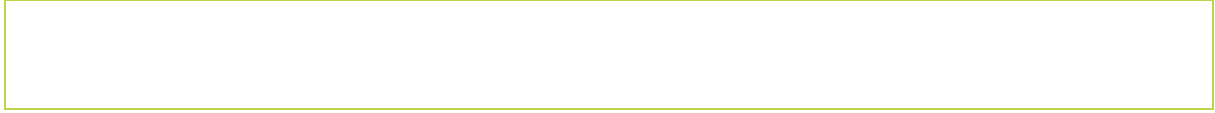


# Riktlinjer

för interna kontroller för referensvärdesadministratörer,  
kreditvärderingsinstitut och infrastrukturer för marknadsinsyn

## Innehållsförteckning

1	Tillämpningsområde .....	4
2	Hänvisningar till lagstiftning, förkortningar och definitioner .....	5
2.1	Hänvisningar till lagstiftning .....	5
2.2	Förkortningar .....	6
2.3	Definitioner .....	6
3	Syfte .....	7
4	Efterlevnads- och rapporteringsskyldigheter .....	7
4.1	Riktlinjernas status .....	7
4.2	Rapporteringskrav .....	8
5	Riktlinjer för interna kontroller .....	9
5.1	Ram för intern kontroll .....	9
	<b>Moment 1.1 Kontrollmiljö .....</b>	<b>9</b>
	<b>Moment 1.2 Riskhantering .....</b>	<b>10</b>
	<b>Moment 1.3 Kontrollverksamhet .....</b>	<b>11</b>
	<b>Moment 1.4 Information och kommunikation .....</b>	<b>13</b>
	<b>Moment 1.5 Övervakningsverksamhet .....</b>	<b>14</b>
5.2	Funktioner för intern kontroll .....	14
	<b>Proportionalitet – funktioner för intern kontroll .....</b>	<b>16</b>
	<b>Moment 2.1 Funktion för regelefterlevnad .....</b>	<b>17</b>
	<b>Moment 2.2 Funktion för riskhantering .....</b>	<b>18</b>
	<b>Moment 2.3 Funktion för ledning av informationssäkerhet (endast för enheter som står under tillsyn och som inte omfattas av DORA-förordningen) .....</b>	<b>18</b>
	<b>Moment 2.4 Funktion för internrevision .....</b>	<b>19</b>
	<b>Moment 2.5 – Funktion för översyn (endast för kreditvärderingsinstitut) .....</b>	<b>20</b>
	<b>Moment 2.6 Övervakningsfunktion (endast för referensvärdesadministratörer) .....</b>	<b>21</b>



# 1 Tillämpningsområde

## Målgrupp

1. Dessa riktlinjer gäller för

(i) referensvärdesadministratörer som är auktoriserade av, registrerade hos eller erkända av Esma i enlighet med referensvärdesförordningen,

(ii) kreditvärderingsinstitut som är etablerade i unionen och registrerade hos Esma i enlighet med förordningen om kreditvärderingsinstitut,

(iii) leverantörer av datarapporteringstjänster (förutom tillhandahållare av konsoliderad handelsinformation [CTP]) som är etablerade i unionen och auktoriserade av Esma i enlighet med förordningen om marknader för finansiella instrument (Mifir),

(iv) värdepapperiseringsregister som är etablerade i unionen och registrerade hos Esma i enlighet med värdepapperiseringsförordningen,

(v) transaktionsregister som är etablerade i unionen och registrerade hos Esma i enlighet med förordningen om Europas marknadsinfrastruktur (Emir),

(vi) transaktionsregister som är etablerade i unionen och registrerade hos Esma i enlighet med förordningen om transparens i transaktioner för värdepappersfinansiering (nedan tillsammans kallade *enheter som står under tillsyn*).

## Omfattning

2. Dessa riktlinjer gäller frågor som rör nödvändiga strukturer och mekanismer avseende intern kontroll för att säkerställa i) en referensvärdesadministratörs faktiska efterlevnad av artiklarna 4–10 i referensvärdesförordningen, ii) ett kreditvärderingsinstituts faktiska efterlevnad av artikel 6.1, 6.2 och 6.4, artikel 9 och avsnitt A i bilaga I till förordningen om kreditvärderingsinstitut, iii) en datarapporteringstjänsteleverantörs faktiska efterlevnad av artikel 27f, 27g och 27i i Mifir samt iv) ett transaktionsregisters eller värdepapperiseringsregisters faktiska efterlevnad av artiklarna 78 och 79 i Emir.

## Ikraftträdande

3. Dessa riktlinjer gäller från och med den 1 oktober 2026.

4. Från och med det datum som avses i punkt 3 upphör riktlinjerna för intern kontroll av kreditvärderingsinstitut (ESMA33-9-371) att gälla.

## 2 Hänvisningar till lagstiftning, förkortningar och definitioner

### 2.1 Hänvisningar till lagstiftning

DORA-förordningen		Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 <sup>1</sup> .
Emir		Europaparlamentets och rådets förordning (EU) nr 648/2012 av den 4 juli 2012 om OTC-derivat, centrala motparter och transaktionsregister <sup>2</sup> .
förordningen om kreditvärderingsinstitut	om	Europaparlamentets och rådets förordning (EG) nr 1060/2009 av den 16 september 2009 om kreditvärderingsinstitut <sup>3</sup> .
förordningen om transparens i transaktioner för värdepappersfinansiering	för	Europaparlamentets och rådets förordning (EU) 2015/2365 av den 25 november 2015 om transparens i transaktioner för värdepappersfinansiering och om återanvändning samt om ändring av förordning (EU) nr 648/2012 <sup>4</sup> .
Mifir		Europaparlamentets och rådets förordning (EU) nr 600/2014 av den 15 maj 2014 om marknader för finansiella instrument och om ändring av förordning (EU) nr 648/2012 <sup>5</sup> .
referensvärdesförordningen		Europaparlamentets och rådets förordning (EU) 2016/1011 av den 8 juni 2016 om index som används som referensvärden för finansiella instrument och finansiella avtal eller för att mäta investeringsfonders resultat, och om ändring av direktiven 2008/48/EG och 2014/17/EU och förordning (EU) nr 596/2014 <sup>6</sup> .
värdepapperiseringsförordningen		Europaparlamentets och rådets förordning (EU) 2017/2402 av den 12 december 2017 om ett allmänt ramverk för värdepapperisering och om inrättande av ett särskilt ramverk för enkel, transparent och standardiserad värdepapperisering samt om ändring av direktiven 2009/65/EG, 2009/138/EG och

<sup>1</sup> EUT L 333, 27.12.2022, s. 1.

<sup>2</sup> EUT L 201, 27.7.2012, s. 1.

<sup>3</sup> EUT L 302, 17.11.2009, s. 1.

<sup>4</sup> EUT L 337, 23.12.2015, s. 1.

<sup>5</sup> EUT L 173, 12.6.2014, s. 84.

<sup>6</sup> EUT L 171, 29.6.2016, s. 1.

2011/61/EU och förordningarna (EG) nr 1060/2009 och (EU) nr 648/2012<sup>7</sup>.

## 2.2 Förkortningar

AI	artificiell intelligens
DORA-förordningen	förordning om digital operativ motståndskraft
Esma	Europeiska värdepappers- och marknadsmyndigheten
EU	Europeiska unionen
IKT	informations- och kommunikationsteknik

## 2.3 Definitioner

enheter som står under tillsyn	<p>I dessa riktlinjer avses med detta de enheter som faller inom Esmas tillsynsområde, nämligen</p> <ul style="list-style-type: none"><li>▪ referensvärdesadministratörer,</li><li>▪ kreditvärderingsinstitut,</li><li>▪ leverantörer av datarapporteringstjänster (förutom tillhandahållare av konsoliderad handelsinformation),</li><li>▪ värdepapperiseringsregister,</li><li>▪ transaktionsregister.</li></ul>
infrastrukturer för marknadsinsyn	<p>I dessa riktlinjer avses med detta</p> <ul style="list-style-type: none"><li>▪ leverantörer av datarapporteringstjänster,</li><li>▪ värdepapperiseringsregister,</li><li>▪ transaktionsregister.</li></ul>
ledningsorgan	<p>Det eller de organ som utses i enlighet med nationell lagstiftning och har behörighet att fastställa enhetens strategi, mål och övergripande inriktning, och som kontrollerar och övervakar ledningens beslutsfattande samt omfattar personer som i praktiken leder enhetens verksamhet.</p> <p>Detta avser de högsta styrande organen inom en organisation.</p>

---

<sup>7</sup> EUT L 347, 28.12.2017, s. 35.

Begreppet definieras i artikel 3.1.20 i referensvärdesförordningen och i artikel 2.1.22 i Mifir.

Det omfattar följande koncept:

- Ett kreditvärderingsinstitut "administrativa styrelse eller tillsynsråd" som utgör en del av "företagsledningen" enligt definitionen i artikel 3.1 n i förordningen om kreditvärderingsinstitut.
- "Administrativ styrelse och/eller tillsynsråd, i enlighet med nationell bolagsrätt", enligt definitionen i artikel 2.27 i Emir.

I dessa riktlinjer avses med detta

relevanta förordningar

- referensvärdesförordningen,
- förordningen om kreditvärderingsinstitut,
- Emir,
- Mifir,
- värdepapperiseringsförordningen,
- förordningen om transparens i transaktioner för värdepappersfinansiering.

verkställande ledning

Detta avser de personer i ledande ställning som på daglig basis leder den enhet som står under tillsyn. Detta är vanligtvis den verkställande direktören eller motsvarande och de personer som rapporterar direkt till den verkställande direktören.

### 3 Syfte

5. I dessa riktlinjer fastställs Esmas förväntningar med avseende på de moment och egenskaper som ingår i en effektiv ram för intern kontroll och de olika interna kontrollernas funktioner inom en enhet som står under tillsyn.

## 4 Efterlevnads- och rapporteringsskyldigheter

### 4.1 Riktlinjernas status

6. Detta dokument innehåller riktlinjer som utfärdats enligt artikel 16 i Esmaförordningen. Enligt artikel 16.3 i Esmaförordningen ska enheter som står under tillsyn med alla tillgängliga medel söka följa dessa riktlinjer.

## 4.2 Rapporteringskrav

7. Finansmarknadsaktörer som omfattas av dessa riktlinjer är inte skyldiga att rapportera om huruvida de följer desamma. Esma kommer att bedöma tillämpningen av dessa riktlinjer genom sin fortlöpande tillsyn och övervakning av den verksamhet som de enheter som står under tillsyn bedriver.
8. Esma kommer att tillämpa proportionalitetsprincipen vid tillämpningen av dessa riktlinjer. Även om alla enheter som står under tillsyn förväntas ha ett effektivt system för intern kontroll som inbegriper de moment och egenskaper som beskrivs i dessa riktlinjer, kommer Esma att anpassa sina förväntningar med avseende på avsnitt 4.2 till den karaktär, omfattning, komplexitet och övergripande riskprofil som en enhet har och baserat på hur dessa egenskaper kan komma att påverka investerarskyddet, marknadens korrekta funktion och den finansiella stabiliteten.
9. Vid bedömningen av karaktären hos en enhet som står under tillsyn kommer Esma att beakta dess affärsområde och den typ av verksamhet som den bedriver, inbegripet dess roll/uppdrag på marknaden samt typ, mångfald och kritikalitet med avseende på de produkter och tjänster som enheten erbjuder.
10. Vid bedömningen av omfattningen på den verksamhet som en enhet som står under tillsyn bedriver kommer Esma att beakta relevanta faktorer, däribland antalet anställda, intäkter, antalet kunder och produkter, marknadsandel, kopplingar till andra branscher/infrastrukturer, anknutna tjänster och deras förhållande till centrala tjänster samt andra faktorer som är specifika för enhetens storlek och dess marknadspåverkan.
11. Vid bedömningen av komplexiteten hos en enhet som står under tillsyn tar Esma hänsyn till faktorer såsom enhetens organisationsstruktur och organisatoriska arrangemang (gruppstruktur/relationer, gemensamma tjänster, utkontraktering osv.) samt dess operativa egenskaper i förhållande till personer, processer, teknik, produktutbud och kopplingar.
12. Genom att anpassa sina förväntningar tar Esma hänsyn till villkoren för registrering eller erkännande av en enhet som står under tillsyn. Karaktären, omfattningen och komplexiteten hos en enhet som står under tillsyn kan förändras efter det att den har registrerats eller erkänts, och det är enhetens ansvar att se till att dess interna kontroller står i proportion till dess karaktär, omfattning och komplexitet. Inom ramen för sin tillsyn kommer Esma att meddela om den har högre förväntningar enligt avsnitt 5.1 och 5.2 än de som fastställdes vid registreringen eller erkännandet.

## 5 Riktlinjer för interna kontroller

13. För att styrka tillämpningen av punkt 2 i dessa riktlinjer bör enheter som står under tillsyn visa att deras policyer, förfaranden och arbetsmetoder uppfyller målen i avsnitten **5.1** ("Ram för intern kontroll") och **5.2** ("Funktioner för intern kontroll") i dessa riktlinjer.

### 5.1 Ram för intern kontroll

14. För att säkerställa en effektiv ram för intern kontroll bör de enheter som står under tillsyn ha policyer, förfaranden och arbetsmetoder som inbegriper följande moment och egenskaper.

#### *Allmänna principer*

15. Ledningsorganet för den enhet som står under tillsyn bör vara ansvarigt för att överse och godkänna samtliga moment inom ramen för intern kontroll samt för att tillse att dessa moment övervakas och regelbundet uppdateras av den verkställande ledningen. Den verkställande ledningen för enheten som står under tillsyn bör ansvara för att fastställa, genomföra och uppdatera de skriftliga policyer, förfaranden och metoder för intern kontroll som stöder de moment som ingår i ramen för intern kontroll.
16. Som en del av inrättandet av dessa policyer och förfaranden bör en enhet som står under tillsyn ha en tydlig, transparent och dokumenterad beslutsprocess och en tydlig fördelning av roller och ansvarsområden inom sin ram för intern kontroll, inbegripet sina affärsområden och funktioner för intern kontroll.

#### **Moment 1.1 Kontrollmiljö**

17. Både ledningsorganet och den verkställande ledningen för en enhet som står under tillsyn bidrar till att på högsta nivå sätta tonen vad gäller vikten av intern kontroll. Den verkställande ledningen ansvarar för utvecklingen och verkställandet av den interna kontrollen och bedömer kontrollmiljöns lämplighet och ändamålsenlighet. Ledningsorganet bör följa upp den verkställande ledningens arbete inom dessa områden.

#### **Egenskaper**

- 1.1.1** Den verkställande ledningen för enheten som står under tillsyn bör ansvara för att etablera en stark kultur av etik och efterlevnad inom enheten medelst genomförande av policyer och förfaranden som styr enhetspersonalens uppförande.
- 1.1.2** Den verkställande ledningen för den enhet som står under tillsyn bör ansvara för att säkerställa följande med avseende på enhetens policyer och förfaranden:

- i. Att det specificeras att den enhet som står under tillsyn bör bedriva sin verksamhet i enlighet med de relevanta förordningarna och enhetens företagsvärderingar.
  - ii. Att det klagörs att personalen utöver att följa rättsliga och regelverksrelaterade krav samt interna policyer även förväntas uppträda med ärlighet och integritet och utföra sina uppgifter med vederbörlig skicklighet, omsorg och aktsamhet.
  - iii. Att det säkerställs att personalen är medveten om de potentiella interna och externa disciplinära åtgärder samt rättsliga åtgärder och sanktioner som kan följa av misskötsamhet.
- 1.1.3** Den verkställande ledningen för den enhet som står under tillsyn bör fastställa, upprätthålla och regelbundet uppdatera lämpliga skriftliga policyer, mekanismer och förfaranden för intern kontroll.
- 1.1.4** Den verkställande ledningen för den enhet som står under tillsyn bör bibehålla ansvaret för sådan verksamhet som utkontrakteras till externa tjänsteleverantörer eller som delegeras till affärspartner.

## **Moment 1.2 Riskhantering**

18. För att åstadkomma en effektiv riskhantering bör enheter som står under tillsyn säkerställa att de har en dynamisk och kontinuerligt föränderlig process för identifiering, bedömning och mätning av alla risker som skulle kunna påverka en enhets förmåga att fullgöra sina skyldigheter enligt de relevanta förordningarna, eller dess fortsatta verksamhet. Detta inbegriper till exempel risker som uppstår till följd av enhetens användning av ny teknik och förändringar av dess yttre risklandskap. Processen bör göra det möjligt för den enhet som står under tillsyn att övervaka, hantera, mildra och korrekt rapportera väsentliga risker för dessa mål.

### **Egenskaper**

- 1.2.1** Den enhet som står under tillsyn bör genomföra sina interna riskbedömningar i enlighet med en fastställd och heltäckande metod för riskbedömning.
- 1.2.2** Den enhet som står under tillsyn bör fastställa sin riskaptit och identifiera risktoleransnivåer.
- 1.2.3** Den metod för riskbedömning som enheten som står under tillsyn använder bör omfatta enhetens alla affärsområden och funktioner för intern kontroll.

- 1.2.4** Riskbedömningsprocessen vid enheten som står under tillsyn bör identifiera och bedöma förändringar som skulle kunna ha en betydande inverkan på systemet för intern kontroll. Detta inbegriper förändringar av dess miljö, organisation, verksamhet och drift.
- 1.2.5** Den metod för riskbedömning som enheten som står under tillsyn använder bör utvecklas och förbättras fortlöpande.

### **Moment 1.3 Kontrollverksamhet**

19. Kontrollverksamheten bör vara förebyggande, avslöjande, korrigerande eller avskräckande till sin karaktär.

#### **Egenskaper**

- 1.3.1** *Åtskillnad mellan ansvarsområden:* Den enhet som står under tillsyn bör säkerställa en lämplig åtskillnad mellan ansvarsområdena för att hantera risken för intressekonflikter, bedrägerier och mänskliga fel. En åtskillnad mellan ansvarsområden bör säkerställa att den anställde som ansvarar för att utföra en viss uppgift inte är ensamt ansvarig för godkännandet av resultatet av uppgiftens utförande. I synnerhet är den anställde som ansvarar för utvecklingen, genomförandet eller godkännandet av en uppgift/ett arbetsmoment inte ensamt ansvarig för att validera, bedöma och se över uppgiften/arbetsmomentet.<sup>8</sup> I den mån detta inte kan undvikas bör situationen mildras genom att den anställde inte är exklusivt ansvarig för aktiviteten.<sup>9</sup>
- 1.3.2** *Dokumentation:* Den enhet som står under tillsyn bör dokumentera sina policyer och förfaranden med avseende på alla de områden av dess affärsverksamhet som omfattas av bestämmelserna i relevanta förordningar.
- 1.3.3** *Dokumenterade kontroller och kontrolltester:* Den enhet som står under tillsyn bör dokumentera de nyckelkontroller som införts för att säkerställa efterlevnad av de policyer och förfaranden som fastställts i enlighet med relevanta förordningar.
- 1.3.4** *Fastställande av ansvarsområden:* Den enhet som står under tillsyn bör på ett tydligt och väl definierat sätt fastställa vilka roller eller funktioner som är ansvariga för att utföra kontroller med avseende på skyldigheterna enligt de

---

<sup>8</sup> De anställda som ansvarar för systemutveckling bör till exempel inte delta i databasadministration, it-drift och it-system samt administration och underhåll av nätverk. För kreditvärderingsinstitut gäller följande: i) personer som utför analysen av en kreditvärdering bör inte ensamt vara ansvariga för godkännandet av kreditvärderingen, ii) personer som ansvarar för utvecklingen av kreditvärderingsmetoder bör inte ensamt vara ansvariga för godkännandet av desamma, iii) personer som ansvarar för validering, bedömning eller översyn av kreditvärderingsmetoden bör inte ensamt vara ansvariga för godkännandet av valideringen, bedömningen eller översynen.

<sup>9</sup> Till exempel genom en kontroll enligt principen om fyra ögon.

relevanta förordningarna och specificera vilka deras respektive roller och ansvarsområden är. Härvid bör den enhet som står under tillsyn skilja mellan dagliga kontroller på verksamhetsnivå och kontroller som utförs av särskilda kontrollfunktioner.

- 1.3.5** *Auktorisationer och godkännanden:* Den enhet som står under tillsyn bör ha auktorisationsprocesser eller auktorisationsmekanismer för säkerställande av att endast behöriga personer har tillgång till information och verktyg enligt principerna för behovsenlig behörighet och begränsad behörighet. Den enhet som står under tillsyn bör också ha processer eller mekanismer inom alla affärsverksamheter för säkerställande av att verksamheterna endast godkänns och utförs av anställda som agerar inom ramen för sin behörighet.<sup>10</sup>
- 1.3.6** *Verifieringar, valideringar, avstämningar och översyner:* Den enhet som står under tillsyn bör vidta åtgärder för att i god tid upptäcka och agera mot olämplig, obehörig, felaktig eller bedräglig verksamhet.<sup>11</sup>
- 1.3.7** *Allmänna kontroller inom IKT (endast för enheter som står under tillsyn och inte omfattas av DORA-förordningen):* Den enhet som står under tillsyn bör genomföra strategier, policyer och förfaranden som säkerställer den digitala operativa motståndskraften hos sina IKT-system för att stödja enhetens affärsprocesser.

Den enhet som står under tillsyn bör utforma sina IKT-kontroller och IKT-lösningar på ett proportionerligt sätt. IKT-kontrollerna kommer därför att variera mellan organisationer beroende på karaktären, omfattningen och komplexiteten hos de underliggande affärsprocesserna och de relevanta funktioner som stöds av dessa system.

Enheter under tillsyn bör säkerställa att de har tillräckliga kontroller för att säkerställa datakvalitet i fråga om tillgänglighet, konfidentialitet och integritet, inklusive datavalidering, kontroller av behandlingar och kontrollförfaranden för datafiler.

Den enhet som står under tillsyn bör upprätta ett relevant system för ledning av informationssäkerhet och tillhörande kontrollverksamhet. Som en del av detta bör en enhet som står under tillsyn fastställa de kontroller som krävs för att

---

<sup>10</sup> För kreditvärderingsinstitut bör till exempel endast de personer som utsetts som ansvariga för respektive uppgift utföra kreditvärderingsprocessen, valideringen av metoderna och översynen av valideringsresultaten.

<sup>11</sup> Detta omfattar kontroller av datavalidering och indata samt översyner av förteckningar för behörig tillgång till konfidentiell information. För kreditvärderingsinstitut gäller sådana kontroller kreditvärderingsverksamheten och de processer som ligger till grund för denna verksamhet, t.ex. validering av kreditmetoder/kreditmodeller.

säkerställa informationens äkthet, konfidentialitet, integritet och tillgänglighet när den behandlas från källa till slutanvändare.

Den enhet som står under tillsyn bör fastställa och dokumentera alla relevanta kontrollåtgärder avseende processer för förvärv, utveckling och underhåll av IKT.

## **Moment 1.4 Information och kommunikation**

20. Enheter som står under tillsyn bör inrätta förfaranden för nedåtriktad kommunikation av korrekta, fullständiga och kvalitativa uppgifter till sin personal och sina externa intressenter. Enheter som står under tillsyn bör också inrätta förfaranden för regelbunden rapportering av information om systemet för intern kontroll och relaterade verksamheter till ledningsorganet och den verkställande ledningen, inbegripet information om beteende och efterlevnad med avseende på interna kontroller.

### **Egenskaper**

- 1.4.1** Den enhet som står under tillsyn bör säkerställa lämplig intern och extern kommunikation och i god tid dela korrekta, fullständiga och kvalitativa uppgifter med marknaden, kunder, användare av enhetens produkter och tjänster och tillsynsmyndigheter.
- 1.4.2** Den enhet som står under tillsyn bör inrätta kanaler för uppåtriktad kommunikation, däribland ett förfarande för visseblåsning, för att möjliggöra en eskalering av väsentliga problem avseende den interna kontrollen till ledningsorganet och den verkställande ledningen. Ledningsorganet och den verkställande ledningen bör också erhålla regelbundna uppdateringar om systemet för intern kontroll och relaterade verksamheter, bland annat vad gäller informationssäkerhet. Den enhet som står under tillsyn bör ha eskaleringsförfaranden i händelse av väsentlig oenighet mellan funktioner för intern kontroll och operativa enheter.
- 1.4.3** Den enhet som står under tillsyn bör inrätta kanaler för nedåtriktad kommunikation från ledningsorganet, den verkställande ledningen och kontrollfunktionerna till personalen. Detta bör omfatta regelbundna uppdateringar av målen och ansvarsområdena inom ramen för intern kontroll, spridning av information om identifierade efterlevnads- eller informationssäkerhetsproblem samt presentationer och utbildning om policyer och förfaranden.

## **Moment 1.5 Övervakningsverksamhet**

21. Enheter som står under tillsyn bör säkerställa att de bedriver övervakningsverksamhet som bidrar till att fastställa om enhetens system för intern kontroll inbegriper de tillbörliga momenten och om de fungerar effektivt.

### **Egenskaper**

- 1.5.1** Den enhet som står under tillsyn bör säkerställa att utvärderingar av systemet för intern kontroll utförs på olika nivåer inom enheten, såsom affärsområden, kontrollfunktioner och funktioner för internrevision eller oberoende bedömning.
- 1.5.2** Övervakningsverksamheten bör utformas och utföras på ett sätt som gör det möjligt för den enhet som står under tillsyn att kontrollera om den uppfyller sina rättsliga och regelverksrelaterade krav, inbegripet efterföljandet av sina interna uppförandekoder, policyer och förfaranden. Detta inbegriper enhetens policyer och förfaranden för informationssäkerhet.
- 1.5.3** Utvärderingarna av systemen för intern kontroll bör utföras på regelbunden eller tematisk basis eller genom en kombination av dessa.
- 1.5.4** De enheter som står under tillsyn bör bygga in fortlöpande utvärderingar i affärsprocesserna och anpassa dem till ändrade förhållanden.
- 1.5.5** De enheter som står under tillsyn bör se till att de brister som identifieras vid de övervakningsrelaterade utvärderingarna och de avhjälpande åtgärder som krävs rapporteras till ledningsorganet och den verkställande ledningen, vilka i sin tur bör följa upp genomförandet av de korrigerande åtgärder och säkerställa att detta sker i tid.
- 1.5.6** Vid utkontraktering bör den enhet som står under tillsyn ge en anställd i uppdrag att följa upp de affärsprocesser som utkontrakterats. De enheter som står under tillsyn bör säkerställa att tillräcklig information vad gäller mål och leveransförväntningar tillhandahålls tjänsteleverantören och att en due diligence-granskning genomförs innan leverantören utses.

## **5.2 Funktioner för intern kontroll**

22. För att säkerställa effektiva funktioner för intern kontroll bör de enheter som står under tillsyn ha policyer, förfaranden och arbetsmetoder som inbegriper följande moment och egenskaper.

*Allmänna principer*

23. Esma anser att funktionerna för intern kontroll vid de enheter som står under tillsyn bör ha tillräckliga resurser och personal med tillräcklig sakkunskap för att kunna fullgöra sina uppgifter. Personal inom funktionerna för intern kontroll bör ha tillräcklig teknisk kunskap om enhetens verksamhet och de därmed förknippade riskerna. Om en enhet har utkontrakterat de operativa uppgifterna för en funktion för intern kontroll på gruppnivå eller till en extern part anser Esma att enheten bibehåller det fulla ansvaret för verksamheten i den utkontrakterade funktionen för intern kontroll. De enheter som står under tillsyn bör se till att den personal som ansvarar för funktionerna för intern kontroll har en tillräckligt hög tjänsteålder för att ha de befogenheter som krävs för att kunna fullgöra sina skyldigheter. Till exempel bör de anställda som ansvarar för funktionerna för regelefterlevnad, riskhantering, internrevision, ledning av informationssäkerhet, översyn (för kreditvärderingsinstitut) och tillsyn (för referensvärdesadministratörer) ha obehindrad tillgång och regelbundet rapportera till ledningsorganet.
24. När det gäller enheter som står under tillsyn får verksamhet bedrivas på gruppnivå eller av andra juridiska personer inom en företagsstruktur, under förutsättning att gruppstrukturen inte utgör ett hinder för ledningsorganets förmåga att sörja för översyn och den verkställande ledningens förmåga att hantera riskerna på ett effektivt sätt, eller Esmas förmåga att utöva tillsyn över enheten på ett effektivt sätt. I samtliga fall gäller riktlinje 1.1.4.
25. För att säkerställa att en enhet som står under tillsyn har oberoende funktioner för intern kontroll förväntar sig Esma att enheterna tar hänsyn till följande principer när de fastställer rollerna och ansvarsområdena för sina funktioner för intern kontroll:
  - i. Funktionerna för intern kontroll bör vara organisatoriskt åtskilda från de funktioner/de verksamheter som de har i uppdrag att övervaka, granska eller kontrollera.
  - ii. Funktionerna för intern kontroll bör inte utföra några operativa uppgifter som faller inom ramen för de affärsverksamheter som de är avsedda att övervaka, granska eller kontrollera.
  - iii. Den anställde som ansvarar för en funktion för intern kontroll bör inte rapportera till en person som har ansvar för att leda de verksamheter som funktionen för intern kontroll övervakar, granskar eller kontrollerar.
26. Personal som fullgör åtaganden relaterade till funktionerna för intern kontroll bör ha tillgång till relevant intern eller extern utbildning för säkerställande av att de har tillräcklig kompetens för att kunna utföra uppgifterna.

## **Proportionalitet – funktioner för intern kontroll**

27. Även om alla enheter som står under tillsyn förväntas uppvisa egenskaper för effektiva funktioner för intern kontroll i enlighet med vad som beskrivs i dessa riktlinjer, anpassar Esma sina förväntningar utifrån enhetens karaktär, omfattning och komplexitet, i enlighet med vad som framgår av avsnitt 3.4 i dessa riktlinjer.
28. I detta avsnitt beskrivs i närmare detalj hur Esma tar hänsyn till proportionalitetsprincipen i sin tillsyn av funktioner för intern kontroll.

## **Åtskillnad mellan ansvarsområden**

29. Åtskillnad mellan ansvarsområden bör integreras i utvecklingen av kontrollverksamheten. Det kan emellertid förekomma fall där unionsrätten inte kräver åtskillnad av ansvarsområden och där en sådan åtskillnad inte är praktiskt genomförbar med tanke på karaktären, omfattningen och komplexiteten hos en enhet som står under tillsyn. I detta fall kan alternativa kontroller vara mer lämpliga. Om andra kontroller används bör de enheter som står under tillsyn dokumentera motiveringen till arrangemanget, identifiera möjliga risker, genomföra kompensande kontroller för att hantera dem och visa att arrangemanget inte har en negativ inverkan på kontrollmiljön.

## **Resurser**

30. För vissa enheter som står under tillsyn kan det vara oproportionerligt att ha heltidsbemanning inom alla funktioner givet deras karaktär, omfattning och komplexitet. I dessa fall kan en enhet som står under tillsyn välja att anpassa resurstimmarna efter kontrollverksamheten eller att utkontraktera verksamheten.

## **Specialisering inom funktioner**

31. I takt med att en enhet som står under tillsyn växer och dess kontrollmiljö mognar bör den använda personalens specialisering för att dra nytta av personalens sakkunskap inom viktiga processer eller riskområden. Enheter med viss karaktär, omfattning och komplexitet bör ha särskilda övervaknings- eller utredningsgrupper inom sin regelefterlevnadsfunktion.

## **Kontrollverksamhetens mognad**

32. Kontrollverksamhetens mognad (dvs. manuell, hybridbaserad, automatiserad och i vissa fall med användning av AI-verktyg) bör återspegla karaktären, omfattningen och komplexiteten samt den övergripande riskprofilen hos en enhet som står under tillsyn. För enheter som står under tillsyn och som har en viss karaktär, omfattning och komplexitet bör det finnas en högre grad av automatiserade kontroller samt en större integrering mellan systemen för kontrollfunktioner för att optimera övervakningsverksamheten och en

enhets rapportering av ledningsinformation till den verkställande ledningen och ledningsorganet.

## **Moment 2.1 Funktion för regelefterlevnad**

33. Funktionen för regelefterlevnad vid en enhet som står under tillsyn ansvarar för att övervaka och rapportera om hur enheten och dess anställda fullgör de skyldigheter som följer av den relevanta förordningen. Funktionen för regelefterlevnad ansvarar för att följa ändringar i de lagar och andra förordningar som gäller för dess verksamhet. Funktionen för regelefterlevnad ansvarar även för att ge ledningsorganet råd om lagar, regler, förordningar och standarder som enheten som står under tillsyn måste följa samt, tillsammans med andra relevanta funktioner, bedöma den eventuella inverkan som ändringar i relevant lagstiftning eller regelverk kan få på enhetens verksamhet.

### **Egenskaper**

- 2.1.1** Funktionen för regelefterlevnad bör utföra sina uppgifter oberoende av affärsområdena och bör regelbundet rapportera till ledningsorganet för den enhet som står under tillsyn och, i förekommande fall, direkt till de oberoende icke-verkställande direktörerna.
- 2.1.2** Funktionen för regelefterlevnad bör råda och stödja de anställda i fullgörandet av de skyldigheter som följer av den relevanta förordningen. Funktionen för regelefterlevnad bör arbeta förebyggande med att identifiera risker och eventuell bristande efterlevnad genom övervakning och utvärdering av verksamheten i rätt tid, samt uppföljning av avhjälpande åtgärder.
- 2.1.3** Funktionen för regelefterlevnad bör säkerställa att övervakningen av efterlevnaden genomförs medelst ett strukturerat och väl definierat efterlevnadsövervakningsprogram. Den efterlevnadsrelaterade verksamheten bör omfatta alla affärs- och it-baserade processer och system som skulle kunna påverka enhetens efterlevnad av den relevanta förordningen.
- 2.1.4** Funktionen för regelefterlevnad, om så är lämpligt i samarbete med andra relevanta funktioner, bör bedöma den eventuella inverkan som ändringar i relevant lagstiftning eller regelverk kan få på enhetens verksamhet och i god tid kommunicera, där så är lämpligt, med funktionen för riskhantering om enhetens risk till följd av bristande regelefterlevnad.
- 2.1.5** Funktionen för regelefterlevnad bör säkerställa att policyer för regelefterlevnad följs och rapportera till ledningsorganet och den verkställande ledningen om enhetens risk till följd av bristande regelefterlevnad.

- 2.1.6 Funktionen för regelefterlevnad bör samarbeta med funktionen för riskhantering för att utbyta information som är nödvändig för deras respektive uppgifter.
- 2.1.7 De slutsatser som dras av funktionen för regelefterlevnad bör beaktas av ledningsorganet och den verkställande ledningen samt av funktionen för riskhantering inom ramen för deras riskbedömningsprocesser.

## **Moment 2.2 Funktion för riskhantering**

- 34. Funktionen för riskhantering vid en enhet som står under tillsyn ansvarar för utvecklingen och genomförandet av ramen för riskhantering.

### **Egenskaper**

- 2.2.1 Funktionen för riskhantering bör utföra sina uppgifter oberoende av de affärsområden och affärsenheter vars risker den övervakar, men bör inte hindras från att interagera med dem.
- 2.2.2 Funktionen för riskhantering bör säkerställa att alla de risker som skulle kunna påverka en enhet som står under tillsyn i fråga om dess förmåga att fullgöra sina skyldigheter enligt de relevanta förordningarna, eller dess fortsatta verksamhet, identifieras, bedöms och mäts. Väsentliga risker avseende dessa mål bör sedan i god tid övervakas, hanteras, mildras och korrekt rapporteras av och till de relevanta enheterna inom den enhet som står under tillsyn.
- 2.2.3 Funktionen för riskhantering bör övervaka riskprofilen för den enhet som står under tillsyn i förhållande till enhetens riskaptit för att möjliggöra beslutsfattande.
- 2.2.4 Funktionen för riskhantering bör ge råd om förslag som utarbetats och riskbeslut som fattats av affärsområden och informera ledningsorganet om huruvida dessa beslut är förenliga med enhetens riskaptit och mål.
- 2.2.5 Funktionen för riskhantering bör vid behov rekommendera förbättringar av ramen för riskhantering och ändringar av riskpolicyer och riskförfaranden. Funktionen för riskhantering bör se över risktrösklarna i enlighet med eventuella förändringar i organisationens riskaptit.

## **Moment 2.3 Funktion för ledning av informationssäkerhet (endast för enheter som står under tillsyn och som inte omfattas av DORA-förordningen)**

- 35. Funktionen för ledning av informationssäkerhet vid en enhet som står under tillsyn ansvarar för utvecklingen och genomförandet av informationssäkerheten inom enheten. En enhet som står under tillsyn bör inrätta en funktion som främjar en informationssäkerhetskultur inom enheten.

## **Egenskaper**

- 2.3.1** Funktionen för ledning av informationssäkerhet bör ansvara för att granska och övervaka enhetens efterlevnad av dess policyer och förfaranden för informationssäkerhet.
- 2.3.2** Funktionen för ledning av informationssäkerhet bör leda informationssäkerhetsverksamheten vid den enhet som står under tillsyn.
- 2.3.3** Funktionen för ledning av informationssäkerhet bör utveckla och införa ett program för att öka medvetenheten om informationssäkerhet bland personalen för att förbättra säkerhetskulturen och utveckla en bred förståelse för enhetens ram för informationssäkerhet.
- 2.3.4** Funktionen för ledning av informationssäkerhet bör rapportera och ge råd till ledningsorganet och den verkställande ledningen om statusen för systemet för ledning av informationssäkerhet och relaterade risker (t.ex. information om informationssäkerhetsprojekt, informationssäkerhetsincidenter och resultaten av översyner av informationssäkerheten).

## **Moment 2.4 Funktion för internrevision**

- 36. Funktionen för internrevision vid en enhet som står under tillsyn ansvarar för att tillhandahålla en oberoende, objektiv försäkrings- och rådgivningsverksamhet som är utformad för att förbättra organisationens verksamhet. Den hjälper organisationen att uppfylla sina mål genom införandet av ett systematiskt och disciplinerat tillvägagångssätt för utvärdering och förbättring av ändamålsenligheten i systemet för intern kontroll.

## **Egenskaper**

- 2.4.1** Funktionen för internrevision bör utföra sina uppgifter oberoende av affärsområdena och andra funktioner för intern kontroll. Funktionen bör regleras av en stadga för internrevision som definierar dess roll och ansvarsområden och som är föremål för ledningsorganets översyn.
- 2.4.2** Funktionen för internrevision bör följa ett riskbaserat tillvägagångssätt och efterleva internationella standarder för internrevision.
- 2.4.3** Funktionen för internrevision bör på ett oberoende sätt granska enhetens verksamheter, inklusive utkontrakterade verksamheter, och på ett objektivt sätt försäkra att de följer enhetens policyer och förfaranden samt uppfyller tillämpliga rättsliga och regelverksrelaterade krav.

- 2.4.4** Funktionen för internrevision bör minst en gång om året, på grundval av de årliga kontrollmålen för internrevision, upprätta en revisionsplan som står under ledningsorganets tillsyn.
- 2.4.5** Funktionen för internrevision bör regelbundet rapportera till ledningsorganets oberoende ledamöter eller till revisionskommittén, om en sådan finns.
- 2.4.6** Funktionen för internrevision bör delge sina revisionsrekommendationer på ett tydligt och enhetligt sätt för att ledningsorganet och den verkställande ledningen ska kunna förstå rekommendationernas väsentlighet och prioritera därefter.
- 2.4.7** Internrevisionsrekommendationerna bör vara föremål för ett formellt uppföljningsförfarande på lämpliga ledningsnivåer för rapportering om och säkerställande av deras effektiva och skyndsamma genomförande.

### **Moment 2.5 – Funktion för översyn (endast för kreditvärderingsinstitut)**

37. Funktionen för översyn vid ett kreditvärderingsinstitut ansvarar för att se över kreditvärderingsmetoderna minst en gång om året. Den ansvarar också för valideringen och översynen av nya metoder och eventuella ändringar av befintliga metoder.

#### **Egenskaper**

- 2.5.1** Funktionen för översyn bör utföra sina uppgifter oberoende av de affärsområden som är ansvariga för kreditvärderingen och tillhandahålla regelbundna rapporter till kreditvärderingsinstitutets oberoende icke-verkställande direktörer.
- 2.5.2** Kreditvärderingsinstitutets aktieägare eller personal som deltar i affärsutvecklingen bör inte utföra översynsfunktionens uppgifter.
- 2.5.3** Personal som arbetar med analys bör inte delta i godkännandet av nya, eller valideringen och granskningen av befintliga metoder, modeller och nyckelantaganden för kreditvärdering som de har utvecklat.
- 2.5.4** Personal som arbetar inom översynsfunktionen bör antingen ensamt vara ansvariga eller ha en majoritet av rösterna i de kommittéer som är ansvariga för att godkänna metoder, modeller och nyckelantaganden för kreditvärdering.
- 2.5.5** Personal som arbetar inom översynsfunktionen och ansvarar för valideringen och/eller översynen av en metod, och som också deltar i dess utvecklingsfas, bör inte ensamt vara ansvariga eller ha en majoritet av rösterna i kommittéerna för metodgodkännande.

**2.5.6** Vid utkontraktering av översynsfunktionen bör kreditvärderingsinstitutet beakta riktlinje 1.5.6. Dessutom bör kreditvärderingsinstitutet ha lämpliga mekanismer för intern kontroll för att säkerställa att det konsekvent följer de regelverksrelaterade kraven och upprätthåller lämpliga analytiska kvalitetsstandarder.

## **Moment 2.6 Övervakningsfunktion (endast för referensvärdesadministratörer)<sup>12</sup>**

38. Övervakningsfunktionen övervakar de viktigaste aspekterna i tillhandahållandet av referensvärden. Detta omfattar, men är inte begränsat till, översynen av referensvärdets definition och metod, förvaltningen av tredje parter som deltar i tillhandahållandet av referensvärdet, bedömningen av interna och externa revisioner eller översyner av administratörens kontrollram samt rapporteringen av eventuella fall av misskötsamhet till de relevanta behöriga myndigheterna.

### **Egenskaper**

**2.6.1** Referensvärdesadministratörens övervakningsfunktion bibehåller sitt oberoende i förhållande till andra ledningsorgan eller funktioner vid referensvärdesadministratören och till andra externa parter till referensvärdesadministratören. Oberoende förutsätter att det inte föreligger några intressekonflikter mellan den verksamhet som medlemmarna i övervakningsfunktionen bedriver i densamma och i deras övriga verksamheter. Referensvärdesadministratören bör införa en operativ ram för intern kontroll för att förebygga och mildra eventuella intressekonflikter.

**2.6.2** Referensvärdesadministratören bör ha tydliga policyer och förfaranden för inrättandet av övervakningsfunktionen samt för dess medlemmar och deras ansvarsområden, inklusive policyer och förfaranden för uppdateringar av referensvärdesmetoden och översyner av dataintegritet.

**2.6.3** Referensvärdesadministratörens övervakningsfunktion bör regelbundet utföra en självutvärdering för att bedöma sin effektivitet och medlemmarnas lämplighet för funktionens mål, och för att identifiera potentiella intressekonflikter och vid behov föreslå förbättringsområden.

**2.6.4** Referensvärdesadministratörens övervakningsfunktion bör upprätthålla en definierad och regelbunden kommunikationskanal med ledningsorganet, den verkställande ledningen och andra nyckelfunktioner. Referensvärdesadministratörens övervakningsfunktion bör också kunna ha

---

<sup>12</sup> Icke-betydande referensvärdesadministratörer som tillämpar artikel 26 i referensvärdesförordningen förväntas tillämpa dessa riktlinjer i proportion till de krav som framgår av artikel 26.

tillgång till och ifrågasätta ledningsinformation och erhålla uppdateringar om statusen för korrigerande åtgärder efter interna och externa revisioner, risker och efterlevnadsrapporter.

- 2.6.5** Referensvärdesadministratörens övervakningsfunktion bör upprätthålla en definierad kommunikationskanal med de relevanta behöriga myndigheterna, inbegripet för rapportering av eventuella fall av misskötsamhet eller överträdelser från administratörers eller rapportörers sida.