
EBA/GL/2024/06

6 juni 2024

Riktlinjer

för minimiinnehållet i styrningsarrangemangen för utgivare av
tillgångsanknutna token

Efterlevnads- och rapporteringskyldigheter

Riktlinjernas status

1. Detta dokument innehåller riktlinjer som har utfärdats i enlighet med artikel 16 i förordning (EU) nr 1093/2010¹. I enlighet med artikel 16.3 i förordning (EU) nr 1093/2010 ska behöriga myndigheter enligt definitionen i artikel 3.1.35' a i förordning (EU) 2023/1114 som omfattas av riktlinjerna och finansinstitut med alla tillgängliga medel söka följa riktlinjerna.
2. I riktlinjerna fastställs Europeiska bankmyndighetens (EBA) syn på lämplig tillsynspraxis inom det europeiska systemet för finansiell tillsyn eller på hur unionslagstiftningen bör tillämpas inom ett särskilt område. Behöriga myndigheter enligt definitionen i artikel 4.2 i förordning (EU) nr 1093/2010 som berörs av dessa riktlinjer bör följa dem genom att på lämpligt sätt införliva dem i sin praxis (till exempel genom att ändra sina rättsliga ramar eller tillsynsrutiner), även när riktlinjerna i första hand riktas till institut.

Rapporteringskrav

3. Enligt artikel 16.3 i förordning (EU) nr 1093/2010 ska behöriga myndigheter anmäla till EBA att de följer eller avser att följa dessa riktlinjer, alternativt ange skälen till att de inte gör det, senast den 20.11.2024. Om någon sådan anmälan inte inkommer inom denna tidsfrist kommer EBA att anse att de behöriga myndigheterna inte följer riktlinjerna. Anmälningarna ska lämnas in med hänvisningen EBA/GL/2024/01 via det formulär som tillhandahålls på EBA:s webbplats . Anmälningarna bör lämnas av personer med befogenhet att rapportera om hur reglerna tillämpas på sina behöriga myndigheters vägnar. Alla förändringar i graden av efterlevnad måste rapporteras till EBA.
4. Anmälningarna kommer att offentliggöras på EBA:s webbplats i enlighet med artikel 16.3.

¹ 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 (EUT L 331, 15.12.2010, s. 12).

Syfte, tillämpningsområde och definitioner

Innehåll

5. I dessa riktlinjer specificeras, i enlighet med artikel 34.13 i förordning (EU) 2023/1114, minimiinnehållet i styrningsarrangemangen för utgivare av tillgångsanknutna token, särskilt när det gäller verktygen för övervakning av riskerna², kontinuitetsplanerna, mekanismen för internkontroll och revisionerna, inbegripet den minimidokumentation som ska användas vid revisionerna.

Tillämpningsområde

6. Dessa riktlinjer gäller vid auktorisation och fortlöpande för behöriga myndigheter, enligt definitionen i artikel 3.1.35 a i förordning (EU) 2023/1114, och för utgivare av tillgångsanknutna token.
7. Riktlinjerna gäller alla utgivare av tillgångsanknutna token, oberoende av deras befintliga styrelsestrukturer.
8. Hänvisningar till ledningsorgan omfattar även utgivare av tillgångsanknutna token som är juridiska personer som leds av en enda fysisk person.
9. Utgivare av tillgångsanknutna token bör följa dessa riktlinjer, och de behöriga myndigheterna bör se till att utgivare av tillgångsanknutna token följer dessa riktlinjer, inbegripet, i tillämpliga fall, på gruppnivå.

Mottagare

10. Dessa riktlinjer riktar sig till behöriga myndigheter enligt definitionen i artikel 3.1.35 a i förordning (EU) 2023/1114.
11. Dessa riktlinjer riktar sig också till utgivare av tillgångsanknutna token enligt definitionen i artikel 3.1.10 i förordning (EU) 2023/1114 och tillgångsanknutna token enligt definitionen i artikel 3.1.6 i samma förordning. Om utgivaren av tillgångsanknutna token är ett kreditinstitut bör den följa avdelning I, avdelning V, avsnitten 12, 12.1, 12.2 12.3 samt avdelning VI och

² Alla hänvisningar till risker i dessa riktlinjer avser alla risker som utgivare av tillgångsanknutna token är eller kan bli exponerade för, inbegripet risker för penningtvätt och finansiering av terrorism.

avdelning VII tillsammans med de krav som fastställs i direktiv 2013/36/EU och EBA:s riktlinjer för intern styrning³.

Definitioner

12. Om inte annat anges har de termer som används och definieras i förordning (EU) 2023/1114, direktiv 2014/65/EU, EBA:s riktlinjer om interna styrningssystem för värdepappersföretag enligt direktivet om värdepappersföretag⁴ och förordning (EU) 2022/2554 samma betydelse i dessa riktlinjer. I dessa riktlinjer gäller dessutom följande definitioner:

Koncern	en koncern enligt definitionen i artikel 2.11 i direktiv 2013/34/EU ⁵ .
Ledningsorganet i dess ledningsfunktion	ledningsorganet när det agerar i sin roll att effektivt styra utgivaren av tillgångsanknutna token, inbegripet de personer som leder dess verksamhet.
Ledningsorganet i dess tillsynsfunktion	ledningsorganet, om det har inrättats, när det agerar i sin roll att ha uppsikt över och övervaka ledningens beslutsfattande.
Operativ motståndskraft	en utgivares förmåga att tillhandahålla kritiska eller viktiga funktioner vid avbrott i verksamheten.
Operativ risk	den operativa risk som anges i artikel 4.1.52 i förordning (EU) nr 575/2013.

Genomförande

Tillämpningsdatum

13. Dessa riktlinjer är tillämpliga från och med 20.12.2024.

³[Riktlinjer för intern styrning enligt direktiv 2013/36/EU](#)

⁴[Riktlinjer för intern styrning enligt direktiv \(EU\) 2019/2034](#)

⁵[Direktiv 2013/34/EU om årsbokslut, koncernredovisning och rapporter i vissa typer av företag](#)

Riktlinjer

Avdelning I – Tillämpning av proportionalitetsprincipen

14. Utgivare av tillgångsanknutna token och behöriga myndigheter bör ta hänsyn till proportionalitetsprincipen när de tillämpar och genomför dessa riktlinjer i syfte att säkerställa att styrningsarrangemangen är förenliga med den individuella riskprofilen för utgivaren av tillgångsanknutna token och koncernen, i tillämpliga fall, i proportion till dess storlek och interna organisation, relevanta för affärsmodellen, lämpliga för verksamhetens art, omfattning och komplexitet och tillräckliga för att effektivt uppnå målen för de relevanta lagstadgade kraven och bestämmelserna.

15. För tillämpningen av proportionalitetsprincipen och för att säkerställa ett lämpligt genomförande av styrningskraven i förordning (EU) 2023/1114, som specificeras närmare i dessa riktlinjer, bör utgivare av tillgångsanknutna token och behöriga myndigheter beakta följande kriterier:
 - a. Storleken på utgivaren av tillgångsanknutna token i förhållande till balansomslutningen.
 - b. Den rättsliga formen för utgivaren av tillgångsanknutna token.
 - c. Huruvida utgivaren av tillgångsanknutna token är börsnoterad eller inte.
 - d. Klassificeringen av det tillgångsanknutna token som utgivits som betydande eller icke-betydande i enlighet med artiklarna 43 och 44 samt artiklarna 56 och 57 i förordning (EU) 2023/1114.
 - e. Närmare uppgifter om samt antal och volym av utgivna tillgångsanknutna token.
 - f. Huruvida utgivna tillgångsanknutna token kommer att tas upp till handel.
 - g. Den konsensusmekanism som används för att ge ut och validera tillgångsanknutna token.
 - h. Samtliga affärsverksamheters art och komplexitet.
 - i. Typen av auktoriserad verksamhet och de tjänster som utförs.

- j. Huruvida gränsöverskridande verksamhet tillhandahålls och storleken på verksamheten i varje jurisdiktion.
 - k. Storleken på tillgångsreserven.
 - l. Typen av och komplexiteten hos de tillgångar som ett token hänvisar till.
 - m. Huruvida innehavarna av tillgångsanknutna token är icke-professionella innehavare.
 - n. Användning av tredjepartsleverantörer av tjänster.
 - o. De distributionskanaler som används, inbegripet de som tillhandahålls av tredjepartsleverantörer av tjänster.
 - p. Befintliga system för informations- och kommunikationsteknik (IKT), inbegripet åtgärder för kontinuitet i verksamheten och användning av IKT-tredjepartsenheter som avses i artikel 34.5 första stycket led h i förordning (EU) 2023/1114.
16. Utgivare av tillgångsanknutna token som förvaltas av en enda fysisk person bör ha alternativa arrangemang som säkerställer en sund och ansvarsfull ledning av sådana utgivare och ett adekvat beaktande av styrningsarrangemang, inbegripet genom att föreskriva adekvata kontroller och motvikter i beslutsfattandet.

Avdelning II – Förvaltningsorganets roll och sammansättning

1. Ledningens roll och ansvar

17. I enlighet med artikel 34 i förordning (EU) 2023/1114 ska ledningsorganet för en utgivare av tillgångsanknutna token definiera, övervaka och ansvara för genomförandet av sunda styrningssystem som säkerställer en effektiv och ansvarsfull ledning av utgivaren och intressena hos innehavarna av tillgångsanknutna token, inbegripet åtskillnad av funktioner och identifiering, förebyggande och hantering av intressekonflikter inom utgivaren av tillgångsanknutna token i enlighet med artikel 32 i förordning (EU) 2023/1114.
18. Ledningsorganets uppgifter bör vara tydligt definierade och, i tillämpliga fall, skilja mellan ledningsfunktionens (verkställande) uppgifter och tillsynsfunktionens (icke-verkställande) uppgifter. Ledningsorganets ansvarsområden och uppgifter bör beskrivas i ett skriftligt dokument och vederbörligen godkännas av ledningsorganet. Alla ledamöter i ledningsorganet bör vara fullt medvetna om ledningsorganets struktur och ansvarsområden och, i tillämpliga fall, om fördelningen av uppgifter mellan ledningsorganets olika funktioner.
19. I tillämpliga fall bör ledningsorganet i sin tillsynsfunktion och sin ledningsfunktion samverka effektivt. Båda funktionerna bör förse varandra med den information som behövs för att de ska kunna fullgöra sina respektive uppgifter. För att det ska finnas lämpliga kontroller och motvikter

bör beslutsfattandet inom ledningsorganet inte domineras av en enda ledamot eller en liten undergrupp av dess ledamöter.

20. Ledningsorganets ansvar bör åtminstone omfatta att fastställa, godkänna och övervaka genomförandet av

- a. utgivarens övergripande affärsstrategi och viktigaste policyer inom den tillämpliga rättsliga ramen, med hänsyn till utgivarens långsiktiga finansiella intressen och solvens och intressen hos innehavarna av tillgångsanknutna token,
- b. de policyer som krävs enligt artikel 34.5 i förordning (EU) 2023/1114; dessa policyer bör vara förenliga med utgivarens riskaptit och risktolerans samt med egenskaperna och behoven hos de kunder till utgivare av tillgångsanknutna token som de kommer att erbjudas till och deras presumtiva innehavare,
- c. utgivarens organisation för utgivning av tillgångsanknutna token, med angivande av färdigheter, kunskaper och expertis som krävs av personalen och nödvändiga resurser,
- d. den övergripande riskstrategin, utgivarens riskaptit och ram för riskhantering, inbegripet lämpliga policyer och förfaranden, med beaktande av den makroekonomiska miljön och konjunkturcykeln, och med specificering av ledningsorganets deltagande i riskhanteringsfrågor,
- e. en lämplig och effektiv ram för intern kontroll, inbegripet en ram för riskhantering och välfungerande mekanismer för internkontroll, för att säkerställa efterlevnad av tillämpliga lagstadgade krav, inbegripet när det gäller förvaltningen av tillgångsreserven,
- f. en ersättningspolicy för utgivare av betydande tillgångsanknutna token som är i linje med artikel 45.1 i förordning (EU) 2023/1114⁶,
- g. policyerna och förfarandena för att identifiera, förhindra, hantera och redovisa intressekonflikter i enlighet med artikel 32 i förordning (EU) 2023/1114⁷,
- h. arrangemang som syftar till att säkerställa att ledningsorganets individuella och kollektiva lämplighetsbedömningar genomförs effektivt, att ledningsorganets

⁶Se de tekniska tillsynsstandarderna om minimiinnehållet i styrningsarrangemangen för ersättningspolicyn för utgivare av betydande tekniska standarder i enlighet med artikel 45.7 a i förordning (EU) 2023/1114.

⁷ Se de tekniska tillsynsstandarderna för intressekonflikter enligt artikel 32.5 i förordning (EU) 2023/1114.

sammansättning är lämplig och att ledningsorganet utför sina uppgifter ändamålsenligt,

- i. en riskkultur i linje med avdelning VI avsnitt 7 som avser riskmedvetenheten och riskbeteendet hos utgivaren av tillgångsanknutna token,
 - j. en företagskultur och värderingar i linje med avdelning IV avsnitt 8 som främjar ansvarstagande och etiskt beteende, inklusive en uppförandekod eller ett liknande instrument,
 - k. arrangemang som syftar till att säkerställa integriteten hos systemen för redovisning och finansiell rapportering, inbegripet finansiella och operativa kontroller samt efterlevnad av lagstiftning och relevanta standarder.
21. När ledningsorganet inrättar, godkänner och övervakar genomförandet av de aspekter som förtecknas i punkt 20 bör det säkerställa att affärsmodellen och styrningsarrangemangen tar hänsyn till alla risker som utgivaren av tillgångsanknutna token är eller kan bli exponerad för och de risker som de utgör eller kan utgöra för andra och för miljön. I detta syfte bör utgivare av tillgångsanknutna token också ta hänsyn till alla relevanta riskfaktorer, inbegripet riskfaktorer avseende miljö, samhällsansvar och bolagsstyrning (ESG) och beakta de klimateffekter och andra miljöeffekter som orsakas av energiförbrukningen i de konsensus- och valideringsmekanismer som används. Andra riskfaktorer avseende miljö, samhällsansvar och bolagsstyrning som bör beaktas inkluderar rättsliga risker på området avtals- eller arbetsrätt, risker relaterade till potentiella människorättskränkningar eller andra riskfaktorer avseende miljö, samhällsansvar och bolagsstyrning som kan påverka det land där en tredjepartsleverantör är etablerad och dess förmåga att tillhandahålla de överenskomna servicenivåerna.
 22. Ledningsorganet bör övervaka förfarandet för offentliggörande, särskilt i enlighet med artikel 30 i förordning (EU) 2023/1114, och kommunikationen med externa intressenter och behöriga myndigheter.
 23. Alla ledamöter i ledningsorganet bör informeras om utgivarens övergripande verksamhet, finansiella situation och risksituation, med beaktande av den ekonomiska miljön och konjunkturcykeln, och även om alla beslut som fattas som har en betydande inverkan på utgivningen av tillgångsanknutna token eller annan väsentlig affärsverksamhet.
 24. En ledamot i ledningsorganet får ansvara för en intern kontrollfunktion enligt vad som anges i avdelning V, förutsatt att ledamoten inte har andra uppdrag som skulle kunna äventyra dennes interna kontrollarbete och den interna kontrollfunktionens oberoende ställning.
 25. Ledningsorganet bör övervaka, regelbundet se över och åtgärda eventuella brister som konstaterats när det gäller genomförandet av processer, strategier och policyer som rör de ansvarsområden som anges i detta avsnitt. Styrningsramen och dess genomförande bör ses

över och uppdateras regelbundet, med beaktande av proportionalitetsprincipen, såsom specificeras närmare i avdelning I. En fördjupad granskning bör utföras om väsentliga förändringar påverkar utgivaren av tillgångsanknutna token.

26. Om utgivarna av tillgångsanknutna token är juridiska personer som förvaltas av en enda fysisk person i enlighet med deras bolagsordning och nationella lagstiftning, bör hänvisningarna i dessa riktlinjer till ett ledningsorgan tolkas som att de gäller för den enda person som ansvarar för genomförandet av alternativa arrangemang för att säkerställa en sund och ansvarsfull ledning av en sådan utgivare och ett lämpligt beaktande av styrningsarrangemang.

2. Ledningsorganets ledningsfunktion

27. Ledningsorganet i sin ledningsfunktion bör aktivt engagera sig i den verksamhet som utgivaren av tillgångsanknutna token bedriver och bör fatta beslut på ett sunt och välinformerat sätt.
28. Ledningsorganet i sin ledningsfunktion bör ansvara för genomförandet av de strategier och policyer som fastställs av ledningsorganet och regelbundet diskutera genomförandet och lämpligheten av dessa strategier och policyer med ledningsorganet i sin tillsynsfunktion. Det operativa genomförandet kan utföras av ledningsorganet för utgivarna av tillgångsanknutna token.
29. Ledamöter i ledningsorganet i dess ledningsfunktion bör konstruktivt ifrågasätta och kritiskt granska förslag, förklaringar och information som personalen får när den utövar sitt omdöme och fattar beslut.
30. Ledningsorganet i sin ledningsfunktion bör i tillämpliga fall regelbundet, uttömmande och i god tid meddela och till ledningsorganet i dess tillsynsfunktion rapportera all relevant information som är nödvändig för att det ska kunna utföra sina uppgifter, inbegripet risker och annan utveckling som påverkar verksamhet för utgivaren av tillgångsanknutna token, t.ex. väsentliga beslut om affärsverksamhet, dess organisation och underliggande teknik, risker som tas och överensstämmelse med riskaptiten och riskstrategin, risker för penningtvätt och finansiering av terrorism, IKT-incidenter och IKT-rapportering, väsentliga förluster till följd av operativa risker, likviditet och tillgångsreserv samt hantering av dessa.

3. Ledningsorganets tillsynsfunktion

31. Utan att det påverkar tilldelade ansvarsområden enligt gällande nationell bolagsrätt bör ledningsorganet i sin tillsynsfunktion
 - a. utöva tillsyn över och övervaka ledningens beslutsfattande och åtgärder och utöva ändamålsenlig tillsyn över ledningsorganet i dess ledningsfunktion, inbegripet att övervaka och granska dess individuella och kollektiva resultat samt fastställandet och genomförandet av strategierna och målen för utgivaren av tillgångsanknutna token,

- b. på ett konstruktivt sätt ifrågasätta och kritiskt granska förslag och information som lämnas av ledamöter i ledningsorganet i dess ledningsfunktion samt ledningsorganets beslut,
- c. säkerställa och regelbundet bedöma ändamålsenligheten i styrningsramen för utgivarna av tillgångsanknutna token och vidta lämpliga åtgärder för att åtgärda eventuella konstaterade brister,
- d. utöva tillsyn över och övervaka att utgivarens strategiska mål, organisationsstruktur och riskstrategi, dess riskaptit och ram för riskhantering samt andra policyer (t.ex. investeringspolicy för reserven av tillgångar) genomförs på ett konsekvent sätt,
- e. övervaka att riskkulturen hos utgivaren av tillgångsanknutna token tillämpas konsekvent,
- f. övervaka genomförandet, uppdateringen och den ändamålsenliga tillämpningen av policyer och förfaranden för att identifiera, förhindra, hantera och redovisa intressekonflikter i enlighet med artikel 32 i förordning (EU) 2023/1114,⁸
- g. övervaka integriteten hos finansiell information och rapportering samt ramen för intern kontroll, inbegripet en effektiv och sund ram för riskhantering,
- h. säkerställa att cheferna för interna kontrollfunktioner kan agera oberoende och oaktat ansvaret att rapportera till andra interna organ, affärsområden eller enheter, har möjlighet att ge uttryck för oro och när så krävs direkt varna ledningsorganet i dess tillsynsfunktion om ogynnsam riskutveckling som påverkar eller kan påverka utgivaren av tillgångsanknutna token,
- i. fastställa och övervaka genomförandet av internrevisionsplanen.

Kapitel III – Styrningsram

4. Organisatorisk ram och struktur

4.1 Organisatorisk ram

32. Ledningsorganet för en utgivare av tillgångsanknutna token bör säkerställa en lämplig och öppen organisatorisk och operativ struktur för utgivaren av tillgångsanknutna token och bör ha en skriftlig beskrivning av den. Strukturen bör främja och visa en ändamålsenligt och ansvarsfull ledning av utgivaren av tillgångsanknutna token och koncernen, i tillämpliga fall.

⁸ Se de tekniska tillsynsstandarderna för intressekonflikter enligt artikel 32.5 i förordning (EU) 2023/1114.

33. Ledningsorganet bör se till att de interna kontrollfunktionerna har de lämpliga ekonomiska resurserna, personalresurserna och befogenheterna som behövs för att de ska kunna fullgöra sina uppgifter på ett ändamålsenligt sätt. Som ett minsta krav bör funktionen för regelefterlevnad fungera oberoende och det bör finnas en lämplig åtskillnad mellan funktioner. Rapporteringsvägarna och ansvarsfördelningen bör vara tydliga, väldefinierade, konsekventa, verkställbara och vederbörligen dokumenterade. Dokumentationen bör uppdateras när så är lämpligt.
34. Strukturen hos utgivaren av tekniska tillsynsstandarder bör inte hindra ledningsorganets förmåga att övervaka och på ett ändamålsenligt sätt hantera dess risker eller koncernen, i tillämpliga fall, är exponerad för eller den behöriga myndighetens förmåga att effektivt övervaka utgivaren av tekniska tillsynsstandarder.
35. Ledningsorganet bör bedöma om och hur väsentliga förändringar i koncernens struktur i tillämpliga fall (t.ex. inrättande av nya dotterbolag, fusioner och förvärv, försäljning eller avvecklingsdelar av koncernen, eller extern utveckling) påverkar sundheten i den organisatoriska ramen för utgivare av ny teknik. Om brister konstateras bör ledningsorganet snabbt göra nödvändiga anpassningar.

4.2 Känna till strukturen

36. Ledningsorganet bör ha full kännedom om och förstå värdepappersföretagets juridiska, organisatoriska och operativa struktur ("känna till strukturen") och se till att den överensstämmer med företagets godkända affärs- och riskstrategi och riskaptit samt att den innefattas i dess ram för riskhantering.
37. Ledningsorganet bör säkerställa att strukturen hos en utgivare av tillgångsanknutna instrument och, i tillämpliga fall, strukturerna inom en koncern är tydlig, effektiv och transparent för personalen, aktieägarna och andra intressenter och för den behöriga myndigheten.
38. Ledningsorganet bör vägleda utgivarens struktur, dess utveckling och dess begränsningar och bör säkerställa att strukturen är motiverad och effektiv och inte medför onödig eller olämplig komplexitet.
39. När sådana strukturer inrättas bör ledningsorganet förstå dem och deras syfte samt de särskilda risker som är förknippade med dem, och se till att de interna kontrollfunktionerna är delaktiga på lämpligt sätt. Dessa strukturer bör godkännas och upprätthållas endast när deras syfte har definierats tydligt och förståtts och när ledningsorganet är förvissat om att alla väsentliga risker, inbegripet anseenderisker, har identifierats, att alla risker kan hanteras effektivt och rapporteras korrekt samt att en effektiv tillsyn har säkerställts. Ju mer komplex den organisatoriska och operativa strukturen är, och ju större riskerna är, desto intensivare bör övervakningen av strukturen vara.

40. Utgivare av tillgångsanknutna token bör i sitt beslutsfattande ta hänsyn till resultaten av en riskbedömning som gjorts för att fastställa om sådana strukturer skulle kunna användas för ett ändamål som är kopplat till penningtvätt och finansiering av terrorism eller annan ekonomisk brottslighet för att säkerställa att utgivaren eller sektorn inte utsätts för en allvarlig risk för penningtvätt och finansiering av terrorism. I detta syfte bör utgivare av tillgångsanknutna token åtminstone ta hänsyn till följande:
- a. Den utsträckning i vilken jurisdiktionen där strukturen ska inrättas effektivt efterlever EU-standarder och internationella standarder för skatteinsyn, bekämpning av penningtvätt och motverkande av finansiering av terrorism.
 - b. I vilken utsträckning strukturen har ett tydligt ekonomiskt och lagligt syfte.
 - c. I vilken utsträckning strukturen skulle kunna användas för att dölja identiteten på den verkliga huvudmannen.
 - d. I vilken utsträckning det skäl som leder till ett eventuellt inrättande av en struktur ger anledning till oro.
 - e. Om strukturen kan hindra lämplig tillsyn från ledningsorganet för utgivaren av tillgångsanknutna token eller utgivarens förmåga att hantera den relaterade risken.
 - f. Huruvida strukturen utgör ett hinder för de behöriga myndigheternas ändamålsenliga tillsyn.
41. I vilket fall som helst bör utgivare av tillgångsanknutna token inte inrätta otydliga eller onödigt komplexa strukturer som inte har något tydligt ekonomiskt rationellt eller rättsligt syfte, eller strukturer som skulle kunna väcka farhågor om att dessa kan komma att skapas för ett ändamål som har samband med ekonomisk brottslighet.
42. Utgivare av tillgångsanknutna token bör dokumentera sina beslut och kunna motivera sina beslut inför behöriga myndigheter.
43. Dessa strukturer och verksamheter, inbegripet deras efterlevnad av lagstiftning och yrkesstandarder, bör ses över regelbundet. Om en internrevisionsfunktion har inrättats bör den genomföra översynen utifrån en riskbaserad metod.

5. Organisatorisk ram i ett koncernsammanhang

44. I tillämpliga fall bör utgivare av tillgångsanknutna token säkerställa att arrangemang, processer och mekanismer för styrning är konsekventa och väl integrerade på gruppnivå. I detta syfte bör utgivare av tillgångsanknutna token säkerställa att deras dotterföretag som omfattas av förordning (EU) 2023/1114 genomför liknande arrangemang, processer och mekanismer för att säkerställa robusta styrformer på gruppnivå. Behöriga funktioner hos en utgivare av

tillgångsanknutna token och dess dotterföretag som omfattas av förordning (EU) 2023/1114 bör samverka och utbyta data och information på lämpligt sätt.

45. Policyer och dokumentation kan ingå i separata dokument, men utgivare av tillgångsanknutna token bör överväga att kombinera dem eller hänvisa till dem i ett enda dokument för styrningsramen.

6. Utkontraktering⁹

46. Ledningsorganet bör godkänna och regelbundet se över och uppdatera utkontrakteringspolicyn för en utgivare av tillgångsanknutna token och se till att lämpliga ändringar genomförs i rätt tid.
47. Utkontrakteringspolicyn bör beakta hur användningen av utkontraktering påverkar en utgivare av tillgångsanknutna token och de risker den står inför (t.ex. operativa risker, inbegripet rättsliga risker, anseenderisker och koncentrationsrisker).
48. Policyn bör omfatta de rapporterings- och övervakningsarrangemang som ska genomföras från början till slutet av utkontrakteringsarrangemangen (inbegripet processen för kundkännedom och riskbedömning, hanteringen och övervakningen av arrangemanget, uppsägning, beredskapsplaner och exitstrategier).
49. Utkontraktering av funktioner får inte leda till delegering av ledningsorganens ansvarsområden. En utgivare av tillgångsanknutna token förblir fullständigt ansvarig för alla utkontrakterade tjänster och verksamheter och ledningsbeslut som följer av dem. I enlighet med detta bör policyn för utkontraktering klargöra att utkontrakteringen inte befriar utgivaren av tillgångsanknutna token från dess förpliktelser enligt lagar och andra författningar.
50. I policyn bör det anges att utkontrakteringsarrangemang inte bör hindra en ändamålsenlig tillsyn av utgivaren av tillgångsanknutna token på plats eller på distans och att de inte bör strida mot eventuella tillsynsbegränsningar av tjänster och verksamhet. Policyn bör också omfatta koncerninterna utkontrakteringsarrangemang och, när så är lämpligt, ta hänsyn till eventuella särskilda koncernförhållanden.
51. Utgivare av tillgångsanknutna token bör alltid ha tillräckligt med substans och inte bli "tomma skal" eller "brevlådeföretag". För detta ändamål bör de
 - a. alltid uppfylla alla villkor för auktorisationen, inbegripet att ledningsorganet på ett ändamålsenligt sätt fullgör sina skyldigheter enligt avsnitt I i dessa riktlinjer,

⁹ Detta avsnitt bör i tillämpliga fall läsas tillsammans med avsnitt 12.3 i dessa riktlinjer. Utgivare av tillgångsanknutna instrument bör, i den mån det är tillämpligt, hänvisa till EBA:s riktlinjer för utkontraktering, med beaktande av tillämpningen av proportionalitetsprincipen.

- b. ha en tydlig och transparent organisatorisk ram och struktur som gör det möjligt för dem att säkerställa efterlevnad av de förpliktelser enligt lagar och andra författningar som avses i avsnitt 4,
- c. om interna kontrollfunktioners operativa uppgifter utkontrakteras, utöva lämplig tillsyn och kunna hantera de risker som genereras vid utkontrakteringen av kritiska eller viktiga funktioner,
- d. ha tillräckliga resurser och kapacitet för att säkerställa efterlevnad av punkterna a till c.

Kapitel IV – Riskkultur och uppförande

7. Riskkultur

- 52. En sund, omsorgsfull och konsekvent riskkultur bör vara central för utgivare av tillgångsanknutna token när det gäller effektiv riskhantering och bör göra det möjligt för dessa utgivare att fatta sunda och välgrundade beslut som är förenliga med deras riskstrategi och riskaptit.
- 53. Utgivare av tillgångsanknutna token bör utveckla en integrerad och företagsövergripande riskkultur, som baseras på en fullständig förståelse av och helhetssyn på de risker de är eller kan bli exponerade för, inbegripet ESG-risker, risker för tillgångsinnehavare, marknadsrisker, operativa risker, risker för penningtvätt och finansiering av terrorism, likviditetsrisker och risker kopplade till investeringar i tillgångarna i reserven, risken för utgivaren av tillgångsanknutna token och hur de hanteras, med beaktande av risktoleransen hos utgivaren av tillgångsanknutna token och de intressekonflikter som kan uppstå till följd av kopplingen mellan aktörer i kryptoecosystemet.
- 54. Utgivare av tillgångsanknutna token bör utveckla en riskkultur genom riktlinjer, kommunikation och fortbildning av personal när det gäller verksamhet, strategi och riskprofil för utgivare av tillgångsanknutna token, och bör anpassa kommunikationen och fortbildningen för att ta hänsyn till personalens ansvar när det gäller risktagande och riskhantering.
- 55. Personalen bör ha full kännedom om sina ansvarsområden och skyldigheter avseende riskhantering. Riskhanteringen bör inte skötas av enbart riskspecialister eller interna kontrollfunktioner. Affärsområden eller affärsenheter bör, under överinseende av ledningsorganet, i första hand ansvara för den dagliga riskhanteringen i linje med riktlinjerna, förfarandena och kontrollerna för utgivare av tillgångsanknutna token, med beaktande av dessa utgivares risktolerans och riskaptit.
- 56. En stark riskkultur bör innefatta, men är inte nödvändigtvis begränsad till, följande:

- a. Ledningens exempel: Ledningsorganet bör ansvara för att fastställa och kommunicera utgivarens kärnvärden och förväntningar. Ledningsorganets ledamöter bör uppföra sig på ett sätt som speglar dessa värden. Ledningsorganet bör bidra till den interna kommunikationen av grundläggande värderingar och förväntningar till personalen. Personalen bör agera i enlighet med alla gällande lagar och regler och skyndsamt anmäla överträdelser som observeras inom eller utanför institutet (exempelvis till den behöriga myndigheten via ett uppgiftslämnarsystem).
- b. Ansvarsskyldighet: relevant personal på alla nivåer bör känna till och förstå de grundläggande värdena hos utgivaren av tillgångsanknutna token och i den mån det är nödvändigt för deras roll och risktolerans och riskaptit. De bör kunna fullgöra sina uppgifter och vara medvetna om att de kommer att ställas till svars för sina handlingar i förhållande till utgivarens risktagande.
- c. Ändamålsenlig kommunikation och ifrågasättande: en sund riskkultur bör främja ett klimat med öppen kommunikation och ändamålsenligt ifrågasättande där beslutsprocesserna gynnar ett brett spektrum av åsikter, ger möjlighet att utmana gällande praxis, uppmuntrar ett konstruktivt och kritiskt förhållningssätt hos personalen och främjar ett klimat präglat av öppet och konstruktivt engagemang i hela organisationen.
- d. Incitament: lämpliga incitament bör spela en viktig roll när det gäller att anpassa riskbeteendet till utgivarens riskprofil och dess långsiktiga intressen, särskilt för utgivare av betydande tillgångsanknutna token.

8. Företagsvärderingar och uppförandekod

57. Ledningsorganet bör utveckla, anta, följa och främja höga etiska och yrkesmässiga standarder, med beaktande av de särskilda behoven och särdragen hos utgivaren av tillgångsanknutna token, och bör säkerställa att sådana standarder genomförs (genom en uppförandekod eller ett liknande instrument). Ledningsorganet bör också övervaka personalens efterlevnad av dessa standarder. I tillämpliga fall kan ledningsorganet anta och genomföra koncernomfattande standarder som tillämpas av utgivare av tillgångsanknutna token och har getts ut av föreningar eller andra relevanta organisationer.
58. Utgivare av tillgångsanknutna token bör säkerställa att det inte förekommer någon diskriminering av personal på grund av kön, ras, hudfärg, etniskt eller socialt ursprung, genetiska särdrag, språk, religion eller övertygelse, politisk eller annan åskådning, tillhörighet till nationell minoritet, förmögenhet, börd, funktionsnedsättning, ålder eller sexuell läggning.

59. De policyer som tillämpas av utgivare av tillgångsanknutna token bör vara könsneutrala¹⁰. Detta inkluderar men är inte begränsat till ersättning, rekryteringspolicyer, karriärutveckling och efterträdarplanering, tillgång till utbildning och möjligheten att söka interna lediga tjänster. Utgivare av tillgångsanknutna token bör säkerställa lika möjligheter¹¹ för all personal oavsett kön, även när det gäller karriärutsikter, och sträva efter att förbättra representationen av det underrepresenterade könet på positioner inom ledningsorganet. Utgivare av betydande tillgångsanknutna token bör övervaka utvecklingen av löneklyftan mellan kvinnor och män.
60. De standarder som genomförs bör syfta till att förbättra utgivarens robusta styrformer och minska de risker som företaget är exponerat för, särskilt operativa risker och anseenderisker, som kan ha en betydande negativ inverkan på utgivarens lönsamhet och hållbarhet genom böter, rättegångskostnader, restriktioner som åläggs av behöriga myndigheter, andra ekonomiska och straffrättsliga påföljder samt förlust av varumärkesvärde och investerarnas förtroende.
61. Ledningsorganet bör ha tydliga och dokumenterade policyer för hur dessa standarder bör uppfyllas. Syftet med dessa policyer bör vara att
- a. påminna personalen om att all verksamhet för utgivare av tillgångsanknutna token bör bedrivas i enlighet med tillämplig lagstiftning och utgivarens företagsvärderingar,
 - b. främja riskmedvetenhet genom en stark riskkultur i enlighet med avdelning IV, avsnitt 6, som förmedlar ledningsorganets förväntningar att verksamheten inte kommer att gå utöver den riskaptit och de riskgränser som fastställts av utgivaren av tillgångsanknutna token samt personalens respektive ansvar,
 - c. fastställa principer för och ge exempel på acceptabla och oacceptabla beteenden som i synnerhet är kopplade till finansiell felrapportering och misskötsamhet, ekonomisk och finansiell brottslighet, inbegripet men inte begränsat till bedrägeri, penningtvätt och finansiering av terrorism, antitrustmetoder, ekonomiska sanktioner, mutor och korruption, otillbörlig marknadspåverkan, vilseledande försäljning och andra överträdelser av konsumentskyddslagstiftningen samt skattebrott, oavsett om de begås direkt eller indirekt,
 - d. klargöra att personalen utöver att uppfylla de krav som ställs i lagar och andra författningar samt interna policyer också förväntas uppföra sig hederligt och med

¹⁰ Se de tekniska tillsynsstandarderna om minimiinhålllet i styrningsarrangemangen för ersättningspolicyer för utgivare av betydande tillgångsanknutna token i enlighet med artikel 45.7 a i förordning (EU) 2023/1114.

¹¹ Se även Europaparlamentets och rådets direktiv 2006/54/EG av den 5 juli 2006 om genomförandet av principen om lika möjligheter och likabehandling av kvinnor och män i arbetslivet.

integritet och utföra sina uppgifter med vederbörlig skicklighet, omsorg och aktsamhet,

- e. se till att personalen är medveten om de potentiella interna och externa disciplinära åtgärder, rättsliga åtgärder och sanktioner som kan följa av tjänstefel och oacceptabla beteenden.

62. Utgivare av tillgångsanknutna token bör övervaka efterlevnaden av sådana standarder och säkerställa personalens medvetenhet, t.ex. genom att tillhandahålla utbildning.

Avdelning V – Ram och mekanismer för intern kontroll

9. Ram för intern kontroll

63. Utgivare av tillgångsanknutna token bör utveckla och upprätthålla en kultur som uppmuntrar till en positiv inställning till riskkontroll och efterlevnad hos utgivaren och en robust och heltäckande ram för intern kontroll. Inom denna ram bör affärsområden eller interna enheter för utgivare av tillgångsanknutna token eller interna enheter vara ansvariga för att hantera de risker de ådrar sig när de bedriver sin verksamhet och bör ha kontroller på plats som syftar till att säkerställa att interna och externa krav efterlevs. Som en del av denna ram bör utgivare av tillgångsanknutna token ha en permanent och ändamålsenlig intern funktion för regelefterlevnad med lämplig och tillräcklig befogenhet, ställning och tillgång till ledningsorganet för att kunna fullgöra sitt uppdrag, samt en ram för riskhantering. Om det är proportionerligt, med beaktande av de kriterier som anges i avdelning I, bör utgivare av tillgångsanknutna token också ha en intern riskhanterings- och revisionsfunktion. Under alla omständigheter bör utgivaren av tillgångsanknutna token ha lämpliga policyer och förfaranden för riskhantering och revision.
64. Ramen för intern kontroll för de berörda utgivarna av tillgångsanknutna token bör anpassas individuellt till verksamhetens särdrag, dess komplexitet och de därmed förbundna riskerna, i förekommande fall med beaktande av koncernsammanhanget. Inom en koncern bör den berörda utgivaren av tillgångsanknutna token organisera utbytet av nödvändig information på ett sätt som säkerställer att varje ledningsorgan, affärsområde och intern enhet, inklusive varje intern kontrollfunktion, kan utföra sina uppgifter.
65. Ramen för intern kontroll bör omfatta hela organisationen, inbegripet ledningsorganets ansvar och uppgifter, samt verksamheten inom alla affärsområden och interna enheter, inbegripet interna kontrollfunktioner, användningen av tredjepartsleverantörer och distributionskanaler.
66. Ramen för intern kontroll för en utgivare av tillgångsanknutna token bör säkerställa följande:
- a. Ändamålsenlig och effektiv verksamhet, inbegripet när det gäller utgivning av tillgångsanknutna token.
 - b. Lämplig identifiering, mätning och begräsning av risker, inbegripet operativa risker och IKT-relaterade risker, i enlighet med förordning (EU) 2022/2554.
 - c. Tillförlitligheten i finansiell och icke-finansiell information som rapporteras både internt och externt.
 - d. Sunda rutiner för administration och redovisning.
 - e. Efterlevnad av lagar och andra författningar samt tillsynskrav och interna policyer, processer, regler och beslut avseende utgivaren av tillgångsanknutna token.

10. Genomförande av en ram för intern kontroll

67. Ledningsorganet bör ansvara för att fastställa och övervaka lämpligheten och ändamålsenligheten i ramen, processerna och mekanismerna för intern kontroll, och för att övervaka alla affärsområden och interna enheter, inbegripet interna kontrollfunktioner (t.ex. regelefterlevnads-, riskhanterings- och internrevisionsfunktioner om sådana inrättats). Utgivare av tillgångsanknutna token bör upprätta, upprätthålla och regelbundet uppdatera lämpliga skriftliga policyer, mekanismer och interna kontrollförfaranden, vilka bör godkännas av ledningsorganet. Om ingen riskhanteringsfunktion har inrättats bör ledningsorganet ansvara för att upprätta, uppdatera och övervaka lämpliga förfaranden och policyer för riskhantering.
68. En utgivare av tillgångsanknutna token bör ha en tydlig, transparent och dokumenterad beslutsprocess och en tydlig fördelning av ansvar och befogenheter inom ramen för internkontroll, inbegripet affärsområden, interna enheter och interna kontrollfunktioner.
69. Utgivare av tillgångsanknutna token bör kommunicera dessa policyer, mekanismer och förfaranden till all personal och varje gång väsentliga ändringar har gjorts.
70. De interna kontrollfunktionerna bör kontrollera att de policyer, mekanismer och förfaranden som föreskrivs i ramen för intern kontroll tillämpas på ett korrekt sätt inom deras respektive behörighetsområden.
71. De interna kontrollfunktionerna bör regelbundet lämna skriftliga rapporter till ledningsorganet om allvarliga brister som har konstaterats. Dessa rapporter bör innehålla information om relevanta risker, en konsekvensbedömning, rekommendationer och korrigerande åtgärder som ska vidtas avseende varje ny allvarlig brist som har konstaterats. Ledningsorganet bör följa upp de interna kontrollfunktionernas slutsatser i god tid och på ett ändamålsenligt sätt och bör utfärda krav om lämpliga korrigerande åtgärder. Ett formellt uppföljningsförfarande för slutsatser och korrigerande åtgärder som har vidtagits bör etableras.

11. Ram för riskhantering

72. Som en del av den övergripande ramen för intern kontroll bör utgivare av tillgångsanknutna token ha en övergripande ram för riskhantering som omfattar hela utgivaren och alla deras affärsområden och interna enheter, däribland interna kontrollfunktioner, och fullt ut erkänner den ekonomiska substansen i alla deras riskexponeringar, inbegripet de risker som utgivaren av tillgångsanknutna token innebär för sig själv, innehavarna av tillgångar, operativa risker och risker som härrör från tillgångsreserver.
73. Ramen för riskhantering bör göra det möjligt för utgivaren av tillgångsanknutna token att fatta välgrundade beslut om alla risker som de är eller kan bli exponerade för, inbegripet IKT-risker i

enlighet med förordning (EU) 2022/2554 (DORA-förordningen) och¹² avsnitt 12. Ramen för riskhantering bör omfatta alla risker, inbegripet faktiska risker och framtida risker som utgivaren av tillgångsanknutna token kan bli exponerad för. Riskerna bör utvärderas nedifrån och upp och uppifrån och ned, inom och mellan affärsområden eller interna enheter, med hjälp av konsekvent terminologi och kompatibla metoder hos hela utgivaren av tillgångsanknutna token och i tillämpliga fall på gruppnivå. Alla relevanta risker bör ingå i ramen för riskhantering med vederbörlig hänsyn till både finansiella och icke-finansiella risker, inbegripet koncentrationsrisker, operativa risker, IKT-risker, anseenderisker, rättsliga risker, uppföranderisker och ESG-risker. Hänsyn bör också tas till kreditrisk, marknadsrisk, koncentrationsrisk och likviditetsrisk som härrör från reservtillgångarna.

74. Ramen för riskhantering för en utgivare av tillgångsanknutna token bör inkludera riktlinjer, förfaranden, riskgränser och riskkontroller som säkerställer lämplig, snabb och kontinuerlig identifiering, mätning eller bedömning, övervakning, hantering, begränsning och rapportering av risker inom affärsområden och interna enheter samt på utgivar- och koncernnivå, i tillämpliga fall.
75. Ramen för riskhantering för en utgivare av tillgångsanknutna token bör ge särskild vägledning om genomförandet av riskstrategier. Denna vägledning bör, när så är lämpligt, fastställa och upprätthålla interna gränser som är förenliga med utgivarens risktolerans och riskaptit och stå i proportion till utgivarens sunda funktion, operativa motståndskraft, finansiella styrka, likviditetsbehov och strategiska mål. Riskprofilen för utgivare av tillgångsanknutna token bör hållas inom de fastställda gränserna. Ramen för riskhantering bör säkerställa att det finns en fastställd process för att rapportera, anmäla och åtgärda överträdelser av riskgränserna genom ett lämpligt uppföljningsförfarande.
76. Ramen för riskhantering bör vara föremål för oberoende intern granskning, som till exempel utförs av internrevisionsfunktionen, och regelbundet bedömas gentemot risktoleransen och riskaptiten för utgivaren av tillgångsanknutna token.
77. Regelbundna och transparenta rapporteringsmekanismer bör inrättas så att ledningsorganet och alla relevanta enheter hos utgivaren av tillgångsanknutna token får rapporter i tid och på ett korrekt, koncist, begripligt och meningsfullt sätt samt kan utbyta relevant information om identifiering, mätning eller bedömning, övervakning och hantering av risker. Rapporteringsramen bör vara tydligt definierad och dokumenterad.
78. Ändamålsenlig kommunikation och medvetenhet om risker och riskstrategin är avgörande för hela riskhanteringsprocessen, inbegripet översyns- och beslutsprocesserna, och bidrar till att förhindra beslut som oavsiktligt kan öka riskerna. Ändamålsenlig riskrapportering innebär ett sunt internt övervägande och kommunikation av riskstrategin och relevanta riskdata, både

¹² Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn: [Publikationsbyrå \(europa.eu\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2554)

horisontellt mellan utgivaren av finansiella transaktioner och uppåt och nedåt i hanteringskedjan.

12. Hantering av operativa risker och operativ motståndskraft

79. En utgivare av tillgångsanknutna token bör ha en lämplig ram för hantering av operativa risker och en ram för operativ motståndskraft. Detta inbegriper effektiva policyer och processer för att
- a. i god tid identifiera, bedöma, utvärdera, övervaka, rapportera och minska operativa risker, och
 - b. identifiera och skydda sig mot hot och potentiella fel, reagera på och anpassa sig till samt återhämta sig från och lära av störande händelser för att minimera deras inverkan på tillhandahållandet av kritiska eller viktiga funktioner¹³.
80. En utgivare av tillgångsanknutna token bör, som en del av ramen för riskhantering, godkänna strategier, policyer och processer för hantering av operativa risker och operativ motståndskraft, inbegripet riskaptiten för ramen för operativa risker och risktoleransen för störning av kritiska eller viktiga funktioner¹⁴. Dessa strategier, policyer och processer bör regelbundet ses över och uppdateras vid behov.
81. Ledningsorganet säkerställer att dessa riktlinjer och processer genomförs på ett ändamålsenligt sätt och integreras fullt ut i utgivarens övergripande ram för riskhantering, inbegripet risken i samband med användningen av tredjepartsenheter, och effektivt kommuniceras till relevant personal.
82. En utgivare av tillgångsanknutna token bör på ett tydligt sätt fastställa ansvaret för bedömnings- och förvaltningssystemet för operativ risk och operativ motståndskraft.
83. En utgivare av tillgångsanknutna token bör identifiera sina exponeringar för operativ risk, spåra relevanta operativa riskdata, inklusive data om väsentliga förluster, och utföra scenarioanalyser.
84. Utgivare av tillgångsanknutna token bör identifiera sin kritiska verksamhet, i enlighet med sin strategi för operativ motståndskraft, samt kartlägga personer, teknik, processer, data, anläggningar, tredje parter, inbegripet koncerninterna enheter, samt de kopplingar och ömsesidiga beroenden mellan dem som är nödvändiga för att tillhandahålla kritiska eller viktiga funktioner i en situation med oförändrade förhållanden och vid störningar.

¹³ Baselkommittén för banktillsyn, Principles for Operational Resilience, mars 2021, <https://www.bis.org/bcbs/publ/d516.pdf>

¹⁴ Toleransen för störningar är nivån på störningar till följd av alla typer av operativa risker som en utgivare är villig att godta mot bakgrund av en rad allvarliga men rimliga scenarier.

85. Ramen för hantering av operativ risk och operativ motståndskraft bör vara föremål för regelbundna granskningar som utförs av interna eller externa revisorer som har den kunskap som krävs för att utföra sådana granskningar. Ramen för hantering av operativa risker och ramen för operativ motståndskraft bör vara uppbyggda med tillräckliga och lämpliga mänskliga och tekniska resurser. Utgivaren av tillgångsanknutna token bör ha ett system för bedömning av operativa risker och en ram för operativ motståndskraft som är helt integrerad i utgivarens ram för riskhantering.
86. Det bör införas ett system för rapportering till ledningsorganet som omfattar adekvata rapporter om operativa risker och operativ motståndskraft från relevanta funktioner hos utgivaren av tillgångsanknutna token. Utgivaren av tillgångsanknutna token bör förfoga över förfaranden som gör det möjligt att utan dröjsmål vidta lämpliga åtgärder, när så är tillämpligt.
87. Utgivaren av tillgångsanknutna token bör identifiera och bedöma den operativa risk som är inneboende i utgivarens verksamhet, processer och system för tillgångsanknutna token för att säkerställa en god förståelse av de inneboende riskerna.
88. Med beaktande av avdelning I om tillämpningen av proportionalitetsprincipen bör utgivare av tillgångsanknutna token identifiera, analysera och mäta ett antal scenarier, inbegripet händelser med låg sannolikhet och hög allvarlighetsgrad, varav vissa kan leda till allvarliga förluster till följd av operativa risker. Bidrag till scenarioanalysen omfattar relevanta interna och externa förlustdata, information från självbedömningar, expertutlåtanden, ramen för intern kontroll, framåtblickande mått, orsaksanalyser och processramen, i förekommande fall. Scenarioanalysprocessen bör användas för att utveckla en rad konsekvenser av potentiella händelser, inbegripet konsekvensbedömningar för riskhanteringsändamål, som komplement till andra verktyg baserade på historiska data eller aktuella riskbedömningar.
89. Med beaktande av avdelning I kan utgivare av tillgångsanknutna token använda kvalitativa riskbedömningsstrategier, men utgivare av betydande tillgångsanknutna token bör ha en mer sofistikerad metod som förekommande fall inbegriper användning av interna och externa förlustdata som underlag för scenarioanalysen.

12.1 Godkännande av nya produkter, system och processer

90. Utgivaren av tillgångsanknutna token bör ha policyer och förfaranden för bedömning och godkännande av nya produkter, processer och system, inbegripet när det gäller nyutgivning av tillgångsanknutna token och tillhörande processer och system.
91. Godkännandeprocessen bör beakta alla risker, inbegripet rättsliga risker och IKT-risker, vid lanseringen av nya produkter och vid införandet av nya processer och system, och inbegripa risker kopplade till personer, processer, system och externa händelser.
92. Godkännandeprocessen bör också beakta effekterna på tillhandahållandet av kritiska eller viktiga funktioner och på deras kopplingar och ömsesidiga beroenden samt förändringar av den

operativa riskprofilen för utgivare av tillgångsanknutna token, inbegripet ändringar av risken i samband med befintliga produkter eller verksamheter, nödvändiga interna kontroller, riskhanteringsprocesser och riskreducering.

93. Utgivaren av tillgångsanknutna token bör säkerställa bedömningen av utvecklingen av risker i samband med nya produkter, system och processer över tid under hela livscykeln för en produkt, verksamhet eller tjänst.
94. Utgivare av tillgångsanknutna token bör ha ett starkt system för intern kontroll i enlighet med avdelning V, även med avseende på nya produkter, processer och system, för att säkerställa att utgivaren av tillgångsanknutna token har en effektiv och ändamålsenlig verksamhet, samt skydda sin tillgångsreserv, ta fram tillförlitlig information och följa tillämpliga lagar och förordningar.

12.2 IKT-riskhantering

95. Utgivare av tillgångsanknutna token bör inrätta en ram för IKT-riskhantering i enlighet med de krav som fastställs i förordning (EU) 2022/2554. I detta avseende bör utgivare av tillgångsanknutna token ha inrättat en ram för intern styrning och kontroll som säkerställer en effektiv och ansvarsfull hantering av IKT-risker för att uppnå en hög nivå av digital operativ motståndskraft¹⁵.

12.3 Arrangemang med tredjepartsenheter för drift av tillgångsreserven, för investering av reservtillgångarna, förvaring av reservtillgångarna eller distribution av tillgångsanknutna token till allmänheten

96. Ledningsorganet för en utgivare av tillgångsanknutna token som har arrangemang med tredjepartsenheter för drift av tillgångsreserven, för investering av reservtillgångarna, förvaring av reservtillgångarna eller, i tillämpliga fall, för distribution av tillgångsanknutna token till allmänheten eller planer på att ingå sådana arrangemang bör godkänna, regelbundet se över och uppdatera en policy för kraven på dessa tredjepartsenheters operativa beroende och säkerställa att de genomförs individuellt och, i tillämpliga fall, på koncernnivå.
97. Denna policy bör omfatta de huvudsakliga faserna i livscykeln för dessa tredjepartsarrangemang och definiera principer, ansvarsområden och processer i förhållande till användningen av tredje part. I synnerhet bör policyn minst omfatta
- a. ledningsorganets ansvar, inbegripet, när så är lämpligt, dess deltagande i beslutsfattandet,

¹⁵ Se förordning (EU) 2022/2554, EUT L 333, 27.12.2022, s. 1–79.

- b. involveringen av affärsområden, interna kontrollfunktioner och andra enskilda personer när det gäller dessa arrangemang,
 - c. planeringen och struktureringen av tredjepartsarrangemang, inbegripet fastställandet av verksamhetskrav rörande användning av tredje parter,
 - d. identifiering, bedömning och hantering av risker i enlighet med avsnitt 11,
 - e. kundkännedomskontroller av presumtiva tredje parter,
 - f. policyer och förfaranden för att identifiera, förebygga, hantera och redovisa intressekonflikter i enlighet med artikel 32 i förordning (EU) 2023/1114,
 - g. kontinuitetsplanerings- och exitstrategier för att säkerställa den operativa motståndskraften hos utgivaren av tillgångsanknutna token i händelse av ett fel eller en störning hos en tredjepartsenhet som påverkar tillhandahållandet av kritisk verksamhet. Kontinuitets- och exitplanerna för utgivaren av tillgångsanknutna token bör bedöma utbytbarheten hos den tredjepartsenhet som används för kritisk verksamhet och andra genomförbara alternativ som kan underlätta den operativa motståndskraften i händelse av avbrott vid en tredjepartsenhet, t.ex. genom att åter utföra verksamheten internt,
 - h. godkännandeförfarandet för nya arrangemang,
 - i. genomförandet, övervakningen och hanteringen av dessa arrangemang, inbegripet den pågående bedömningen av tredjepartsenheternas resultat för att säkerställa att förbindelsen ligger inom ramen för riskaptiten och toleransen för störningar av kritiska verksamheter och kärnaffärsområden hos utgivaren av tillgångsanknutna token,
 - j. förfarandena för att underrättas om och svara på ändringar i ett arrangemang från tredjepartsenheter,
 - k. den oberoende granskningen och revisionen av efterlevnad av lagar och andra författningar samt policyer,
 - l. förnyelseprocesserna för arrangemang med tredjepartsenheter,
 - m. dokumentation och registerföring och
 - n. exitstrategier och uppsägningsprocesser, inbegripet ett krav på en dokumenterad exitplan för varje arrangemang med en tredjepartsenhet, om en sådan exit anses vara möjlig, med beaktande av eventuella avbrott i tjänsten eller oväntad uppsägning av avtal.
98. Utgivare av tillgångsanknutna token bör bedöma den potentiella effekten av arrangemang med tredjepartsenheter på deras operativa risk och operativa motståndskraft, i enlighet med avsnitt

- 12, och bör ta hänsyn till bedömningsresultaten när de beslutar om huruvida en funktion bör utföras av en tredjepartsenhet och bör vidta lämpliga åtgärder för att undvika onödiga ytterligare operativa risker innan de ingår dessa arrangemang.
99. Inom ramen för riskbedömningen bör utgivaren av tillgångsanknutna token också ta hänsyn till de förväntade fördelarna och kostnaderna med det föreslagna arrangemanget, inbegripet en avvägning av eventuella risker som kan reduceras eller hanteras bättre mot eventuella risker som kan uppstå till följd av det föreslagna arrangemanget, med beaktande av åtminstone de åtgärder som vidtagits av utgivaren av tillgångsanknutna token och av tjänsteleverantören för att hantera och minska dessa risker.
100. Vid genomförandet av riskbedömningen, innan man förlitar sig på en tredjepartsenhet och under den pågående övervakningen av tredjepartsenhetens resultat, bör utgivare av tillgångsanknutna token åtminstone göra följande:
- a. Identifiera och klassificera relevanta funktioner och tillhörande data och system med avseende på deras känslighet och kritikalitet samt nödvändiga säkerhetsåtgärder.
 - b. Genomföra en grundlig riskbaserad analys av de funktioner och tillhörande data och system som övervägs för arrangemanget och hantera de potentiella riskerna, särskilt de operativa riskerna, inbegripet underleverantörsrisker, rättsliga risker, IKT-risker, efterlevnadsrisker och anseenderisker, och de tillsynsbegränsningar som rör de länder där tjänsterna tillhandahålls eller kan komma att tillhandahållas.
 - c. Beakta de geografiska beroendena och hanteringen av tillhörande risker. Dessa risker kan hänföra sig till den ekonomiska, finansiella, politiska och rättsliga miljön i den eller de jurisdiktioner där den berörda tjänsten kommer att finnas.
101. Innan de ingår ett avtal med en tredje part och med beaktande av riskerna, inbegripet operativa risker och motpartsrisker, bör utgivare av tillgångsanknutna token i sin urvals- och bedömningsprocess säkerställa att tredjepartsenheten är lämplig.
102. Utgivare av tillgångsanknutna token bör säkerställa att tredjepartsenheten har ett gott affärsansesende, lämplig och tillräcklig kompetens, sakkunskap, kapacitet, resurser (t.ex. personal, it, ekonomi), organisationsstruktur och, i tillämpliga fall, de lagstadgade tillstånd eller registreringar som krävs för att utföra funktionen på ett tillförlitligt och professionellt sätt för att uppfylla sina skyldigheter under avtalets löptid.
103. Ytterligare faktorer som ska beaktas vid kundkännedomsgrensning av en potentiell tredjepartsenhet omfattar, men är inte begränsade till, följande:
- a. Dess affärsmodell, karaktär, omfattning, komplexitet, finansiella situation, ägarstruktur och koncernstruktur.

- b. De långsiktiga förbindelserna med den tredje part som redan har bedömts och utför tjänster för utgivaren av tillgångsanknutna token.
 - c. Graden av utbytbarhet hos tjänsten och tjänsteleverantören, inbegripet möjligheten att lämna tredjepartsarrangemanget och antingen övergå till en annan tjänsteleverantör eller åter utföra den kritiska tjänsten internt, eller hur sådant utbyte kan påverka den kritiska verksamheten hos utgivaren av tillgångsanknutna token.
 - d. Huruvida tredjepartsenheten står under de behöriga myndigheternas tillsyn.
104. Utgivare av tillgångsanknutna token bör vidta lämpliga åtgärder för att säkerställa att tredje parten agerar på ett sätt som är förenligt med deras värderingar och uppförandekod.
105. Utgivare av tillgångsanknutna token bör alltid säkerställa att den tredje part de använder för att distribuera tillgångsanknutna token till allmänheten följer de förfaranden som säkerställer efterlevnad av skyldigheterna när det gäller förebyggande av penningtvätt och finansiering av terrorism enligt direktiv (EU) 2015/849 och, i tillämpliga fall, förordning (EU) 2023/1113 om uppgifter som ska åtfölja överföringar av medel och vissa kryptotillgångar. Tredjepartsenheten bör i sina interna kontrollsystem säkerställa en kontinuerlig efterlevnad av skyldigheterna avseende förhindrande av penningtvätt och finansiering av terrorism enligt direktiv (EU) 2015/849 och, i tillämpliga fall, förordning (EU) 2023/1113 om uppgifter som ska åtfölja överföringar av medel och vissa kryptotillgångar.

13. Interna kontrollfunktioner

106. De interna kontrollfunktionerna bör inbegripa en ändamålsenlig och permanent intern funktion för regelefterlevnad och, när så är lämpligt och proportionellt med beaktande av de kriterier som anges i avdelning I, en riskhanteringsfunktion samt en internrevisionsfunktion. I de fall utgivare av tillgångsanknutna token inte inrättar och upprätthåller en riskhanteringsfunktion och en internrevisionsfunktion bör de på begäran kunna visa att de policyer och förfaranden som antagits och införts för en ram för intern kontroll leder till samma resultat som riktlinjerna som föreskrivs i denna avdelning V.
107. Utgivare av betydande tillgångsanknutna token uppmuntras att inrätta interna riskhanterings- och internrevisionsfunktioner. Om utgivaren av tillgångsanknutna token inte inrättar en intern riskhanteringsfunktion eller en internrevisionsfunktion ska ansvaret för dessa funktioner enligt dessa riktlinjer ligga hos ledningsorganet, som kan delegera de operativa uppgifterna internt eller externt till en tredjepartsleverantör, t.ex. i form av ett utkontrakteringsarrangemang¹⁶.

13.1 Chefer för de interna kontrollfunktionerna

108. Chefer för de interna kontrollfunktionerna bör tillsättas på en nivå i hierarkin som är tillräcklig för att dessa chefer ska ha den befogenhet och ställning som krävs för att de ska kunna

¹⁶ Utkontraktering av operativa uppgifter i fråga om efterlevnad kan fortfarande vara möjlig.

fullgöra sina skyldigheter. Chefen för regelefterlevnad och, i förekommande fall, cheferna för riskhanterings- och internrevisionsfunktionerna bör rapportera till och vara direkt ansvariga inför ledningsorganet, och chefernas resultat och prestationer bör granskas av ledningsorganet.

109. Cheferna för interna kontrollfunktioner bör i tillämpliga fall ha tillgång till, samt rapportera direkt till, ledningsorganet i dess tillsynsfunktion så att cheferna har möjlighet att lyfta frågor och problem samt om lämpligt varna tillsynsfunktionen när specifika skeenden påverkar eller kan komma att påverka värdepappersföretaget. Detta bör inte hindra cheferna för de interna kontrollfunktionerna från att även kunna rapportera via de vanliga rapporteringsvägarna.
110. Utgivare av tillgångsanknutna token bör ha dokumenterade processer för att tillsätta tjänsten som chef för en intern kontrollfunktion och för att dra tillbaka dennes ansvar. I vilket fall som helst bör cheferna för interna kontrollfunktioner inte avsättas utan förhandsgodkännande från ledningsorganet i dess tillsynsfunktion där det är etablerat.

13.2 De interna kontrollfunktionernas oberoende ställning

111. För att de interna kontrollfunktionerna ska anses vara oberoende bör följande villkor vara uppfyllda:
- a. Deras personal utför inte några verksamhetsuppgifter som faller inom ramen för den verksamhet som de interna kontrollfunktionerna är avsedda att övervaka och kontrollera, såvida det inte kan påvisas att de interna kontrollfunktionerna förblir ändamålsenliga mot bakgrund av de kriterier som anges i avdelning I för tillämpningen av proportionalitetsprincipen. I detta fall bör utgivaren av tillgångsanknutna token bedöma huruvida deras interna kontrollfunktioners ändamålsenlighet äventyras.
 - b. De är, när så är lämpligt, organisatoriskt åtskilda från den verksamhet som de ska övervaka och kontrollera.
 - c. Ersättningen till de interna kontrollfunktionernas personal bör inte vara kopplad till genomförandet av den verksamhet som respektive kontrollfunktion ska övervaka och kontrollera och bör inte heller på annat sätt kunna äventyra personalens objektivitet¹⁷.

13.3 De interna kontrollfunktionernas resurser

112. De interna kontrollfunktionerna bör ha tillräckliga resurser. Med beaktande av tillämpningen av proportionalitetsprincipen enligt avdelning I bör de ha ett tillräckligt antal

¹⁷ Se även EBA:s riktlinjer för en sund ersättningspolicy, som finns på <https://www.eba.europa.eu/regulation-and-policy/remuneration/guidelines-on-sound-remuneration-policies>.

kvalificerade anställda med lämpliga färdigheter, kunskaper och erfarenheter. Personalen bör förbli kvalificerad och få fortbildning när så behövs.

113. Interna kontrollfunktioner bör ha lämpliga IKT-system och stöd till sitt förfogande samt ha tillgång till den interna och externa information som är nödvändig för att de ska kunna fullgöra sina skyldigheter. De bör ha tillgång till all nödvändig information om alla affärsområden och relevanta riskbärande dotterföretag, särskilt sådana som potentiellt kan ge upphov till väsentliga risker för utgivaren av tillgångsanknutna token.

14. Riskhanteringsfunktion

114. Om en riskhanteringsfunktion har inrättats bör den omfatta hela utgivaren av tillgångsanknutna token. Riskhanteringsfunktionen bör, med beaktande av de proportionalitetskriterier som anges i avdelning I, ha de befogenheter och resurser samt den ställning som krävs för att kunna genomföra riskpolicyer och inrätta den ram för riskhantering som beskrivs i avsnitt 11.
115. Riskhanteringsfunktionen bör vid behov ha direkt tillgång till ledningsorganet i dess tillsynsfunktion, om en sådan har inrättats.
116. Riskhanteringsfunktionen bör ha tillgång till alla affärsområden och andra interna enheter som har potential att generera risker.
117. Personalen vid riskhanteringsfunktionen bör ha tillräckliga kunskaper, färdigheter och erfarenheter när det gäller riskhanteringsmetoder och riskhanteringsförfaranden samt marknader och produkter, och bör ha tillgång till regelbunden fortbildning.
118. Riskhanteringsfunktionen bör, om en sådan har inrättats, vara ett centralt organisatoriskt inslag hos utgivaren av tillgångsanknutna token och vara strukturerad så att den kan genomföra riskpolicyer och kontrollera ramen för riskhantering. Riskhanteringsfunktionen bör spela en viktig roll för att säkerställa att utgivaren av tillgångsanknutna token har effektiva riskhanteringsprocesser på plats. Riskhanteringsfunktionen bör vara delaktig i alla väsentliga beslut som rör riskhantering. I en koncern bör riskhanteringsfunktionen i moderföretaget inom unionen i tillämpliga fall kunna ge en koncernövergripande helhetssyn på alla risker och säkerställa att riskstrategin följs.
119. Riskhanteringsfunktionen bör tillhandahålla relevant, oberoende information, analyser och expertbedömningar om riskexponeringar, och ge råd om förslag och riskbeslut från affärsområden eller interna enheter, samt bör informera ledningsorganet om huruvida sådan information och rådgivning är förenlig med riskprofilen för utgivaren av tillgångsanknutna token. Riskhanteringsfunktionen får rekommendera förbättringar av ramen för riskhantering och korrigerande åtgärder för att åtgärda överträdelser av riskrelaterade policyer, förfaranden och gränser.

14.1 Riskhanteringsfunktionens roll i riskstrategi och riskbeslut

120. Riskhanteringsfunktionens delaktighet i beslutsprocesser bör säkerställa att risköverbägganden beaktas på lämpligt sätt. Ansvar för de beslut som fattas bör emellertid ligga kvar hos affärsenheterna och de interna enheterna, och det yttersta ansvaret bör ligga hos ledningsorganet.

14.2 Riskhanteringsfunktionens roll vid väsentliga förändringar

121. Innan beslut fattas om väsentliga ändringar av produkter, processer eller system eller om exceptionella transaktioner bör riskhanteringsfunktionen vara delaktig i utvärderingen av effekten av sådana förändringar på utgivaren av tillgångsanknutna token och rapportera sina resultat direkt till ledningsorganet innan ett beslut fattas.
122. Riskhanteringsfunktionen bör utvärdera hur de identifierade riskerna kan påverka förmågan hos utgivaren av tillgångsanknutna token att hantera sin riskprofil och de risker som är kopplade till tillgångsreserven.

14.3 Riskhanteringsfunktionens roll när det gäller att identifiera, mäta, bedöma, hantera, reducera, övervaka och rapportera risker

123. Riskhanteringsfunktionen bör säkerställa ett lämpligt genomförande av ramen för riskhantering och att alla risker identifieras, bedöms, mäts, övervakas, hanteras och rapporteras på ett korrekt sätt av de relevanta enheterna hos utgivaren av tillgångsanknutna token.
124. Riskhanteringsfunktionen bör säkerställa att identifieringen och bedömningen av risker inte enbart utgår från kvantitativ information eller modellresultat, utan även grundas på kvalitativa metoder. Riskhanteringsfunktionen bör hålla ledningsorganet informerat om de antaganden som används i och de potentiella bristerna hos verktygen och metoderna för riskkvantifiering, inbegripet modeller och analyser.
125. Riskhanteringsfunktionen bör säkerställa att transaktioner med närstående parter granskas och att de risker de utgör för utgivaren av tillgångsanknutna token identifieras och bedöms på lämpligt sätt.
126. Riskhanteringsfunktionen bör säkerställa att alla identifierade risker övervakas effektivt av affärsenheterna eller de interna enheterna.
127. Riskhanteringsfunktionen bör regelbundet övervaka den faktiska riskprofilen för utgivaren av tillgångsanknutna token och granska den mot de strategiska målen och riskaptiten samt rapportera resultaten för att göra det möjligt för ledningsorganet att fatta beslut i sin ledningsfunktion och för ledningsorganet att hantera utmaningar i sin tillsynsfunktion.

128. Riskhanteringsfunktionen bör analysera tendenser och erkänna nya eller framväxande risker och riskökningar som uppstår till följd av förändrade omständigheter och förhållanden. Den bör också regelbundet granska faktiska riskresultat i förhållande till tidigare uppskattningar (dvs. utfallstester) för att bedöma och förbättra riskbedömningsmetodernas och riskhanteringsprocessens exakthet och effektivitet.
129. Riskhanteringsfunktionen bör utvärdera möjliga sätt att minska de identifierade riskerna. Riskrapporteringen till ledningsorganet bör innehålla förslag till lämpliga riskreducerande åtgärder.

14.4 Riskhanteringsfunktionens roll i fråga om riskaptit och riskgränser

130. Riskhanteringsfunktionen bör göra en oberoende bedömning av överträdelser av riskaptiten eller riskgränserna. Riskhanteringsfunktionen bör informera de berörda affärsenheterna eller interna enheterna och ledningsorganet och rekommendera möjliga avhjälpande åtgärder. Riskhanteringsfunktionen bör rapportera direkt till ledningsorganet i dess tillsynsfunktion när överträdelsen är väsentlig, utan att det påverkar riskhanteringsfunktionens möjlighet att även rapportera till andra interna funktioner.
131. Riskhanteringsfunktionen bör ha en central roll i att säkerställa att ett beslut beträffande dess rekommendation fattas på relevant nivå och att beslutet efterlevs av de relevanta affärsenheterna samt rapporteras på lämpligt sätt till ledningsorganet och i förekommande fall riskkommittén.

14.5 Chef för riskhanteringsfunktionen

132. Chefen för riskhanteringsfunktionen bör, om en sådan har inrättats, ansvara för att tillhandahålla heltäckande och begriplig information om risker och ge råd till ledningsorganet, så att detta organ kan förstå riskprofilen för utgivaren av tillgångsanknutna token. I de fall ingen oberoende funktion har inrättats ligger de ansvarsområden som tilldelas chefen för riskhanteringsfunktionen hos den personal som ansvarar för riskhanteringsförfarandena eller hos ledamöterna i ledningsorganet.
133. Chefen för riskhanteringsfunktionen bör ha tillräcklig sakkunskap, oberoende och senioritet för att kunna bestrida beslut som påverkar riskexponeringen för en utgivare av tillgångsanknutna token. I de fall chefen för riskhanteringsfunktionen inte är en ledamot i ledningsorganet bör utgivaren av tillgångsanknutna token, med beaktande av proportionalitetsprincipen i avdelning I, utse en oberoende person till rollen som chef för riskhanteringsfunktionen som inte har ansvar för några andra funktioner och som rapporterar direkt till ledningsorganet. Om det inte är proportionerligt att utse en person som enbart ägnar sig åt rollen som chef för riskhanteringsfunktionen mot bakgrund av proportionalitetsprincipen i avdelning I, kan denna roll kombineras med rollen som chef för funktionen för regelefterlevnad eller utföras av en annan person i ledande ställning, förutsatt att det inte

föreligger någon intressekonflikt mellan de uppgifter som utförs. Under alla omständigheter bör denna person ha tillräcklig auktoritet och ställning samt vara oberoende (t.ex. chef för rättsliga frågor).

134. Chefen för riskhanteringsfunktionen bör kunna ifrågasätta de beslut som fattas av utgivarens ledning och dess ledningsorgan, och skälen till invändningarna bör dokumenteras formellt. Om en utgivare av tillgångsanknutna token vill ge chefen för riskhanteringsfunktionen rätten att inlägga veto mot beslut (t.ex. ett kredit- eller investeringsbeslut eller fastställandet av en gräns) på nivåer under ledningsorganet, bör denne ange omfattningen av en sådan vetorätt, förfaranden för upptrappning eller överklagande och på vilket sätt ledningsorganet ska involveras i processen.
135. Utgivare av tillgångsanknutna token bör inrätta förstärkta processer för godkännande av beslut om vilka chefen för riskhanteringsfunktionen har uttryckt en negativ uppfattning. Ledningsorganet bör i sin tillsynsfunktion kunna kommunicera direkt med chefen för riskhanteringsfunktionen om viktiga riskfrågor, inbegripet utveckling som kan vara oförenlig med riskstrategin och riskaptiten för utgivaren av tillgångsanknutna token, och chefen för riskhanteringsfunktionen bör kunna rapportera väsentliga problem direkt till ledningsorganet i dess ledningsfunktion.

15. Funktion för regelefterlevnad

136. Utgivare av tillgångsanknutna token bör inrätta en permanent och effektiv funktion för regelefterlevnad för att hantera efterlevnadsrisker och bör utse en person som ska ansvara för denna funktion inom hela enhetens verksamhet (den regelefterlevnadsansvarige).
137. Den regelefterlevnadsansvariges roll kan, med beaktande av proportionalitetsprincipen i avdelning I, kombineras med rollen som chef för riskhanteringsfunktionen eller, om det inte är proportionellt att utse en person som enbart ägnar sig åt denna roll, utföras av en annan person i ledande ställning (t.ex. chef för rättsliga frågor), förutsatt att det inte föreligger någon intressekonflikt mellan de uppgifter som utförs.
138. Personalen vid funktionen för regelefterlevnad bör ha tillräckliga kunskaper, färdigheter och erfarenheter när det gäller regelefterlevnad och relevanta förfaranden, och bör ha tillgång till regelbunden fortbildning.
139. Ledningsorganet i dess tillsynsfunktion bör övervaka genomförandet av en väldokumenterad policy för regelefterlevnad, och denna bör förmedlas till all personal. Utgivare av tillgångsanknutna token bör inrätta en process för att regelbundet bedöma ändringar i de lagar och förordningar som är tillämpliga på dess verksamhet.
140. Funktionen för regelefterlevnad bör ge ledningsorganet råd om åtgärder som ska vidtas för att säkerställa efterlevnad av tillämpliga lagar, regler, förordningar och standarder, och bör

bedöma de potentiella följder som ändringar av lagstiftningen eller regelverket kan få för värdepappersföretagets verksamhet och regelefterlevnadsram.

141. Funktionen för regelefterlevnad bör se till att efterlevnaden övervakas med hjälp av ett strukturerat och väldefinierat program för efterlevnadsövervakning och att efterlevnadspolicyn följs. Funktionen för regelefterlevnad bör rapportera till ledningsorganet och i förekommande fall kommunicera med riskhanteringsfunktionen om efterlevnadsrisken för utgivaren av tillgångsanknutna token och hanteringen av denna risk. Funktionen för regelefterlevnad och riskhanteringsfunktionen bör samarbeta och utbyta information på lämpligt sätt för att fullgöra sina respektive uppgifter. Iakttagelser som görs av funktionen för regelefterlevnad bör beaktas av ledningsorganet och riskhanteringsfunktionen när dessa fattar beslut.
142. Utgivare av tillgångsanknutna token bör vidta lämpliga åtgärder mot internt eller externt beteende som skulle kunna underlätta eller möjliggöra bedrägeri eller ekonomisk brottslighet och disciplinöverträdelser (t.ex. överträdelser av interna förfaranden eller överskridanden av gränser).

16. Internrevisionsfunktion

143. Om en internrevisionsfunktion har inrättats bör den vara oberoende och ha tillräckliga befogenheter och resurser samt tillräcklig ställning. Utgivare av tillgångsanknutna token bör i synnerhet se till att kvalificeringen av internrevisionsfunktionens personal och internrevisionsfunktionens resurser, särskilt dess revisionsverktyg och riskanalysmetoder, är lämplig för storleken på och placeringen av utgivaren av tillgångsanknutna token samt för arten, omfattningen och komplexiteten av de risker som är förknippade med affärsmodellen, verksamheten, riskkulturen och riskaptiten för utgivaren av tillgångsanknutna token.
144. Internrevisionsfunktionen bör vara oberoende av den verksamhet som den granskar. Den bör därför inte kombineras med andra funktioner.
145. Internrevisionsfunktionen bör, genom ett riskbaserat tillvägagångssätt, på ett oberoende sätt granska och ge objektiv försäkran om att alla verksamheter och enheter hos en utgivare av tillgångsanknutna token, inbegripet användningen av tredjepartsenheter, följer utgivarens policyer och förfaranden och uppfyller externa lagstadgade krav.
146. Internrevisionsfunktionen bör inte vara delaktig i utformningen, urvalet, fastställandet eller genomförandet av specifika policyer, mekanismer, förfaranden och riskgränser för intern kontroll. Detta bör dock inte hindra ledningsorganet i dess ledningsfunktion från att begära in synpunkter från internrevisionsfunktionen i frågor som rör risker, intern kontroll och efterlevnad av tillämpliga regler.
147. Internrevisionsfunktionen bör bedöma om ramen för intern kontroll för utgivaren av tillgångsanknutna token enligt avdelning V är både ändamålsenlig och effektiv. Internrevisionsfunktionen bör särskilt bedöma

- a. lämpligheten hos styrningsramen för utgivaren av tillgångsanknutna token,
 - b. huruvida befintliga policyer och förfaranden fortfarande är lämpliga och överensstämmer med krav enligt lagar och andra författningar samt med riskstrategin och riskaptiten för utgivaren av tillgångsanknutna token,
 - c. att förfarandena är förenliga med tillämpliga lagar och förordningar och med ledningsorganets beslut,
 - d. huruvida förfarandena genomförs på ett korrekt och ändamålsenligt sätt (t.ex. efterlevnad i samband med transaktioner och den faktiska risknivå som föreligger),
 - e. lämpligheten, kvaliteten och ändamålsenligheten avseende de kontroller som utförs och den rapportering som görs av affärsenheterna (första försvarslinjen) samt av funktionerna för riskhantering och regelefterlevnad.
148. Internrevisionsfunktionen bör särskilt kontrollera integriteten hos de processer som säkerställer tillförlitligheten hos de metoder och tekniker för riskkvantifiering som utgivaren av tillgångsanknutna token använder, inbegripet modeller. Den bör också utvärdera kvaliteten på och användningen av verktyg för identifiering och bedömning av kvalitativa risker och de riskreducerande åtgärder som vidtagits.
149. Internrevisionsfunktionen bör granska lämpligheten i processerna för utarbetande av vitböcker, deras godkännande och processerna för hur tillgångsanknutna token erbjuds allmänheten.
150. Internrevisionsfunktionen bör ha obehindrad tillgång till alla register, dokument, uppgifter och byggnader för utgivaren av tillgångsanknutna token. Detta bör innefatta tillgång till förvaltningsinformationssystem och protokoll från alla kommittéer och beslutsfattande organ.
151. Internrevisionsfunktionen bör följa nationella och internationella yrkesstandarder. Ett exempel på sådana yrkesstandarder är de normer som föreskrivs av Institute of Internal Auditors.
152. Internrevisionsarbetet bör utföras regelbundet enligt en revisionsplan och ett detaljerat revisionsprogram som utgår från en riskbaserad metod.
153. En internrevisionsplan bör utarbetas minst en gång per år på grundval av de årliga målen för internrevisionskontroll. Internrevisionsplanen bör godkännas av ledningsorganet.
154. Alla revisionsrekommendationer bör bli föremål för ett formellt uppföljningsförfarande på lämplig ledningsnivå, meddelas ledningsorganet för utgivaren av tillgångsanknutna token och göras tillgängliga för den behöriga myndigheten för att man ska kunna säkerställa och rapportera om deras effektiva och snabba åtgärdande.

Avdelning VI – Hantering av driftskontinuitet

155. Utan att det påverkar tillämpningen av de tillämpliga kraven enligt DORA-förordningen bör utgivare av tillgångsanknutna token, som en del av genomförandet av sin kontinuitetspolicy och sina kontinuitetsplaner som upprättats i enlighet med artikel 34.9 i förordning (EU) 2023/1114, upprätta sunda kontinuitets- och åtgärds- och återhämtningsplaner för att säkerställa sin förmåga att bedriva löpande verksamhet, hantera incidenter som skulle kunna störa tillhandahållandet av kritisk verksamhet i linje med utgivarens riskaptit och tolerans för avbrott, och för att begränsa förluster och avbrott i tillhandahållandet av tjänster i händelse av allvarliga avbrott i verksamheten. Utgivare av tillgångsanknutna token kan inrätta en särskild oberoende kontinuitetsfunktion med beaktande av de proportionalitetskriterier som anges i avdelning I.
156. En utgivare av tillgångsanknutna token förlitar sig på flera kritiska resurser (t.ex. it-system, inklusive molntjänster, kommunikationssystem, kärnpersonal och byggnader). Syftet med kontinuitetshanteringen är att minska de operativa, finansiella, rättsliga, anseendemässiga och andra väsentliga konsekvenserna som en katastrof eller ett större avbrott får för dessa resurser och därmed förbundna avbrott i utgivarens normala affärsförfaranden. Andra riskhanteringsåtgärder kan vara avsedda att minska sannolikheten för sådana incidenter eller överföra deras ekonomiska effekter till tredje parter (t.ex. genom försäkringar).
157. För att upprätta en sund plan för kontinuitetshantering bör värdepappersföretaget noggrant analysera riskfaktorer och sin exponering för allvarliga avbrott i verksamheten samt (kvantitativt och kvalitativt) bedöma de potentiella effekterna av sådana avbrott med hjälp av interna och/eller externa data samt scenarioanalyser. Denna analys bör testa utgivarens förmåga att tillhandahålla kritisk verksamhet vid avbrott och bör omfatta alla affärsområden och interna enheter, inbegripet riskhanteringsfunktionen eller riskhanteringsförfarandena, samt bör ta hänsyn till deras inbördes beroende. Analysresultaten bör bidra till att fastställa prioriteringar och mål för utgivare av tillgångsanknutna token.
158. På grundval av ovanstående analys bör en utgivare av tillgångsanknutna token införa följande:
- a. Beredskaps- och kontinuitetsplaner som säkerställer att utgivaren av tillgångsanknutna token reagerar på nödsituationer på lämpligt sätt och kan tillhandahålla kritisk verksamhet och bevara väsentliga data om det uppstår störningar i dess normala affärsförfaranden.
 - b. Återhämtningsplaner för kritiska resurser och kritiska eller viktiga funktioner för att återhämta sig från störningar och göra det möjligt för utgivaren av tillgångsanknutna token att återgå till normala affärsförfaranden inom en lämplig tidsram. Eventuella kvarstående risker till följd av potentiella störningar i verksamheten bör vara förenliga med utgivarens riskbenägenhet.

- c. För annan verksamhet, eller där kontinuiteten för kritiska väsentliga funktioner är omöjlig att säkerställa, bör utgivare av tillgångsanknutna token ha förfaranden för snabbt återställande av data och funktioner och ett snabbt återupptagande av verksamheten.
159. Beredskapsplaner, kontinuitetsplaner och återhämtningsplaner bör dokumenteras och genomföras noggrant. Dokumentationen bör finnas tillgänglig inom affärsområdena, de interna enheterna och riskhanteringsfunktionen för den personal som ansvarar för riskhanteringsförfaranden, och bör finnas bevarad i system som är fysiskt åtskilda och lättillgängliga i händelse av oförutsedda situationer. Lämplig utbildning på detta område bör tillhandahållas. Planerna bör testas och uppdateras regelbundet. Problem eller brister som konstateras när dessa tester genomförs bör dokumenteras och analyseras, och planerna bör ses över i enlighet med detta.

Kapitel VII –Transparens

160. Strategier, policyer och förfaranden bör kommuniceras till all relevant personal för utgivaren av tillgångsanknutna transaktioner. Personalen bör förstå och följa de riktlinjer och förfaranden som rör dess uppgifter och ansvar.
161. Ledningsorganet bör därför på ett tydligt och konsekvent sätt informera och uppdatera den berörda personalen om utgivarens strategier och riktlinjer, åtminstone till den nivå som krävs för att de ska kunna utföra sina särskilda uppgifter. Detta kan ske genom skriftliga riktlinjer, handböcker eller på annat sätt.