EBA/GL/2017/05

11/09/2017

Riktlinjer

Riktlinjer om IKT-riskbedömning inom ramen för översyns- och utvärderingsprocessen (ÖUP)

1. Efterlevnads- och rapporteringsskyldigheter

Riktlinjernas status

1. Detta dokument innehåller riktlinjer som har utfärdats enligt artikel 16 i förordning (EU) nr 1093/2010[1]. I enlighet med artikel 16.3 i förordning (EU) nr 1093/2010 måste behöriga myndigheter och finansinstituten med alla tillgängliga medel försöka följa riktlinjerna.

2. Avriktlinjerframgår Europeiska bankmyndighetens (EBA) syn på lämplig tillsynspraxis inom det europeiska systemet för finansiell tillsyn eller på hur unionslagstiftningen ska tillämpas inom ett särskilt område. Behöriga myndigheter enligt definitionen i artikel 4.2 i förordning (EU) nr 1093/2010 som berörs av riktlinjerna ska 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 finansinstitut.

Rapporteringskrav

3. Enligt artikel 16.3 i förordning (EU) nr 1093/2010 måste de behöriga myndigheterna meddela EBA om de följer eller avser att följa dessa riktlinjer, alternativt ange skälen till att de inte gör det, senast den 13.11.2017. Om någon sådan anmälan inte inkommer inom denna tidsfrist kommer EBA att anse att de behöriga myndigheterna inte följer riktlinjerna. Anmälningar ska lämnas på det formulär som tillhandahålls på EBA:s webbplats till compliance@eba.europa.eu med hänvisningen ”EBA/GL/2017/05”. Anmälningar ska inges av personer som har befogenhet att rapportera om hur reglerna efterlevs på de behöriga myndigheternas 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).

2. Syfte, tillämpningsområde och definitioner

Syfte och tillämpningsområde

5. Dessa riktlinjer har utarbetats i enlighet med artikel 107.3 i direktiv 2013/36/EU[2] och har som syfte att säkerställa samstämmiga tillsynsmetoder vid riskbedömning av informations- och kommunikationsteknik (IKT) inom ramen för den översyns- och utvärderingsprocess (ÖUP) som avses i artikel 97 i direktiv 2013/36/EU, och som specificeras ytterligare i EBA:s riktlinjer om gemensamma förfaranden och metoder för översyns- och utvärderingsprocessen (ÖUP)[3]. I dessa riktlinjer specificeras de bedömningskriterier som behöriga myndigheter ska tillämpa vid tillsynsbedömning av institutens styrning och strategi avseende IKT, liksom vid tillsynsbedömning av institutens IKT-riskexponeringar och riskkontroller. Dessa riktlinjer utgör en integrerad del av EBA:s ÖUP-riktlinjer.

6. Behöriga myndigheter ska tillämpa dessa riktlinjer i överensstämmelse med tillämpningen av ÖUP såsom specificeras i EBA:s ÖUP-riktlinjer och i enlighet med modellen för minsta insats och de proportionalitetskrav som fastställs däri.

Adressater

7. Dessa riktlinjer vänder sig till de behöriga myndigheter som avses i artikel 4.2 i i förordning (EU) nr 1093/2010.

Definitioner

8. Om inget annat anges har de termer som används och definieras i direktiv 2013/36/EG, förordning (EU) nr 575/2013 och definitionerna från EBA:s ÖUP-riktlinjer samma innebörd i dessa riktlinjer. I riktlinjerna gäller dessutom följande definitioner:

IKT-system	IKT som upprättats som del av en mekanism eller ett sammanlänkat nätverk som stödjer ett instituts verksamhet.
IKT-tjänster	Tjänster som tillhandahålls av IKT-system till en eller flera interna eller externa användare. Detta omfattar till exempel

[2] Europaparlamentets och rådets direktiv 2013/36/EU av den 26 juni 2013 om behörighet att utöva verksamhet i kreditinstitut och om tillsyn av kreditinstitut och värdepappersföretag, om ändring av direktiv 2002/87/EG och om upphävande av direktiv 2006/48/EG och 2006/49/EG (1) – EUT L 176, 27.6.2013, s. 338.

[3] EBA/GL/2014/13

	ingivande av data, lagring av data, behandling av data och rapporteringstjänster, men även övervakning och tjänster för verksamhets- och beslutsstöd.
IKT-risk med avseende på tillgänglighet och kontinuitet	Risken att prestanda och tillgänglighet i IKT-system och uppgifter påverkas negativt, inbegripet bristande återställning av institutets tjänster i rätt tid, beroende på att hårdvaru- eller programvarukomponenter är ur funktion, på brister i förvaltningen av IKT-systemet eller på någon annan händelse såsom specificeras ytterligare i bilagan.
IKT-säkerhetsrisk	Risken för obehörig åtkomst till IKT-system och IKT-data inifrån eller utifrån institutet (t.ex. genom cyber-attacker), såsom specificeras ytterligare i bilagan.
Risk förknippad med IKT-ändringar	Den risk som uppstår när institutet är oförmöget att hantera ändringar i IKT-system i rätt tid och på ett kontrollerat sätt, i synnerhet avseende stora och komplexa programförändringar, såsom specificeras ytterligare i bilagan.
IKT-dataintegritetsrisk	Risken att uppgifter som lagras och bearbetas av IKT-system är ofullständiga, felaktiga eller inte är samstämmiga över olika IKT-system, till exempel till följd av bristfälliga IKT-kontroller eller avsaknad av sådana kontroller under de olika faserna av uppgifternas livscykel (t.ex. utformning av datastruktur, upprättande av datamodell och/eller datalexikon, verifiering av indata, kontroll av datautvinning, överföring och bearbetning, inbegripet erhållna utgående data), vilket försämrar möjligheterna för ett institut att tillhandahålla tjänster samt ledningsinformation, information om riskhantering och finansiell information i rätt tid och på ett korrekt sätt, såsom specificeras ytterligare i bilagan.
IKT-risk vid uppdragsavtal	Risken att anlitandet av en tredje part eller en annan enhet inom gruppen (gruppinterna uppdragsavtal), för att tillhandahålla IKT-system eller därmed sammanhängande tjänster, har negativ påverkan på institutets resultat och riskhantering, såsom specificeras ytterligare i bilagan.

3. Genomförande

Tillämpningsdatum

9. Dessa riktlinjer gäller från och med den 1 januari 2018.

4. Krav på IKT-riskbedömningen

Kapitel 1 – Allmänna bestämmelser

10. Behöriga myndigheter ska genomföra bedömningen av IKT-risken och strukturen på den interna styrningen och IKT-strategin som en del av ÖUP-processen med iakttagande av modellen för minsta insats och proportionalitetskriterierna såsom de specificeras i kapitel 2 i EBA:s ÖUP-riktlinjer. Detta innebär i synnerhet att

    a. frekvensen för IKT-riskbedömningen beror på modellen för minsta insats i överensstämmelse med den ÖUP-kategori som ett institut tillhör och dess särskilda tillsynsprogram, och att

    b. IKT-bedömningens djup, detaljrikedom och intensitet ska vara proportionerlig till institutets storlek, struktur och operativa miljö såväl som dess verksamhets natur, omfattning och komplexitet.

11. Proportionalitetsprincipen är genomgående tillämplig i dessa riktlinjer när det gäller tillsynsinsatsens och dialogens omfattning, frekvens och intensitet, och när det gäller förväntningarna på de standarder som institutet ska uppfylla.

12. Behöriga myndigheter kan förlita sig på och beakta det arbete som redan utförts av institutet eller den behöriga myndigheten inom ramen för bedömningar av andra risker eller ÖUP-element för att få en uppdaterad bedömning. Särskilt vid genomförande av bedömningar som specificeras i dessa riktlinjer ska de behöriga myndigheterna välja den tillsynsmetod och det tillvägagångssätt som är lämpligast och mest proportionerligt för institutet, och de behöriga myndigheterna ska använda befintlig och tillgänglig dokumentation (t.ex. relevanta rapporter och andra handlingar, möten med ledningen och riskkontrollfunktioner, resultat från inspektioner på plats) som ska tjäna som underlag för de behöriga myndigheternas bedömning.

13. Behöriga myndigheter ska sammanfatta resultaten från sina bedömningar av kriterierna som specificeras i dessa riktlinjer, och använda dem för sina slutsatser vid bedömningen av de ÖUP-element som specificeras i EBA:s ÖUP-riktlinjer.

14. I synnerhet ska den bedömning av styrningen och IKT-strategin som genomförs i enlighet med kapitel 2 i dessa riktlinjer tjäna som underlag för sammanfattningen av resultaten av bedömningen av den interna styrningen och de institutionsomfattande ÖUP-kontrollelementen, såsom specificeras i kapitel 5 i EBA:s ÖUP-riktlinjer och reflekteras i respektive betygsättning av ÖUP-elementet. Vidare bör de behöriga myndigheterna beakta att all väsentlig negativ påverkan från IKT-strategibedömningen på institutets affärsstrategi, eller farhågor om att institutet kanske inte har tillräckliga IKT-resurser och IKT-kapacitet för att genomföra och stödja viktiga planerade strategiska förändringar, ska tjäna som underlag för analysen av affärsmodellen i enlighet med kapitel 4 i EBA:s ÖUP-riktlinjer.

15. Resultatet från bedömningen av IKT-risken, såsom den specificeras i kapitel 3 i dessa riktlinjer, ska tjäna som underlag för bedömningen av operativ risk och ska anses tjäna som underlag för relevant betygsättning såsom specificeras i kapitel 6.4 i EBA:s ÖUP-riktlinjer.

16. Det ska observeras att medan behöriga myndigheter i allmänhet ska bedöma underkategorier av risker som en del av huvudkategorierna (dvs. IKT-risken ska bedömas som en del av operativ risk), får behöriga myndigheter anse vissa underkategorier vara väsentliga och även bedöma sådana underkategorier på individuell basis. Om den behöriga myndigheten mot denna bakgrund skulle identifiera IKT-risken som en väsentlig risk, tillhandahålls även en betygstabell (tabell 1) i dessa riktlinjer som ska användas för en självständig betygsättning av IKT-risk som underkategori och som följer det övergripande tillvägagångssättet vid betygsättning av kapitalrisker i EBA:s ÖUP-riktlinjer.

17. För att få en uppfattning om huruvida IKT-risker kan anses vara väsentliga och således möjligheten att IKT-risker bedöms och betygsätts som en individuell underkategori av operativ risk får behöriga myndigheter använda de kriterier som fastställs i avsnitt 6.1 i EBA:s ÖUP-riktlinjer.

18. De behöriga myndigheterna ska i förekommande fall beakta den icke-uttömmande förteckningen över underkategorier och riskscenarier för IKT-risker som anges i bilagan, och observera att fokus i bilagan ligger på IKT-risker som kan medföra allvarliga förluster. Behöriga myndigheter kan utesluta några av de IKT-risker som omfattas av klassificeringen om de inte är relevanta för deras bedömning. Instituten förväntas bibehålla sina egna riskklassificeringar i stället för att använda den IKT-riskklassificering som anges i bilagan.

19. Om dessa riktlinjer tillämpas med avseende på gränsöverskridande bankgrupper och deras enheter, och om ett tillsynskollegium har inrättats, bör de behöriga myndigheterna, inom ramen för deras samarbete avseende ÖUP-bedömningen i enlighet med avsnitt 11.1 i EBA:s ÖUP-riktlinjer, i största möjliga utsträckning samordna den exakta och detaljerade omfattningen av varje informationspost på ett konsekvent sätt för alla gruppenheter.

Kapitel 2 – Bedömning av institutens styrning och IKT-strategi

2.1 Allmänna principer

20. Behöriga myndigheter ska bedöma huruvida institutets allmänna styrning och ramverk för intern kontroll på ett vederbörligt sätt omfattar IKT-systemen och därmed relaterade risker och om ledningsorganet hanterar dessa aspekter på ett lämpligt sätt, eftersom IKT är en integrerad del av ett instituts funktion.

21. Vid denna bedömning ska de behöriga myndigheterna hänvisa till kraven och standarderna för god intern styrning och åtgärder för riskkontroll såsom specificeras i EBA:s riktlinjer för intern styrning (GL 44)[4] och till internationell vägledning på detta område i den utsträckning de är tillämpliga med tanke på IKT-systemens särdrag och risker.

22. Bedömningen i detta kapitel omfattar inte de särskilda delar av IKT-systems styrning, riskhantering och kontroller vars fokus ligger på att hantera särskilda IKT-risker som behandlas i kapitel 3 i dessa riktlinjer, utan fokuserar på följande områden:

    a. IKT-strategi – huruvida institutet har en IKT-strategi som omfattas av lämplig styrning och som överensstämmer med institutets affärsstrategi.

    b. Övergripande intern styrning – huruvida institutets övergripande interna styrningsåtgärder är tillräckliga i förhållande till institutets IKT-system.

    c. IKT-risk inom ramen för institutets riskhantering – huruvida institutets riskhantering och ramverk för intern kontroll säkerställer tillräckligt skydd för institutets IKT-system.

23. Led a i punkt 22, som tillhandahåller information om delarna i institutets styrning, ska huvudsakligen ingå i bedömningen av den affärsmodell som avses i kapitel 4 i EBA:s ÖUP-riktlinjer. Leden b och c kompletterar ytterligare bedömningen av ämnen som omfattas av kapitel 5 i EBA:s ÖUP-riktlinjer, och den bedömning som beskrivs i dessa riktlinjer ska ingå i respektive bedömning enligt kapitel 5 i EBA:s ÖUP-riktlinjer.

24. Resultatet av denna bedömning ska, i förekommande fall, tjäna som underlag för bedömningen av riskhanteringen och kontrollerna i kapitel 3 i dessa riktlinjer.

2.2 IKT-strategi

25. I detta avsnitt ska de behöriga myndigheterna bedöma huruvida institutet har infört en IKT-strategi som är föremål för tillräcklig övervakning från institutets ledningsorgan och som är förenlig med

[4] EBA:s riktlinjer för intern styrning, GL 44, 27 september 2011.

affärsstrategin, i synnerhet när det gäller att hålla IKT-systemen uppdaterade och genomföra viktiga och komplexa IKT-förändringar, samt att den stödjer institutets affärsmodell.

2.2.1 Utveckling av IKT-strategin och dess lämplighet

26. Behöriga myndigheter ska bedöma huruvida institutet har ett befintligt ramverk för att förbereda och utveckla IKT-strategin, och som är proportionerligt i förhållande till IKT-verksamhetens karaktär, omfattning och komplexitet. Vid denna bedömning ska de behöriga myndigheterna beakta följande:

    a. Om verkställande ledningen[5] för affärsområdet/affärsområdena är tillräckligt delaktig i framtagandet av institutets strategiska IKT-prioriteringar och att verkställande ledningen för IKT-funktionen i sin tur har kännedom om utvecklingen, utformningen och införandet av väsentliga affärsstrategier och initiativ, för att säkerställa fortsatt anpassning mellan IKT-system, IKT-tjänster och IKT-funktionen (dvs. de personer som är ansvariga för ledning och utbyggnad av dessa system och tjänster) samt institutets affärsstrategi, liksom att IKT uppdateras på ett effektivt sätt.

    b. Om IKT-strategin är dokumenterad och stödjs av konkreta genomförandeplaner, i synnerhet med avseende på viktiga milstolpar och resursplanering (inbegripet finansiella resurser och personalresurser) för att säkerställa att de är realistiska och möjliggör leverans av IKT-strategin.

    c. Om institutet regelbundet uppdaterar sin IKT-strategi, särskilt när det ändrar affärsstrategi, för att säkerställa fortsatt överensstämmelse mellan IKT och verksamhetsmål, planer och aktiviteter på medellång till lång sikt.

    d. Om institutets ledningsorgan godkänner IKT-strategin och genomförandeplanerna och övervakar dess genomförande.

2.2.2 Genomförande av IKT-strategin

27. Om institutets IKT-strategi kräver att det genomförs viktiga och komplexa IKT-ändringar, eller ändringar som medför väsentlig påverkan på institutets affärsmodell, ska de behöriga myndigheterna bedöma huruvida institutets kontrollramverk är lämpligt med hänsyn till dess storlek, dess IKT-aktiviteter samt i vilken omfattning det krävs förändringar i verksamheten för att stödja ett effektivt genomförande av institutets IKT-strategi. I samband med denna bedömning ska de behöriga myndigheterna beakta huruvida kontrollsystemet

    a. omfattar styrningsprocesser (t.ex. övervakning av genomförande och budget samt rapportering) och relevanta organ (t.ex. ett projektledningskontor, en IKT-styrgrupp eller liknande) för att effektivt kunna stödja genomförandet av de strategiska IKT-programmen,

    b. omfattar definition och tilldelning av roller och ansvarsområden för genomförandet av de strategiska IKT-programmen, med särskilt beaktande av de erfarenheter som viktiga intressenter har avseende organisation, styrning och övervakning av viktiga och komplexa

[5] Verkställande ledning och ledningsorgan såsom de definieras i direktiv 2013/36/EU av den 26 juni 2013 i artikel 3.7 om ”ledningsorgan” och i artikel 3.9 om ”verkställande ledning”.

IKT-förändringar och hanteringen av den mer vidsträckta organisatoriska och mänskliga påverkan (t.ex. hantering av förändringsmotstånd, utbildning, kommunikation),

c. innebär att de oberoende kontrollfunktionerna och funktionen för internrevision används för att säkerställa att de risker som genomförandet av IKT-strategin medför har identifierats, bedömts och minskats på ett effektivt sätt och att det styrningsramverk som införts för att genomföra IKT-strategin är effektivt, och

d. innehåller en planeringsprocess och en översyn av denna process som är flexibla när det gäller att reagera på viktiga frågor som identifierats (t.ex. problem eller förseningar i genomförandet) eller den externa utvecklingen (t.ex. viktiga förändringar i affärsmiljön, tekniska frågor eller innovationer) för att säkerställa att den strategiska genomförandeplanen anpassas i tid.

2.3 Övergripande intern styrning

28. I enlighet med kapitel 5 i EBA:s ÖUP-riktlinjer ska de behöriga myndigheterna bedöma om institutet har en lämplig och transparent bolagsstruktur som är ”lämplig för ändamålet”, och om institutet har infört lämpliga styrningsarrangemang. Denna bedömning ska, med särskilt beaktande av IKT-systemen och i överensstämmelse med EBA:s riktlinjer för intern styrning, innefatta en bedömning av huruvida institutet har

    a. en stabil och transparent organisationsstruktur med en tydlig ansvarsfördelning vad gäller IKT, bland annat för ledningsorganet och dess kommittéer, och att de personer som ansvarar för IKT (t.ex. IKT-chefen [CIO], operativa chefen [COO] eller liknande roll) har lämplig indirekt eller direkt tillgång till ledningsorganet, för att säkerställa att viktig information eller viktiga frågor som har samband med IKT rapporteras, diskuteras och avgörs på ett adekvat sätt på ledningsnivå, liksom

    b. ett ledningsorgan som är insatt i och hanterar de risker som är förknippade med IKT.

29. Enligt avsnitt 5.2 i EBA:s ÖUP-riktlinjer ska de behöriga myndigheterna bedöma huruvida institutets IKT-policy och strategi för uppdragsavtal, i förekommande fall, beaktar hur IKT-uppdragsavtal påverkar institutets verksamhet och affärsmodell.

2.4 IKT-risk inom ramen för institutets riskhantering

30. Vid bedömningen av institutets institutomfattande riskhantering och interna kontroller, såsom föreskrivs i kapitel 5 i EBA:s ÖUP-riktlinjer, ska de behöriga myndigheterna överväga huruvida institutets riskhantering och ramverk för intern kontroll säkerställer tillräckligt skydd av institutets IKT-system på ett sätt som står i proportion till institutets storlek och verksamhet och dess IKT-riskprofil såsom den definieras i kapitel 3. De behöriga myndigheterna ska särskilt fastställa huruvida

    a. riskaptiten och IKU omfattar IKT-riskerna som en del av den mer övergripande kategorin för operativa risker, för framtagandet av den övergripande riskstrategin och fastställande av internt kapital, och huruvida

b. IKT-riskerna omfattas av den institutomfattande riskhanteringen och ramverken för intern kontroll.

31. Behöriga myndigheter ska genomföra bedömningen enligt led a ovan med beaktande av både förväntade och ogynnsamma scenarier, t.ex. scenarier som omfattas av stresstester för institutet eller från tillsynsmyndigheten.

32. Särskilt med avseende på led b ska de behöriga myndigheterna bedöma huruvida funktionerna för oberoende kontroll och internrevision, såsom föreskrivs i punkterna 104 a, 104 d, 105 a och 105 c i EBA:s ÖUP-riktlinjer, är lämpliga för att säkerställa en tillräcklig grad av oberoende mellan IKT och kontroll- och revisionsfunktionerna, med hänsyn till institutets storlek och IKT-riskprofil.

2.5 Resultatsammanfattning

33. Dessa resultat ska återspeglas i resultatsammanfattningen enligt kapitel 5 i EBA:s ÖUP-riktlinjer och ska vara del av betygsättningen i enlighet med övervägandena i tabell 3 i EBA:s ÖUP-riktlinjer.

34. Vid bedömningen av IKT-strategin ska följande punkter beaktas vid genomförandet av ovanstående bedömning:

a. Om de behöriga myndigheterna drar slutsatsen att institutets styrningsramverk är olämplig för att utveckla och genomföra dess IKT-strategi enligt 2.2 ska detta tjäna som underlag för bedömningen av institutets interna styrning i kapitel 5 i EBA:s ÖUP-riktlinjer enligt punkt 87 a.

b. Om de behöriga myndigheterna vid ovanstående bedömning enligt 2.2 drar slutsatsen att det finns en betydande diskrepans mellan IKT-strategin och affärsstrategin som väsentligen skulle kunna påverka institutets långsiktiga affärsmål och/eller finansiella mål, institutets hållbarhet och/eller affärsmodell, eller institutets affärsområden som har fastställts som mest väsentliga enligt punkt 62 a i EBA:s ÖUP-riktlinjer, ska detta tjäna som underlag för affärsmodellsbedömningen enligt punkt 70 b och 70 c i kapitel 4 i nämnda riktlinjer.

c. Om de behöriga myndigheterna vid ovanstående bedömning enligt 2.2 drar slutsatsen att institutet eventuellt inte har tillräckliga IKT-resurser och tillräcklig IKT-kapacitet för att genomföra och stödja viktiga planerade strategiska förändringar ska detta tjäna som underlag för affärsmodellsbedömningen enligt punkt 70 b i kapitel 4 i EBA:s ÖUP-riktlinjer.

Kapitel 3 – Bedömning av institutens exponering för och kontroll av IKT-risker

3.1 Allmänna överväganden

35. Behöriga myndigheter ska bedöma huruvida institutet på ett lämpligt sätt har identifierat, bedömt och minskat sina IKT-risker. Denna process ska vara del av det operativa riskhanteringsramverket och överensstämma med det tillvägagångssätt som är tillämpligt på operativa risker.

36. Behöriga myndigheter ska först identifiera de väsentliga inneboende IKT-risker för vilka institutet är eller kan bli exponerat, följt av en bedömning av effektiviteten i institutets ramverk för hantering av IKT-risker samt förfaranden och kontroller för att minska dessa risker. Resultatet av bedömningen ska avspeglas i en resultatsammanfattning som upptas i betyget för operativ risk i ÖUP-riktlinjerna. När IKT-risken anses vara väsentlig och de behöriga myndigheterna vill sätta ett enskilt betyg ska tabell 1 användas för att betygsätta en underordnad risk till den operativa risken.

37. I samband med bedömningen enligt detta kapitel ska de behöriga myndigheterna använda alla tillgängliga informationskällor som fastställs i punkt 127 i kapitel 6 i EBA:s ÖUP-riktlinjer, t.ex. institutets riskhanteringsverksamhet, rapportering och resultat som grund för fastställandet av deras prioriteringar med avseende på tillsynsmyndighetens bedömning. Behöriga myndigheter ska även använda andra informationskällor för att göra denna bedömning, inbegripet följande i tillämpliga fall:

    a. Självbedömningar av IKT-risker och kontroller (om detta föreskrivs i IKU-informationen).
    b. Ledningsinformation som rör IKT-risker som ingetts till institutets ledningsorgan, t.ex. periodisk IKT-rapportering och rapportering som grundas på enskilda incidenter (inbegripet i databasen över operativa förluster), uppgifter om exponering för IKT-risker från institutets riskhanteringsfunktion.
    c. IKT-relaterade interna och externa granskningsresultat som rapporterats till institutets revisionskommitté.

3.2 Identifiering av väsentliga IKT-risker

38. Behöriga myndigheter ska identifiera de väsentliga IKT-risker som institutet är eller kan bli exponerat för genom att följa stegen nedan.

3.2.1 Granskning av institutets IKT-riskprofil

39. Vid granskning av institutets IKT-riskprofil ska de behöriga myndigheterna beakta all relevant information om institutets IKT-riskexponering, inbegripet information enligt punkt 37 och de väsentliga brister och svagheter som identifierats i IKT-organisationen liksom institutomfattande kontroller enligt kapitel 2 i dessa riktlinjer, och i förekommande fall granska denna information på ett proportionerligt sätt. Som en del av denna granskning ska de behöriga myndigheterna beakta följande:

a. Möjlig påverkan från en allvarlig störning i institutets IKT-system på det finansiella systemet, antingen på nationell eller på internationell nivå.
b. Huruvida institutet kan vara föremål för IKT-säkerhetsrisker eller IKT-risker med avseende på tillgänglighet och kontinuitet på grund av beroendet av internet, införandet av ett stort antal innovativa IKT-lösningar eller andra affärsdistributionskanaler som kan öka sannolikheten att det utsätts för cyber-attacker.
c. Huruvida institutet kan vara mer exponerat för IKT-säkerhetsrisker, IKT-risker med avseende på tillgänglighet och kontinuitet, IKT-dataintegritetsrisker eller risker förknippade med IKT-ändringar på grund av att systemet är komplext (t.ex. till följd av fusioner eller förvärv) eller föråldrat.
d. Huruvida institutet genomför väsentliga ändringar i sitt IKT-system och/eller sina IKT-funktioner (t.ex. till följd av fusioner, förvärv, avyttringar eller utbyte av centrala IKT-system), vilket kan påverka IKT-systemens stabilitet eller korrekta funktion på ett negativt sätt och medföra väsentliga IKT-risker med avseende på tillgänglighet och kontinuitet, IKT-säkerhetsrisker, risker förknippade med IKT-förändringar eller IKT-dataintegritetsrisker.
e. Huruvida institutet har utkontrakterat IKT-tjänster eller IKT-system inom eller utom gruppen som innebär att det kan exponeras för väsentliga IKT-risker på grund av utkontraktering.
f. Huruvida institutet genomför åtgärder för att kraftigt minska IKT-kostnaderna, vilket kan leda till en minskning av nödvändiga IKT-investeringar, resurser och it-expertis och kan öka exponeringen för alla typer av IKT-risker i klassificeringen.
g. Huruvida lokaliseringen av viktiga IKT-verksamheter/datacentraler (t.ex. regioner, länder) kan exponera institutet för naturkatastrofer (t.ex. översvämningar, jordbävningar), politisk instabilitet eller arbetsmarknadskonflikter och civila oroligheter som kan leda till väsentligt ökade IKT-risker med avseende på tillgänglighet och kontinuitet och IKT-säkerhetsrisker.

3.2.2 Granskning av kritiska IKT-system och IKT-tjänster

40. Som ett led i processen med att identifiera de IKT-risker som kan ha en betydande inverkan på institutet ska de behöriga myndigheterna granska dokumentation från institutet och bilda sig en uppfattning om vilka IKT-system och IKT-tjänster som är avgörande för att institutets väsentliga verksamhet ska fungera på ett tillfredsställande sätt samt med avseende på tillgänglighet, kontinuitet och säkerhet.

41. I detta syfte ska de behöriga myndigheterna granska den metod och de processer som institutet tillämpar för att identifiera kritiska IKT-system och IKT-tjänster, med beaktande av att institutet kan anse att vissa IKT-system och IKT-tjänster är avgörande av hänsyn till kontinuiteten och tillgängligheten samt ur säkerhets- (t.ex. förebyggande av bedrägerier) och/eller konfidentialitetsperspektiv (t.ex. konfidentiella uppgifter). De behöriga myndigheterna ska i sin granskning beakta att kritiska IKT-system och IKT-tjänster ska uppfylla minst ett av följande villkor:

a. De ska stödja institutets kärnverksamhet och distributionskanaler (t.ex. uttagsautomater, webbaserade och mobila banktjänster).

b. De ska stödja väsentliga styrningsprocesser och affärsfunktioner, inbegripet riskhantering (t.ex. riskhanterings- och likviditetsförvaltningssystem).

c. De ska omfattas av särskilda rättsliga eller lagstadgade krav (om sådana finns) enligt vilka det föreskrivs ökad tillgänglighet, motståndskraft, konfidentialitet eller säkerhet (t.ex. dataskyddslagstiftning eller eventuella mål för återställningstid [RTO], den maximala tid inom vilken ett system eller en process ska återställas efter en incident, och mål för återställning av data [RPO], den maximala period under vilken data kan förloras vid en incident) för vissa viktiga tjänster (i förekommande fall).

d. De bearbetar eller lagrar konfidentiella eller känsliga uppgifter för vilka obehörig åtkomst väsentligen kan påverka institutets rykte, finansiella resultat eller sundheten och kontinuiteten i verksamheten (t.ex. databaser med känsliga kunduppgifter).

e. De ska tillhandahålla grundläggande funktioner som är väsentliga för att institutet ska kunna fungera korrekt (t.ex. telefon- och anslutningstjänster, IKT och cyber-säkerhetstjänster).

3.2.3 Identifiering av väsentliga IKT-risker för kritiska IKT-system och IKT-tjänster

42. Med beaktande av den granskning av institutets IKT-riskprofil och kritiska IKT-system och IKT-tjänster som genomförts ovan ska de behöriga myndigheterna bilda sig en uppfattning om de väsentliga IKT-risker som, enligt deras bedömning, kan ha en betydande negativ inverkan på institutets kritiska IKT-system och IKT-tjänster.

43. Vid bedömningen av IKT-riskernas möjliga påverkan på ett instituts kritiska IKT-system och IKT-tjänster ska de behöriga myndigheterna beakta följande:

a. Den finansiella påverkan, inbegripet (men inte begränsat till) förlust av medel eller tillgångar, möjlig ersättning till kunder, rättsliga kostnader och kostnader för avhjälpande, skadestånd för avtalsbrott, utebliven vinst.

b. Risken för verksamhetsstörningar, med beaktande av (men inte begränsat till) hur kritiska de finansiella tjänster som påverkas är, det möjliga antal kunder och/eller filialer och anställda som påverkas.

c. Den potentiella påverkan på institutets anseende, beroende på hur kritiska banktjänster eller operativa verksamheter som påverkas är (t.ex. stöld av kunduppgifter), den externa profilen/synligheten för de IKT-system och IKT-tjänster som påverkas (t.ex. mobila eller webbaserade banksystem, försäljningsställe, uttagsautomater eller betalningssystem).

d. Påverkan av lagstiftningen, inbegripet lagstiftarens möjlighet till offentlig kritik, böter eller till och med ändring av tillstånd.

e. Den strategiska påverkan på institutet, till exempel om strategiska produkter eller affärsplaner äventyras eller stjäls.

44. Behöriga myndigheter ska sedan kartlägga de IKT-risker som identifierats och som anses vara väsentliga i följande IKT-riskkategorier för vilka ytterligare riskbeskrivningar och exempel tillhandahålls i bilagan. Behöriga myndigheter ska beakta IKT-riskerna i bilagan som en del av bedömningen enligt kapitel 3:

a. IKT-risk med avseende på tillgänglighet och kontinuitet

b. IKT-säkerhetsrisk
c. Risk förknippad med IKT-ändringar
d. IKT-dataintegritetsrisk
e. IKT-risk vid uppdragsavtal

Kartläggningen ska hjälpa de behöriga myndigheterna att fastställa vilka risker som är väsentliga (i förekommande fall) och ska därför omfattas av en närmare och/eller mer långtgående granskning under följande bedömningssteg.

3.3 Bedömning av kontrollerna för att minska väsentliga IKT-risker

45. För att bedöma institutets resterande IKT-riskexponering ska de behöriga myndigheterna granska hur institutet identifierar, övervakar, bedömer och minskar de väsentliga risker som de behöriga myndigheterna har identifierat vid bedömningen ovan.

46. Mot denna bakgrund ska de behöriga myndigheterna – för de identifierade väsentliga IKT-riskerna – granska tillämpliga

    a. policyer, processer och trösklar för risktolerans för IKT-riskhantering,
    b. ramverk för organisatorisk förvaltning och tillsyn,
    c. omfattning och resultat av den interna revisionen, och
    d. IKT-riskkontroller som är specifika för de väsentliga IKT-risker som har identifierats.

47. Vid bedömningen ska resultatet från analysen av den övergripande riskhanteringen och ramen för intern kontroll som avses i kapitel 5 i EBA:s ÖUP-riktlinjer beaktas, samt institutets styrning och strategi såsom behandlas i kapitel 2 i dessa riktlinjer, eftersom väsentliga brister som identifierats på dessa områden kan påverka institutets förmåga att hantera och minska sin IKT-riskexponering. I förekommande fall ska de behöriga myndigheterna även använda informationskällorna i punkt 37 i dessa riktlinjer.

48. Behöriga myndigheter ska genomföra följande bedömningssteg på ett sätt som står i proportion till karaktär, omfattning och komplexitet vad gäller institutets verksamhet och genom att göra en översyn som står i proportion till institutets riskprofil.

3.3.1 Policyer, förfaranden och trösklar för tolerans för IKT-riskhantering

49. Behöriga myndigheter ska granska huruvida institutet har lämpliga policyer, förfaranden och tröskelvärden för tolerans för de väsentliga IKT-risker som identifierats. Dessa kan vara del av ramverket för hantering av operativ risk eller ett separat dokument. Vid denna bedömning ska de behöriga myndigheterna beakta följande:

    a. Om riskhanteringspolicyn är formaliserad och godkänd av ledningsorganet och innehåller tillräcklig vägledning om institutets IKT-riskaptit och om de huvudsakliga mål som eftersträvas vad gäller IKT-riskhantering och/eller tillämpade tröskelvärden för IKT-risktolerans. Relevant policy för hantering av IKT-risker ska också kommuniceras till alla berörda intressenter.

b. Om den tillämpliga policyn omfattar alla väsentliga element för riskhanteringen av de identifierade väsentliga IKT-riskerna.

c. Om institutet har infört en process och underliggande förfaranden för identifiering (t.ex. självbedömningar av risker och kontroller, analys av riskscenarier) liksom övervakning av de aktuella väsentliga IKT-riskerna.

d. Om institutet rapporterar om hanteringen av IKT-risker och lämnar information i tid till verkställande ledningen och ledningsorganet och gör det möjligt för verkställande ledningen och/eller ledningsorganet att bedöma och övervaka huruvida institutets planer och åtgärder för att reducera IKT-riskerna är förenliga med den godkända riskaptiten och/eller toleransnivåerna (i förekommande fall) och att granska förändringar av väsentliga IKT-risker.

3.3.2 Ram för organisatorisk förvaltning och tillsyn

50. Behöriga myndigheter ska bedöma hur de tillämpliga rollerna och ansvarsområdena för riskhantering är införlivande och integrerade i den interna organisationen för att förvalta och övervaka de väsentliga IKT-risker som identifierats. I detta avseende ska de behöriga myndigheterna bedöma huruvida institutet uppvisar följande:

a. Tydliga roller och ansvarsområden för identifiering, bedömning, övervakning, minskning, rapportering och tillsyn av de aktuella väsentliga IKT-riskerna.

b. Roller och ansvarsområden avseende risk som är tydligt kommunicerade, fördelade och inbyggda i alla relevanta delar (t.ex. affärsområden, it) och att det finns organisationsprocesser, inbegripet roller och ansvarsområden för insamling och sammanställning av riskinformation och rapportering av denna till verkställande ledningen och/eller ledningsorganet.

c. IKT-riskhanteringsåtgärder som vidtas med tillräckliga och i kvalitativt hänseende lämpliga personalresurser och tekniska resurser. För att bedöma trovärdigheten i de tillämpliga planerna för riskreducering ska de behöriga myndigheterna även bedöma huruvida institutet har avsatt tillräckliga finansiella resurser och/eller andra resurser som krävs för deras genomförande.

d. Lämplig uppföljning och lämpliga åtgärder från ledningsorganet vad gäller viktiga resultat från de oberoende kontrollfunktionerna med avseende på risken/riskerna, med beaktande av en möjlig delegering av vissa aspekter till en kommitté, om det finns en sådan.

e. Undantag från tillämpliga IKT-bestämmelser och policyer noteras och är föremål för en dokumenterad granskning och rapportering genom den oberoende kontrollfunktionen med fokus på de relaterade riskerna.

3.3.3 Omfattning och resultat från den interna revisionen

51. Behöriga myndigheter ska överväga huruvida funktionen för internrevision är effektiv vad gäller revisionen av det tillämpliga IKT-riskkontrollramverket, genom att granska huruvida

a. revisionen av riskkontrollramverket görs med den kvalitet, det djup och den frekvens som står i proportion till institutets storlek, verksamhet och IKT-riskprofil,

b. revisionsplanen innefattar revision av de kritiska IKT-risker som institutet identifierat,

c. viktiga resultat från IKT-revisionen, inbegripet överenskomna åtgärder, rapporteras till ledningsorganet, och om

d. resultat från IKT-revisionen, inbegripet överenskomna åtgärder, följs upp och lägesrapporter granskas med regelbundna mellanrum av verkställande ledningen och/eller revisionskommittén.

3.3.4 IKT-riskkontroller som är specifika för de väsentliga IKT-risker som har identifierats

52. För de väsentliga IKT-risker som har identifierats ska de behöriga myndigheterna bedöma huruvida institutet har specifika kontroller för att hantera dessa risker. Följande avsnitt innehåller en icke-uttömmande förteckning över de specifika kontroller som ska övervägas vid bedömning av de väsentliga risker som har identifierats enligt punkt 3.2.3 och som har kartlagts till följande IKT-riskkategorier:

a. IKT-risker med avseende på tillgänglighet och kontinuitet.
b. IKT-säkerhetsrisker.
c. Risker förknippade med IKT-ändringar.
d. IKT-dataintegritetsrisker.
e. IKT-risker vid uppdragsavtal.

(a) Kontroller för att hantera väsentliga IKT-risker med avseende på tillgänglighet och kontinuitet

53. Utöver kraven i EBA:s ÖUP-riktlinjer (punkterna 297–281) ska de behöriga myndigheterna bedöma huruvida institutet har ett lämpligt ramverk för att identifiera, förstå, mäta och minska IKT-risker med avseende på tillgänglighet och kontinuitet.

54. Vid denna bedömning ska de behöriga myndigheterna särskilt beakta huruvida ramverket

a. identifierar de kritiska IKT-processer och de relevanta stödjande IKT-system som ska vara del av resiliens- och kontinuitetsplanerna med följande:

i. En omfattande analys av beroenden mellan de kritiska affärsprocesserna och stödsystemen.

ii. Fastställande av återställningsmål för de stödjande IKT-systemen (t.ex. typiskt fastställda genom verksamheten och/eller bestämmelser vad gäller RTO och RPO).

iii. Lämplig beredskapsplanering för att möjliggöra tillgänglighet, kontinuitet och återställning av kritiska IKT-system och tjänster för att minimera avbrott i institutets verksamhet inom acceptabla gränser.

b. Huruvida ramverket har policyer och standarder för resiliens, kontinuitet och operativa kontroller som omfattar följande:

i. Åtgärder för att undvika att ett enskilt scenario eller en enskild incident eller katastrof påverkar både IKT-produktionssystem och reservsystem.

ii. IKT-backup- och återställningsprocesser för kritisk programvara och data som säkerställer att dessa säkerhetskopior lagras på en säker och tillräckligt avlägsen plats, så att en incident eller katastrof inte kan förstöra eller förvanska dessa kritiska data.

iii. Övervakningssystem så att incidenter som rör tillgänglighet eller kontinuitet kan upptäckas i tid.

iv. En dokumenterad process för hantering och eskalering av incidenter som också tillhandahåller vägledning avseende de olika rollerna och ansvarsområdena för hantering av incidenter och medlemmarna i kriskommittén/kriskommittéerna och beslutskedjan i en nödsituation.

v. Fysiska åtgärder såväl för att skydda institutets kritiska IKT-infrastruktur (t.ex. datacentraler) från miljörisker (t.ex. översvämning och andra naturkatastrofer) och säkerställa en lämplig operativ miljö för IKT-systemen (t.ex. luftkonditionering).

vi. Processer, roller och ansvarsområden för att säkerställa att även utkontrakterade IKT-system och IKT-tjänster omfattas av tillräcklig resiliens och kontinuitetslösningar och planer.

vii. Planering av IKT-prestanda och kapacitet samt övervakningslösningar för kritiska IKT-system och IKT-tjänster med fastställda krav på tillgänglighet, för att upptäcka viktiga begränsningar i prestanda och kapacitet i rätt tid.

viii. Lösningar för att skydda kritisk internetverksamhet eller kritiska tjänster (t.ex. e-banktjänster), när det är nödvändigt och lämpligt, mot överbelastnings- och andra cyber-attacker från internet i syfte att förhindra eller störa åtkomst till denna verksamhet och dessa tjänster.

c. Huruvida ramverket testar lösningar för tillgänglighet och kontinuitet mot en rad realistiska scenarier, inbegripet cyber-attacker, omställningstester (fail-over) och tester av backup för kritisk programvara och data, som

i. är planerade, formaliserade och dokumenterade, och testresultaten används för att öka effektiviteten i lösningar som avser tillgänglighet och kontinuitet,

ii. innefattar berörda parter och funktioner inom organisationen, såsom hantering av affärsområden, inbegripet arbetsgrupper som är ansvariga för kontinuitets-, incident- och krishantering, samt relevanta externa intressenter i ekosystemet,

iii. ledningsorgan och verkställande ledning är delaktiga i på ett lämpligt sätt (t.ex. som en del av en krishanteringsgrupp), vilka också får information om testresultat.

(b) Kontroller för att hantera väsentliga IKT-säkerhetsrisker

55. Behöriga myndigheter ska bedöma huruvida institutet har ett effektivt ramverk för att identifiera, förstå, mäta och minska IKT-säkerhetsrisker. Vid denna bedömning ska de behöriga myndigheterna i synnerhet ta hänsyn till huruvida ramverket beaktar följande:

a. Klart definierade roller och ansvarsområden avseende

   i. den person/de personer och/eller kommittéer som är ansvariga för den dagliga IKT-säkerhetshanteringen och utarbetandet av de övergripande IKT-säkerhetspolicyerna, med beaktande av det oberoende som de behöver,
   ii. utformning, genomförande, hantering och övervakning av IKT-säkerhetskontroller,
   iii. skydd av kritiska IKT-system och IKT-tjänster, exempelvis genom att anta en process för bedömning av sårbarhet, uppdateringsprocess av programvara, klientskydd (t.ex. antivirusprogram), system för upptäckt av intrång (IDS) och för förhindrande av intrång (IPS),
   iv. övervakning, klassificering och hantering av externa eller interna IKT-säkerhetsincidenter, inbegripet incidenthantering och återupptagande och återställning av IKT-system och IKT-tjänster, samt
   v. regelbundna och förebyggande bedömningar av hot för att bibehålla lämpliga säkerhetskontroller.

b. En IKT-säkerhetspolicy som beaktar och, i förekommande fall, följer internationellt erkända IKT-säkerhetsstandarder och IKT-säkerhetsprinciper (t.ex. principen om begränsad behörighet, dvs. en begränsning av åtkomsten till den miniminivå som medger normala funktioner för hantering av åtkomsträttigheter och principen om ”försvar på djupet”, dvs. säkerhetsmekanismer i flera nivåer för att öka systemets säkerhet i sin helhet för utformning av en säkerhetsstruktur).

c. Ett förfarande för att identifiera IKT-system och IKT-tjänster i proportion till säkerhetskraven som återspeglar den potentiella risken för bedrägerier och/eller möjligt missbruk av konfidentiella uppgifter tillsammans med dokumenterade förväntningar på säkerhet som ska följas för dessa identifierade system, tjänster och uppgifter i proportion till institutets risktolerans och med övervakning för ett korrekt genomförande.

d. En dokumenterad process för hantering och eskalering av säkerhetsincidenter som tillhandahåller vägledning avseende de olika rollerna och ansvarsområdena för hantering av incidenter och medlemmarna i kriskommittén/kriskommittéerna och beslutskedjan i en nödsituation.

e. Loggning av användare och administrativa åtgärder för att möjliggöra effektiv övervakning och snabb upptäckt och hantering av otillåten aktivitet, för att bistå vid eller genomföra tekniska undersökningar av säkerhetsincidenter. Institutet ska ha en loggningspolicy som definierar lämpliga typer av loggar som ska tillämpas och deras lagringstid.

f. Medvetandehöjande och informationskampanjer eller initiativ för att informera samtliga nivåer i institutet om säker användning och skydd av institutets IKT-system och de huvudsakliga IKT-säkerhetsriskerna (och andra risker) som de ska vara medvetna om, särskilt vad gäller befintliga och framväxande it-hot (t.ex. datavirus, möjligt internt eller externt missbruk eller attacker, cyber-attacker) och deras roll när det gäller att minska säkerhetsöverträdelserna.

g. Lämpliga fysiska säkerhetsåtgärder (t.ex. kameraövervakningssystem, inbrottslarm, säkerhetsdörrar) för att förhindra otillåten fysisk åtkomst till kritiska och känsliga IKT-system (t.ex. datacentraler).

h. Åtgärder för att skydda IKT-systemen från attacker från internet (dvs. cyber-attacker) eller andra externa nätverk (t.ex. traditionella telefonförbindelser eller förbindelser med betrodda partner). Behöriga myndigheter bör granska huruvida institutets ramverk beaktar följande:

   i. En process och lösningar för att bibehålla en fullständig och uppdaterad kartläggning och överblick över alla utåtriktade anslutningspunkter i nätverket (t.ex. webbplatser, internetapplikationer, wifi, fjärråtkomst) genom vilka tredje parter skulle kunna bryta sig in i de interna IKT-systemen.

   ii. Noggrant hanterade och övervakade säkerhetsåtgärder (t.ex. brandväggar, proxyservrar, e-postreläer, antivirus och innehållskontroll) för att säkra inkommande och utgående nätverkstrafik (t.ex. e-post) och de utgående nätverksförbindelser genom vilka tredje parter skulle kunna ta sig in i de interna IKT-systemen.

   iii. Processer och lösningar för att säkra webbplatser och applikationer som kan attackeras direkt från internet och/eller utifrån, vilka kan fungera som ingångspunkt till de interna IKT-systemen. I allmänhet omfattar detta en kombination av erkända säkra utvecklingsmetoder, härdning av IKT-system och metoder för att upptäcka sårbarheter, och/eller införande av ytterligare säkerhetslösningar som till exempel brandväggar för applikationer och/eller system för upptäckt av intrång (IDS) och/eller system för förhindrande av intrång (IPS).

   iv. Periodisk penetrationstestning för att bedöma hur effektiva de genomförda IKT-säkerhetsåtgärderna och processerna är. Dessa tester ska genomföras av anställda och/eller externa experter med nödvändiga kunskaper, med dokumenterade testresultat och slutsatser som rapporteras till verkställande ledningen och/eller ledningsorganet. Vid behov och i förekommande fall ska institutet lära sig från dessa tester var det kan förbättra säkerhetskontrollerna och processerna ytterligare och/eller få bättre försäkran för deras effektivitet.

(c) Kontroller för att hantera risker förknippade med väsentliga IKT-ändringar

56. Behöriga myndigheter ska bedöma huruvida institutet har ett effektivt ramverk för att identifiera, förstå, mäta och minska risker vid IKT-förändringar i proportion till karaktär, omfattning och komplexitet vad gäller institutets verksamhet och dess IKT-riskprofil. Institutets ramverk ska omfatta de risker som är förknippade med utveckling, testning och godkännande av IKT-systemförändringar, inbegripet utveckling och förändringar av programvara, innan de införs i produktionsmiljön, och säkerställa en lämplig förvaltning av IKT-livscykeln. Vid denna bedömning ska de behöriga myndigheterna i synnerhet ta hänsyn till huruvida ramverket beaktar följande:

   a. Dokumenterade processer för hantering och kontroll av ändringar av IKT-systemen (t.ex. konfigurering och uppdateringshantering) och data (t.ex. korrigering av programfel och justering av uppgifter), varigenom tillräcklig IKT-riskhantering säkerställs för viktiga IKT-förändringar som väsentligen kan påverka institutets riskprofil eller riskexponering.

b. Specifikationer avseende den nödvändiga ansvarsuppdelningen under de olika faserna i processen för de IKT-ändringar som genomförs (t.ex. utformning och utveckling av lösningar, testning och godkännande av ny programvara och/eller ändringar, införande i produktionsmiljön, liksom rättning av programfel), med fokus på de genomförda lösningarna och ansvarsuppdelningen för att hantera och kontrollera ändringar i IKT-produktionssystemen och data från IKT-personalen (t.ex. utvecklare, IKT-systemadministratörer, databasadministratörer) eller någon annan part (t.ex. användare, tjänsteleverantörer).

c. Testmiljöer som korrekt avspeglar produktionsmiljöerna.

d. Ett tillgångsregister av befintliga applikationer och IKT-system i produktionsmiljön, liksom i test- och utvecklingsmiljön, vilket innebär att de ändringar som krävs (t.ex. versionsuppdateringar eller uppgraderingar, systemuppdateringar, ändring av konfiguration) kan hanteras, genomföras och övervakas på ett korrekt sätt för de IKT-system som berörs.

e. En process för att övervaka och hantera de använda IKT-systemens livscykel, för att säkerställa att de fortsätter att uppfylla och stödja de faktiska kraven från affärsverksamheten och riskhanteringen och att säkerställa att de IKT-lösningar och IKT-system som används fortfarande stödjs av leverantören, samt att detta åtföljs av lämpliga processer för systemutveckling.

f. Ett kontrollsystem för källkod och lämpliga processer för att hindra otillåtna ändringar i källkoden för internt utvecklad programvara.

g. Ett förfarande för att genomföra en säkerhets- och sårbarhetsgranskning av nya eller väsentligen ändrade IKT-system och programvara innan de tas i bruk och exponeras för eventuella cyber-attacker.

h. En process och lösningar för att förhindra otillåtet eller oavsiktligt utlämnande av konfidentiella uppgifter vid utbyte, arkivering, kassering eller förstörelse av IKT-system.

i. Ett oberoende gransknings- och valideringsförfarande för att minska riskerna för mänskliga misstag vid genomförande av ändringar i IKT-systemen som kan ha väsentliga negativa effekter på institutets tillgänglighet, kontinuitet eller säkerhet (t.ex. viktiga ändringar i brandväggskonfiguration), eller institutets säkerhet (t.ex. ändringar av brandväggarna).

(d) Kontroller för att hantera väsentliga IKT-dataintegritetsrisker

57. Behöriga myndigheter ska bedöma huruvida institutet har ett effektivt ramverk för att identifiera, förstå, mäta och minska IKT-dataintegritetsrisker i proportion till karaktär, omfattning och komplexitet vad gäller institutets verksamhet och dess IKT-riskprofil. Institutets ramverk ska beakta de risker som har samband med bevarandet av integriteten hos de uppgifter som lagras och bearbetas av IKT-systemen. Vid denna bedömning ska de behöriga myndigheterna i synnerhet ta hänsyn till huruvida ramen beaktar följande:

    a. En policy som definierar roller och ansvarsområden för hantering av integriteten hos uppgifterna i IKT-systemen (t.ex. datautvecklare, databehandlare[6], dataförvarare[7] och ägare/förvaltare till data[8]) och som ger vägledning om vilka uppgifter som är avgörande från ett dataintegritetsperspektiv och ska vara föremål för särskilda IKT-kontroller (t.ex. automatiska kontroller för ingångsvalidering, kontroller av dataöverföring, avstämning etc.) eller granskningar (t.ex. kontroll av överensstämmelse med dataarkitektur) under de olika faserna i IKT-datans livscykel.

    b. En dokumenterad dataarkitektur, datamodell och/eller lexikon som validerats av relevanta intressenter från affärsverksamheten och it-verksamheten och som stödjer den nödvändiga samstämmigheten hos uppgifter mellan IKT-systemen och säkerställer att dataarkitekturen, datamodellen och/eller lexikonet överensstämmer med affärs- och riskhanteringsbehoven.

    c. En policy rörande den tillåtna användningen och beroendet av anveckling, särskilt med avseende på identifiering, registrering och dokumentering av viktiga lösningar för anveckling (t.ex. vid bearbetning av viktiga uppgifter) och de förväntade säkerhetsnivåerna för att förhindra otillåtna ändringar, både i själva verktyget och i de uppgifter som lagras där.

    d. Dokumenterade processer för hantering av avvikelser för att lösa identifierade problem rörande IKT-dataintegritet i överensstämmelse med hur kritiska och känsliga de är.

58. För övervakade institut som omfattas av principerna i BCBS 239 om effektiv sammanställning av riskdata och riskrapportering[9] ska de behöriga myndigheterna granska institutets riskanalys av sin egen riskrapportering och förmåga att sammanställa uppgifter i jämförelse med principerna och den dokumentation som tagits fram, med beaktande av tidsfristen för genomförandet och övergångsbestämmelserna i dessa principer.

(e) Kontroller för att hantera väsentliga IKT-risker vid uppdragsavtal

59. Behöriga myndigheter ska bedöma huruvida institutets strategi om uppdragsavtal, i överensstämmelse med kraven i CEBS riktlinjer om uppdragsavtal (2006) samt kravet i punkt 85 d i EBA:s ÖUP-riktlinjer, tillämpas på ett tillfredsställande sätt på IKT-uppdragsavtal, inbegripet uppdragsavtal inom gruppen där

[6] En databehandlare är ansvarig för bearbetning och användning av data.

[7] En dataförvarare är ansvarig för säker förvaring, transport och lagring av data.

[8] En dataförvaltare är ansvarig för hantering av och ändamålsenlighet för dataelement – både vad gäller innehåll och metadata.

[9] Baselkommittén för banktillsyn, Principles for effective risk data aggregation and risk reporting, januari 2013, tillgängliga online på http://www.bis.org/publ/bcbs239.pdf.

IKT-tjänster tillhandahålls inom gruppen. De behöriga myndigheterna ska vid bedömningen av IKT-risker vid uppdragsavtal beakta att dessa risker även kan omfattas som en del av bedömningen av de inneboende operativa riskerna enligt punkt 240 j i EBA:s ÖUP-riktlinjer, för att undvika dubbelarbete eller dubbelräkning.

60. Behöriga myndigheter ska särskilt bedöma huruvida institutet har ett effektivt ramverk för att identifiera, förstå och mäta IKT-risker vid uppdragsavtal, och i synnerhet har kontroller och en kontrollmiljö för att minska risker i samband med väsentliga utkontrakterade IKT-tjänster som är proportionerliga till institutets storlek, verksamhet och IKT-riskprofil, och som omfattar följande:

    a. En bedömning av vilken påverkan som IKT-utkontrakteringen får på institutets riskhantering med avseende på användningen av tjänsteleverantörer (t.ex. leverantörer av molntjänster) och deras tjänster under upphandlingsprocessen som är dokumenterad och beaktas av verkställande ledningen eller ledningsorganet vid beslutet att utkontraktera tjänsten eller inte. Institutet ska granska policyer för IKT-riskhantering och IKT-kontroller och tjänsteleverantörens kontrollmiljö för att säkerställa att de uppfyller institutets interna riskhanteringsmål och riskaptit. Denna granskning ska uppdateras regelbundet under uppdragsavtalets löptid, med beaktande av de utkontrakterade tjänsternas karaktär.

    b. Övervakning av de IKT-risker som de utkontrakterade tjänsterna medför under uppdragsavtalets löptid som en del av institutets riskhantering och som ingår i institutets rapportering om IKT-riskhantering (t.ex. rapportering om kontinuitet och säkerhet).

    c. Övervakning och jämförelse av de erhållna servicenivåerna med de avtalade servicenivåer som ska vara del av uppdragsavtalet eller servicenivåavtalet.

    d. Tillräckligt med personal, resurser och kompetens för att övervaka och hantera IKT-riskerna från de utkontrakterade tjänsterna.

3.4 Resultatsammanfattning och betygsättning

61. Efter bedömningen ovan ska de behöriga myndigheterna bilda sig en uppfattning om institutets IKT-risk. Denna uppfattning ska återges i en resultatsammanfattning som de behöriga myndigheterna ska beakta vid betygsättningen av operativ risk i tabell 6 i EBA:s ÖUP-riktlinjer. Behöriga myndigheter ska grunda sin uppfattning på väsentliga IKT-risker med beaktande av följande överväganden som ska ingå i bedömningen av den operativa risken:

    a. Riskövervägande:

        i. Institutets IKT-riskprofil och riskexponering,
        ii. de identifierade kritiska IKT-systemen och IKT-tjänsterna, liksom
        iii. hur allvarlig IKT-risken är avseende kritiska IKT-system.

    b. Överväganden avseende hantering och kontroll:

        i. Huruvida institutets policy och strategi för IKT-riskhantering är förenliga med dess övergripande strategi och riskaptit.

ii. Huruvida det organisatoriska ramverket för IKT-riskhantering är stabil med tydliga ansvarsområden och en tydlig uppdelning av uppgifter mellan risktagare och riskhanterings- och kontrollfunktioner.
iii. Huruvida mätnings-, övervaknings- och rapporteringssystemen för IKT-risker är lämpliga.
iv. Huruvida kontrollramverken för väsentliga IKT-risker är sunda.

62. Om de behöriga myndigheterna anser att IKT-risken är väsentlig och den behöriga myndigheten beslutar att bedöma och betygsätta denna risk som en underkategori till den operativa risken, anges överväganden för betygsättning av IKT-risken i tabellen nedan (tabell 1).

Tabell 1: Tillsynsöverväganden vid betygsättning av IKT-risk

Riskbetyg	Tillsynsmyndighetens uppfattning	Överväganden för inneboende risk	Överväganden för lämplig hantering och lämpliga kontroller
1	Det finns ingen identifierbar risk för en betydande inverkan på institutets stabilitet till följd av inneboende risknivå och riskhanterings- och kontrollfunktioner.	• De informationskällor som ska beaktas enligt punkt 37 har inte visat någon betydande IKT-riskexponering. • Institutets IKT-riskprofil samt granskningen av de kritiska IKT-systemen och de väsentliga IKT-riskerna för IKT-systemen och IKT-tjänsterna har inte visat några väsentliga IKT-risker.	• Institutets policy och strategi för IKT-risker är förenliga med dess övergripande strategi och riskaptit. • Det organisatoriska ramverket för IKT-risker är stabilt med tydliga ansvarsområden och en tydlig uppdelning av uppgifter mellan risktagare och riskhanterings- och kontrollfunktioner. • Mätnings-, övervaknings- och
2	Det finns en låg risk för betydande inverkan på institutets stabilitet till följd av inneboende risknivå och riskhanterings- och kontrollfunktioner.	• De informationskällor som ska beaktas enligt punkt 37 har inte visat någon betydande IKT-riskexponering. • Institutets IKT-riskprofil samt granskningen av de kritiska IKT-systemen och de väsentliga IKT-riskerna för IKT-systemen och IKT-tjänsterna har visat en begränsad exponering för IKT-risker (dvs. inte mer än 2 av 5 i de fastställda IKT-riskkategorierna).	
3	Det finns en medelhög risk för betydande inverkan på institutets stabilitet till följd av inneboende risknivå	• De informationskällor som ska beaktas enligt punkt 37 har visat tecken på möjlig betydande IKT-riskexponering. • Institutets IKT-riskprofil samt granskningen av de kritiska IKT-	

	och riskhanterings- och kontrollfunktioner.	systemen och de väsentliga IKT-riskerna för IKT-systemen och IKT-tjänsterna har visat en förhöjd exponering för IKT-risker (dvs. 3 eller mer av 5 i de fastställda IKT-riskkategorierna).	rapporteringssystemen för IKT-risker är lämpliga. • Kontrollramen för IKT-risker är sund.
4	Det finns en hög risk för betydande inverkan på institutets stabilitet till följd av inneboende risknivå och riskhanterings- och kontrollfunktioner.	• De informationskällor som ska beaktas enligt punkt 37 har visat ett flertal tecken på väsentlig IKT-riskexponering. • Institutets IKT-riskprofil samt granskningen av de kritiska IKT-systemen och de väsentliga IKT-riskerna för IKT-systemen och IKT-tjänsterna har visat en hög exponering för IKT-risker (dvs. 4 eller 5 av 5 i de fastställda IKT-riskkategorierna).	

Bilaga – Klassificering av IKT-risker

Fem IKT-riskkategorier med en icke-uttömmande förteckning över IKT-risker som potentiellt är mycket allvarliga och/eller med operativa, anseendemässiga eller finansiella konsekvenser

IKT-riskkategorier	IKT-risker (icke-uttömmande[10])	Riskbeskrivning	Exempel
IKT-risker med avseende på tillgänglighet och kontinuitet	Bristande kapacitetshantering	Brist på resurser (t.ex. hårdvara, mjukvara, personal, tjänsteleverantörer) kan leda till en oförmåga att tillhandahålla tjänster för att möta affärsbehov, systemavbrott, försämrad service och/eller operativa fel.	• Kapacitetsbrist kan påverka överföringshastigheten och nätverkets tillgänglighet (internet) för tjänster såsom webbaserade banktjänster. • Brist på personal (intern eller från tredje part) kan medföra systemavbrott och/eller operativa fel.
	IKT-systemfel	Bristande tillgänglighet på grund av fel i hårdvara.	• Fel/brister vid lagring (hårddiskar), servrar eller annan IKT-utrustning, t.ex. beroende på bristande underhåll.
		Bristande tillgänglighet på grund av fel i mjukvara och programfel.	• En oändlig loop i applikationsprogramvaran hindrar utförandet av transaktionen. • Driftsavbrott på grund av fortsatt användning av föråldrade IKT-system och lösningar som inte längre uppfyller de aktuella kraven vad gäller tillgänglighet och motståndskraft och/eller inte längre stödjs av leverantören.
	Bristande planering av IKT-kontinuitet och återställning	Brister i planerad IKT-tillgänglighet och/eller kontinuitetslösningar och/eller återställning (t.ex. reservdatacentral) vid aktivering i samband med en incident.	• Skillnader i konfiguration mellan den primära och sekundära datacentralen kan leda till att reservdatacentralen är oförmöget att tillhandahålla den planerade kontinuiteten för tjänsten.
	Störande och skadliga it-attacker	Attacker med olika syften (t.ex. aktivism, utpressning) som leder till en överbelastning av system och nätverk och förhindrar åtkomst för legitima användare till onlinetjänster.	• Distribuerade överbelastningsattacker (Distributed Denial of Service attacks) utförs genom att ett stort antal datorsystem på internet som kontrolleras av en hackare skickar ett stort antal förfrågningar som

[10] IKT-riskerna är upptagna under den riskkategori som de påverkar mest, men de kan påverka andra riskkategorier.

IKT-riskkategorier	IKT-risker (icke-uttömmande[10])	Riskbeskrivning	Exempel
			förefaller legitima till internettjänster (t.ex. e-banktjänster).
IKT-säkerhetsrisker	Cyber-attacker och andra externa IKT-baserade attacker	Attacker som genomförs från internet eller utomstående nätverk i olika syften (t.ex. bedrägeri, spionage, aktivism/sabotage, cyber-terrorism) med användning av olika metoder (t.ex. social manipulation, försök till intrång genom utnyttjande av svagheter, användning av sabotageprogram) som leder till ett övertagande av kontrollen över interna IKT-system.	Olika typer av attacker: • APT (avancerat ihållande hot) för att ta över kontrollen av interna system eller stjäla information (t.ex. information som hör samman med identitetskapning, kreditkortsinformation). • Sabotageprogram (t.ex. utpressningsprogram) som krypterar data i utpressningssyfte. • Infiltrering av IKT-system med trojaner för att genomföra illvilliga handlingar i systemet på ett dolt sätt. • Utnyttjande av svagheter i IKT-systemet och/eller i (webb)applikationer (t.ex. SQL-injektion ...) för att få åtkomst till interna IKT-system.
		Genomförande av bedrägliga betalningstransaktioner av hackare genom att bryta sig igenom eller kringgå säkerheten vid e-banking och betalningstjänster och/eller genom att attackera och utnyttja säkerhetsbrister i institutets interna betalningssystem.	• Attacker mot betalnings- eller e-banktjänster i syfte att genomföra obehöriga transaktioner. • Upprättande och utskick av bedrägliga betalningstransaktioner inifrån institutets interna betalningssystem (t.ex. bedrägliga Swiftmeddelanden).
		Utförande av bedrägliga värdepapperstransaktioner av hackare genom att bryta sig igenom eller kringgå säkerheten vid e-banktjänster som även ger tillgång till kundens värdepapperskonto.	• ”Pump and dump”-attacker där den som utför attacken får tillgång till kundernas värdepapperskonton genom e-banktjänster och placerar bedrägliga köp- eller säljorder för att påverka marknadspriset och/eller göra vinst på grundval av tidigare upprättade värdepapperspositioner.
		Attacker på kommunikationsförbindelser och konversationer av alla typer eller på IKT-system i syfte att samla in information och/eller begå bedrägerier.	• Avlyssning av oskyddade överföringar av autentiseringsdata i klartext.

IKT-riskkategorier	IKT-risker (icke-uttömmande[10])	Riskbeskrivning	Exempel
	Bristande intern IKT-säkerhet	Obehörig åtkomst till kritiska IKT-system inifrån institutet i olika syften (t.ex. bedrägeri, genomförande och döljande av oseriös handelsverksamhet, datastöld, aktivism/sabotage) genom ett flertal metoder (t.ex. missbruk och/eller utökning av privilegier, identitetskapning, social ingenjörskonst, utnyttjande av svagheter i IKT-systemet, användning av sabotageprogram).	• Installation av keyloggers för att stjäla användar-id och lösenord för att få obehörig åtkomst till konfidentiella uppgifter och/eller begå bedrägerier. • Knäcka/gissa svaga lösenord för att få olaglig eller utökad åtkomst. • Systemadministratörer använder operativsystem eller databasverktyg (för direkta modifieringar av databaser) för att begå bedrägerier.
		Olovliga IKT-manipulationer på grund av otillräckliga processer och kontroller för IKT-behörighetshantering.	• Underlåtenhet att avaktivera eller radera onödiga konton såsom sådana från personal som har bytt tjänst och/eller har lämnat institutet, inbegripet gäster eller leverantörer som inte längre behöver åtkomst, vilka ger obehörig tillgång till IKT-systemen. • Beviljande av höga behörigheter, som medger obehörig åtkomst och/eller gör det möjligt att dölja oseriös verksamhet.
		Säkerhetshot på grund av bristande medvetenhet, varvid anställda inte förstår, försummar eller misslyckas med att följa policyer och regler för IKT-säkerhet.	• Anställda som luras att ge stöd till en attack (dvs. social manipulation). • Dålig praxis avseende autentiseringsuppgifter: delning av lösenord, användning av lösenord som är ”lätta” att gissa, användning av samma lösenord i många olika syften, etc. • Lagring av okrypterade konfidentiella uppgifter i bärbara datorer och bärbara datalagringslösningar (t.ex. usb-minnen) som kan tappas bort eller bli stulna.
		Obehörig lagring eller överföring av konfidentiella uppgifter utanför institutet.	• Personer som stjäl eller avsiktligt läcker eller smugglar ut konfidentiella uppgifter till obehöriga personer eller till allmänheten.
	Bristande fysisk IKT-säkerhet	Missbruk eller stöld av IKT-tillgångar genom fysisk tillgång som vållar skada, förlust av tillgångar eller	• Fysiska inbrott i kontorsbyggnader och/eller datacentraler för att stjäla IKT-utrustning (t.ex.

IKT-riskkategorier	IKT-risker (icke-uttömmande[10])	Riskbeskrivning	Exempel
		data eller för att möjliggöra andra hot.	datorer, bärbara datorer, lagringslösningar) och/eller att kopiera uppgifter genom fysisk tillgång till IKT-system.
		Uppsåtlig eller oavsiktlig skada på fysiska IKT-tillgångar som orsakas av terrorism, olyckor eller olyckliga/felaktiga manipulationer från institutets personal och/eller från tredje part (leverantörer, reparatörer).	• Fysisk terrorism (dvs. terroristbomber) eller sabotage av IKT-tillgångar. • Förstörelse av datacentral genom brand, vattenskada eller andra faktorer.
		Otillräckligt fysiskt skydd mot naturkatastrofer som leder till delvis eller komplett förstörelse av IKT-system/datacentraler på grund av naturkatastrofer.	• Jordbävningar, extrem hetta, stormar, massiva snöstormar, översvämningar, bränder, blixtnedslag.
Risker förknippade med IKT-ändringar	Bristande kontroll vid förändringar av IKT-system och IKT-utveckling	Incidenter som orsakas av oupptäckta fel eller svagheter beroende på ändringen (t.ex. oförutsedda effekter av en ändring eller en dåligt hanterad ändring på grund av bristande testning eller bristande praxis vid hantering av ändringar) av t.ex. programvara, IKT-system eller uppgifter.	• Idrifttagande av programvara som inte testats tillräckligt eller konfigureringar med oväntade negativa effekter på data (t.ex. förvanskning, radering) och/eller IKT-systemets prestanda (t.ex. avbrott, försämrad prestanda). • Okontrollerade förändringar av IKT-system eller uppgifter i produktionsmiljön. • Idrifttagande av IKT-system och internetapplikationer med dålig säkerhet, vilket ger hackare möjlighet att attackera de internettjänster som tillhandahålls och/eller att bryta sig in i de interna IKT-systemen. • Okontrollerade ändringar i källkoden för internt utvecklad programvara. • Otillräcklig testning på grund av att det saknas lämpliga provningsmiljöer.
	Bristande IKT-arkitektur	En svag IKT-arkitektur vid utformning, upprättande och underhåll av IKT-system (t.ex. programvara, maskinvara, uppgifter) kan, med tiden, leda till komplexa, svåra och rigida IKT-system som är svåra att hantera, inte längre motsvarar affärsbehoven	• Bristande hantering av ändringar i IKT-system, programvara och/eller data över en längre period som leder till komplexa, oenhetliga och svårhanterade IKT-system och arkitektur, vilket leder till mycket negativ påverkan på verksamheten

IKT-riskkategorier	IKT-risker (icke-uttömmande[10])	Riskbeskrivning	Exempel
		och underpresterar jämfört med de faktiska riskhanteringsbehoven.	och riskhanteringen (t.ex. brist på flexibilitet och smidighet, IKT-incidenter och fel, höga operativa kostnader, försvagad IKT-säkerhet och motståndskraft, minskad datakvalitet och rapporteringsförmåga). • Stora anpassningar och utökning av kommersiella programvarupaket med internt utvecklad programvara, vilket ger en oförmåga att införliva framtida versioner och uppdateringar av den kommersiella programvaran och risken att leverantören inte längre tillhandahåller någon support.
	Otillräcklig livscykelshantering och hantering av uppdateringar	Misslyckande att åstadkomma en lämplig inventering av alla IKT-tillgångar med stöd för och i kombination med en sund praxis avseende livscykel och hantering av uppdateringar. Detta leder till otillräckligt uppdaterade (och således mer sårbara) och föråldrade IKT-system som kanske inte uppfyller affärsbehoven och riskhanteringsbehoven.	• Föråldrade IKT-system som inte är uppdaterade och kan medföra negativ påverkan på verksamheten och riskhanteringen (t.ex. bristande flexibilitet och smidighet, IKT-driftavbrott, minskad IKT-säkerhet och motståndskraft).
IKT-dataintegritetsrisker	Felaktig IKT-databearbetning eller hantering	På grund av system-, kommunikations- och/eller applikationsfel eller brister, eller en felaktigt genomförd process för extrahering, överföring och laddning av data, kan uppgifter förvanskas eller förloras.	• It-systemfel vid satsbearbetning som orsakar felaktiga saldon på kundernas bankkonton. • Felaktigt genomförda förfrågningar. • Dataförlust på grund av fel vid datareplikering (backup).
	Felaktigt utformade kontroller för datavalidering i IKT-system	Fel som rör avsaknad av eller ineffektiva kontroller av automatiska indata för godkännande (t.ex. för uppgifter som använts från tredje part), överföring och hantering av data och kontroller av utdata i IKT-system (t.ex. validitetskontroller av resultat, avstämningar av uppgifter).	• Bristande eller ogiltig formatering/validering av indata i applikationer och/eller användargränssnitt. • Avsaknad av kontroller som rör avstämningar av uppgifter om producerade resultat. • Avsaknad av kontroller av genomförda processer för dataextrahering (t.ex. databasförfrågningar) som leder till felaktiga uppgifter. • Användning av felaktiga externa uppgifter.

IKT-riskkategorier	IKT-risker (icke-uttömmande[10])	Riskbeskrivning	Exempel
	Bristande kontroll av dataförändringar i IKT-driftsystem	Datafel som beror på avsaknad av kontroll huruvida datamanipulationer som genomförs vid idrifttagningen av IKT-system är korrekta och berättigade.	• Utvecklare eller databasadministratörer som har direkt tillgång till och kan ändra data i IKT-driftsystem på ett okontrollerat sätt, t.ex. vid en IKT-incident.
	Bristande utformning och/eller hantering av dataarkitektur, dataflöde, datamodeller eller datalexikon	Dataarkitektur, datamodeller, dataflöde eller datalexikon som hanteras bristfälligt kan leda till flera versioner av samma data i IKT-system som inte längre än konsekventa på grund av datamodeller eller datadefinitioner som tillämpas på olika sätt och/eller skillnader i den underliggande datagenereringen och ändringsprocessen.	• Förekomst av olika kunddatabaser per produkt eller affärsenhet med olika definitioner och fält för data vilket leder till inkonsekventa kunddata som är svåra att jämföra på nivån för hela finansinstitutet eller gruppen.
IKT-risker vid uppdragsavtal	Bristande motståndskraft hos en tredje part eller tjänst från en annan gruppenhet	Avsaknad av kritiskt utkontrakterade IKT-tjänster, telekommunikationstjänster och allmännyttiga tjänster. Förlust eller förvanskning av kritiska/känsliga uppgifter som anförtrotts tjänsteleverantören.	• Viktiga tjänster är inte tillgängliga till följd av fel i leverantörernas (utkontrakterade) IKT-system eller IKT-applikationer. • Störningar av telekommunikationslänkar. • Bristande strömförsörjning.
	Otillräcklig styrning av uppdragsavtal	Väsentligt försämrad service eller fel på grund av ineffektiv beredskap eller ineffektiva kontrollprocesser hos den tjänsteleverantör som erhållit uppdragsavtalet. Ineffektiv styrning vid utkontraktering kan ge brister på lämplig kompetens och kapacitet att fullt ut identifiera, bedöma, minska och övervaka IKT-riskerna och kan begränsa institutets operativa kapacitet.	• Dåliga processer för hantering av incidenter, avtalskontrollmekanismer och garantier som är inbyggda i avtalet med tjänsteleverantören och som ökar beroendet av tredje parter och leverantörer. • Otillräcklig kontroll av hantering av ändringar avseende tjänsteleverantörens IKT-miljö kan leda till väsentligt nedsatt service eller fel.
	Bristande säkerhet hos tredje part eller en annan enhet inom gruppen	Tjänsteleverantörens IKT-system kan hackas, vilket har direkt påverkan på de utkontrakterade tjänsterna eller kritiska/konfidentiella data som lagras hos tjänsteleverantören. Personal från tjänsteleverantörer får obehörig åtkomst till kritiska/känsliga data som lagras hos	• Tjänsteleverantörer hackas av kriminella eller terrorister som en ingångspunkt till institutets IKT-system eller för att få tillgång till/förstöra kritiska eller känsliga uppgifter som lagras hos tjänsteleverantören. • Illvilliga insiderpersoner från tjänsteleverantörens

IKT-riskkategorier	IKT-risker (icke-uttömmande[10])	Riskbeskrivning	Exempel
		tjänsteleverantören.	sida försöker stjäla och sälja känsliga uppgifter.