EBA/GL/2017/05

11/09/2017

Retningslinjer

Retningslinjer om IKT-risikovurdering under tilsynskontrol- og vurderingsprocessen (SREP)

1. Compliance- og indberetningsforpligtelser

Status for disse retningslinjer

1. Dette dokument indeholder retningslinjer, der er udstedt i henhold til artikel 16 i forordning (EU) nr. 1093/2010[1]. I henhold til artikel 16, stk. 3, i forordning (EU) nr. 1093/2010 skal de kompetente myndigheder og finansielle institutioner bestræbe sig på at efterleve disse retningslinjer bedst muligt.

2. Retningslinjerne afspejler EBA's syn på passende tilsynspraksis inden for det europæiske finanstilsynssystem eller på, hvordan EU-retten bør anvendes inden for et bestemt område. De kompetente myndigheder, som er omhandlet i artikel 4, stk. 2, i forordning (EU) nr. 1093/2010, og som er omfattet af retningslinjerne, bør efterleve disse ved i fornødent omfang at indarbejde dem i deres praksis (f.eks. ved at ændre deres retlige rammer eller deres tilsynsprocesser), også hvor retningslinjerne primært er rettet mod institutioner.

Indberetningskrav

3. I henhold til artikel 16, stk. 3, i forordning (EU) nr. 1093/2010 skal de kompetente myndigheder senest den 13.11.2017 underrette EBA om, hvorvidt de efterlever eller agter at efterleve disse retningslinjer, eller begrunde en eventuel manglende efterlevelse. Hvis EBA ikke er blevet underrettet inden denne dato, anser EBA de kompetente myndigheder for ikke at efterleve retningslinjerne. Underretninger fremsendes ved hjælp af det skema, der er tilgængeligt på EBA's websted, til compliance@eba.europa.eu med referencen "EBA/GL/2017/05". Underretninger fremsendes af personer med behørig beføjelse til at indberette efterlevelse på vegne af deres kompetente myndigheder. Enhver ændring af status med hensyn til efterlevelse skal også meddeles EBA.

4. Underretninger offentliggøres på EBA's websted i henhold til artikel 16, stk. 3.

[1] Europa-Parlamentets og Rådets forordning (EU) nr. 1093/2010 af 24. november 2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Banktilsynsmyndighed), om ændring af afgørelse nr. 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/78/EF (EUT L 331 af 15.12.2010, s. 12).

2. Genstand, anvendelsesområde og definitioner

Genstand og anvendelsesområde

5. Disse retningslinjer, som er udarbejdet i henhold til artikel 107, stk. 3, i direktiv 2013/36/EU[2], har til formål at sikre konvergens i tilsynspraksis i vurderingen af informations- og kommunikationsteknologi (IKT) i tilsynskontrol- og vurderingsprocessen (SREP), som fremgår af artikel 97 i direktiv 2013/36/EU og yderligere er angivet i EBA's retningslinjer om fælles procedurer og metoder for tilsynskontrol- og vurderingsprocessen (SREP)[3]. Disse retningslinjer specificerer vurderingskriterier, som kompetente myndigheder bør anvende i tilsynsvurderingen af institutternes governance og IKT-strategi samt tilsynsvurderingen af institutternes IKT-risikoeksponeringer og kontrol. Disse retningslinjer udgør en integreret del af EBA's SREP-retningslinjer.

6. De kompetente myndigheder bør anvende disse retningslinjer i overensstemmelse med anvendelsen af SREP, som er angivet i EBA's SREP-retningslinjer, og med den minimumsengagementsmodel og de proportionalitetskrav, som er fastlagt deri.

Adressater

7. Disse retningslinjer er rettet til de kompetente myndigheder som defineret i artikel 4, stk. 2, litra i), i forordning (EU) nr. 1093/2010.

Definitioner

8. Medmindre andet er angivet, har de termer, der er anvendt og defineret i direktiv 2013/36/EU og forordning (EU) nr. 575/2013, og definitionerne i EBA's SREP-retningslinjer samme betydning i disse retningslinjer. I disse retningslinjer finder endvidere følgende definitioner anvendelse:

IKT-systemer	IKT etableret som en del af en mekanisme eller et sammenkoblet net, der støtter et instituts drift.
IKT-tjenester	Tjenester fra IKT-systemer til en eller flere interne eller

[2] Europa-Parlamentets og Rådets direktiv 2013/36/EU af 26. juni 2013 om adgang til at udøve virksomhed som kreditinstitut og om tilsyn med kreditinstitutter og investeringsselskaber, om ændring af direktiv 2002/87/EF og om ophævelse af direktiv 2006/48/EF og 2006/49/EF. (1) – EUT L 176 af 27.6.2013, s. 338.

[3] EBA/GL/2014/13.

	eksterne brugere. Dette kan f.eks. være dataindlæsning, databehandling, dataopbevaring og indberetning, men også overvågning, forretnings- og beslutningstjenester.
IKT-tilgængelighed og kontinuitetsrisiko	Risikoen for, at IKT-systemer og data påvirkes negativt i henseende til ydeevne og tilgængelighed, herunder manglende evne til at genoprette instituttets tjenester i rette tid som følge af fejl i IKT-hardware- eller softwarekomponenter, svagheder i forvaltningen af IKT-systemer eller andre hændelser som beskrevet i bilaget.
IKT-sikkerhedsrisiko	Risikoen for uautoriseret adgang til IKT-systemer og -data i eller uden for instituttet (f.eks. cyberangreb) som beskrevet yderligere i bilaget.
IKT-ændringsrisiko	Den risiko, som opstår, når instituttet er ude af stand til at forvalte IKT-systemændringer på en rettidig og kontrolleret måde, navnlig for store og komplicerede ændringsprogrammer som beskrevet yderligere i bilaget.
IKT-dataintegritetsrisiko	Risikoen for, at data, der lagres og behandles af IKT-systemer, er ufuldstændige, upræcise eller ikke identiske på tværs af forskellige IKT-systemer, f.eks. som følge af svage eller manglende IKT-kontroller i de forskellige faser af IKT-datas livscyklus (f.eks. udformning af dataenes arkitektur, opbygning af datamodellen og/eller datastruktur/relationer, kontrol af datainput, kontrol af dataudtræk, overførsler og behandling af data, herunder dataoutput), svækkelse af et instituts mulighed for at yde tjenester og evne til at frembringe oplysninger om (risiko)forvaltning og finansielle oplysninger på korrekt og rettidig vis som beskrevet i bilaget.
IKT-outsourcingrisiko	Risikoen for, at inddragelse af en tredjepart eller en anden koncernenhed (koncernintern outsourcing) til levering af IKT-systemer eller tilknyttede tjenester har en negativ indvirkning på instituttets resultater og risikostyring som beskrevet nærmere i bilaget.

3. Implementering

Ikrafttrædelsesdato

9. Retningslinjerne træder i kraft den 1. januar 2018.

4. Krav til IKT-risikovurdering

Afsnit 1 – Generelle bestemmelser

10. Kompetente myndigheder bør gennemføre vurderingen af IKT-risikoen, governance og IKT-strategien som led i SREP-processen efter minimumsengagementsmodellen og proportionalitetskriterierne i afsnit 2 i EBA's SREP-retningslinjer. Dette betyder navnlig, at:

    a. hyppigheden af IKT-risikovurderingen afhænger af den minimumsengagementsmodel, som anføres af den SREP-kategori, et institut tildeles, og dets specifikke tilsynsprogram og

    b. dybden, detaljerne og intensiteten i IKT-vurderingen bør stå i forhold til størrelsen, strukturen og driftsmiljøet i instituttet samt arten, omfanget og kompleksiteten af dets aktiviteter.

11. Proportionalitetsprincippet gælder i disse retningslinjer for omfanget, hyppigheden og intensiteten af tilsynet og dialogen med et institut og de tilsynsmæssige forventninger til de standarder, som instituttet bør opfylde.

12. De kompetente myndigheder kan anvende og tage højde for det arbejde, som instituttet eller den kompetente myndighed allerede har udført i forbindelse med vurderingen af andre risici eller SREP-elementer for at få en opdateret vurdering. I forbindelse med gennemførelse af vurderingerne i disse retningslinjer bør de kompetente myndigheder udvælge den mest hensigtsmæssige tilsynsstrategi og metode, der passer bedst til instituttet, og de kompetente myndigheder bør bruge eksisterende og tilgængelig dokumentation (f.eks. relevante rapporter og andre dokumenter, møder med (risiko)ledelsen, resultater af undersøgelser på stedet) som hjælp til de kompetente myndigheders vurdering.

13. De kompetente myndigheder bør sammenfatte resultaterne af deres vurderinger ud fra kriterierne specificeret i disse retningslinjer og anvende dem med henblik på at nå frem til en konklusion om vurderingen af SREP-elementerne som angivet i EBA's SREP-retningslinjer.

14. Især bør vurderingen af governance- og IKT-strategien i overensstemmelse med afsnit 2 i disse retningslinjer afstedkomme resultater, der hjælper med at sammenfatte observationerne af vurderingen af den interne governance og instituttets kontrolelementer i SREP som angivet i afsnit 5 i EBA's SREP-retningslinjer og afspejlet i SREP-scoren. Endvidere bør de kompetente myndigheder overveje, om enhver negativ påvirkning af vurderingen af IKT-strategien på instituttets forretningsstrategi eller bekymringer om, at instituttet ikke har tilstrækkelige IKT-ressourcer og IKT-muligheder til at gennemføre og støtte vigtige planlagte strategiske ændringer, bør indgå i analysen af forretningsmodellen i overensstemmelse med afsnit 4 i EBA's SREP-retningslinjer

15. Resultatet af IKT-risikovurderingen som er specificeret i afsnit 3 i disse retningslinjer bør indgå i resultaterne af vurderingen af driftsrisikoen og bør anses for at indgå i den relevante score i afsnit 6.4 i EBA's SREP-retningslinjer.

16. Det bemærkes, at selv om de kompetente myndigheder generelt bør vurdere underkategorier af risici som led i de vigtigste kategorier (dvs. IKT-risikoen vurderes som led i driftsrisikoen), hvor de kompetente myndigheder anser visse underkategorier for at være væsentlige, kan de vurdere sådanne underkategorier individuelt. IKT-risikoen bør derfor identificeres som en væsentlig risiko af den kompetente myndighed, og disse retningslinjer bør desuden indeholde en scoringstabel (tabel 1), som bør anvendes til at give en separat underkategoriscore for IKT-risiko efter den generelle tilgang til scorer for kapitalrisici i EBA's SREP-retningslinjer.

17. For at nå frem til, hvorvidt IKT-risikoen bør anses som væsentlig, og IKT-risiko derfor bør vurderes og tildeles en score som en individuel underkategori af den operationelle risiko, kan de kompetente myndigheder anvende kriterierne i afsnit 6.1 i EBA's SREP-retningslinjer.

18. Når de kompetente myndigheder anvender disse retningslinjer, bør de, hvor det er relevant, tage højde for den ikke-udtømmende liste over underkategorier af IKT-risici og risikoscenarier som anført i bilaget, idet det bemærkes, at bilaget fokuserer på IKT-risici, som kan medføre meget alvorlige tab. De kompetente myndigheder kan udelukke nogle af de IKT-risici, som indgår i klassificeringen, hvis de ikke er relevante for deres vurdering. Institutterne ventes at fastholde deres egne risikoklassificeringer i stedet for IKT-risikoklassificeringen i bilaget.

19. Når disse retningslinjer anvendes i forbindelse med internationale bankkoncerner og de enheder, som de består af, og tilsynskollegiet er oprettet, bør de kompetente myndigheder, inden for rammerne af deres samarbejde om SREP-vurderingen i henhold til punkt 11.1 i EBA's SREP-retningslinjer, i videst muligt omfang samordne det nøjagtige og detaljerede anvendelsesområde for hver oplysning på en konsekvent måde for alle koncernenheder.

Afsnit 2 – Vurdering af institutternes governance og IKT-strategi

2.1 Almindelige principper

20. De kompetente myndigheder bør vurdere, om instituttets generelle rammer for governance og intern kontrol dækker IKT-systemerne og de dermed forbundne risici, og om ledelsesorganisationen håndterer og forvalter disse aspekter i tilstrækkeligt omfang, eftersom IKT er en integreret del af et instituts funktioner.

21. I forbindelse med udførelsen af vurderingen bør de kompetente myndigheder henvise til krav og standarder for god intern governance og risikokontrol som anført i EBA's retningslinjer om intern governance[4] og internationale retningslinjer på dette område, i det omfang disse kan anvendes i lyset af IKT-systemer og -risici.

22. Vurderingen i dette afsnit dækker ikke de specifikke elementer af forvaltningen af IKT-systemet, risikostyring og kontroller med fokus på at forvalte specifikke IKT-risici i afsnit 3 i disse retningslinjer, men fokuserer på følgende områder:

    a. IKT-strategi – om instituttet har en IKT-strategi, som er tilstrækkeligt forvaltet og i overensstemmelse med instituttets forretningsstrategi

    b. den overordnede interne governance – om instituttets overordnede interne governance er tilstrækkelig i forhold til instituttets IKT-systemer, og

    c. IKT-risikoen i instituttets risikostyringsrammer – om instituttets rammer for risikostyring og intern kontrol sikrer instituttets IKT-systemer på tilstrækkelig vis.

23. Pkt. 22, litra a), indeholder oplysninger om elementer af instituttets governance, men bør primært indgå i vurderingen af forretningsmodellen i afsnit 4 i EBA's SREP-retningslinjer. Litra b) og c) supplerer vurderingerne af emnerne i afsnit 5 i EBA's SREP-retningslinjer, og vurderingen i disse retningslinjer bør indgå i den relevante vurdering i afsnit 5 i EBA's SREP-retningslinjer.

24. Resultatet af denne vurdering bør, hvor det er relevant, indgå i vurderingen af risikostyring og -kontrol i afsnit 3 i disse retningslinjer.

2.2 IKT-strategi

25. I dette afsnit bør de kompetente myndigheder vurdere, om instituttet har en IKT-strategi, der er underlagt et tilstrækkeligt tilsyn fra instituttets ledelse, som stemmer overens med

[4] EBA's retningslinjer om intern ledelse, GL 44, 27. september 2011.

forretningsstrategien, navnlig med hensyn til at holde IKT ajourført og planlægge eller gennemføre vigtige og komplekse IKT-ændringer, og som støtter instituttets forretningsmodel.

2.2.1 Udvikling af IKT-strategien og dens tilstrækkelighed

26. De kompetente myndigheder bør vurdere, om instituttet har indført rammer, som står i forhold til arten, omfanget og kompleksiteten af IKT-aktiviteterne med hensyn til at udarbejde og udvikle instituttets IKT-strategi. I forbindelse med denne vurdering skal de kompetente myndigheder overveje, om:

    a. den daglige ledelse[5] for forretningsområdet eller -områderne er tilstrækkeligt involveret i definitionen af instituttets strategiske IKT-prioriteter, og at den daglige ledelse af IKT-funktionen er klar over udviklingen, udformningen og indledningen af store forretningsstrategier og initiativer, der skal sikre en fortsat ensretning af IKT-systemer, IKT-tjenester og IKT-funktionen (dvs. de ansvarlige for forvaltningen og anvendelsen af disse systemer og tjenester) og instituttets forretningsstrategi, og at IKT er opdateret

    b. IKT-strategien er dokumenteret og støttes af konkrete implementeringsplaner, navnlig vedrørende vigtige milepæle og ressourceplanlægning (herunder finansielle og menneskelige ressourcer), som skal sikre, at de er realistiske og gør det muligt at levere IKT-strategien

    c. instituttet løbende ajourfører sin IKT-strategi, navnlig i forbindelse med en ny forretningsstrategi, for at sikre fortsat strømlining mellem IKT- og forretningsmæssige mellemlangsigtede og/eller langsigtede mål, planer og aktiviteter og

    d. instituttets ledelsesorgan godkender IKT-strategien og implementeringsplaner og overvåger gennemførelsen deraf.

2.2.2 Implementering af IKT-strategien

27. Hvis instituttets IKT-strategi kræver, at der implementeres vigtige og komplicerede IKT-ændringer eller ændringer med store konsekvenser for instituttets forretningsmodel, bør de kompetente myndigheder vurdere, om instituttet har kontrolrammer på plads, som svarer til dets størrelse, dets IKT-aktiviteter samt niveauet af ændringsaktiviteter, for at støtte en effektiv implementering af instituttets IKT-strategi. I forbindelse med denne vurdering bør de kompetente myndigheder tage hensyn til, om kontrolrammerne:

    a. omfatter ledelsesprocesser (dvs. status- og budgetovervågning og rapportering) og relevante organer (f.eks. et projektstyringskontor (PMO)), en IKT-styringsgruppe eller lignende), som effektivt støtter implementeringen af IKT-strategiprogrammerne

    b. har defineret og tildelt roller og ansvarsområder for implementeringen af IKT-strategiprogrammerne, navnlig med hensyn til vigtige interessenters erfaring med at tilrettelægge, styre og overvåge vigtige og komplekse IKT-ændringer og styring af mere

[5] Den daglige ledelse og ledelsesorganet som defineret i direktiv 2013/36/EU af 26. juni 2013 i artikel 3, stk. 7, "ledelsesorgan" og artikel 3, stk. 9, "den daglige ledelse".

generelle organisatoriske og menneskelige konsekvenser (f.eks. styring af modstand mod ændringer, uddannelse, kommunikation)

c. inddrager den uafhængige funktion for kontrol og intern revision for at sikre, at risikoen i forbindelse med implementeringen af IKT-strategien er identificeret, vurderet og effektivt håndteret, og at rammerne for governance af implementeringen af IKT-strategien er effektive, og

d. indeholder en planlægnings- og planlægningsevalueringsproces, der giver fleksibilitet i forhold til vigtige identificerede problemer (f.eks. implementeringsproblemer eller -forsinkelser) eller eksterne hændelser (f.eks. vigtige ændringer i forretningsmiljøet, teknologiske problemer eller innovation), for at sikre rettidig tilpasning af den strategiske implementeringsplan.

2.3 Overordnet intern governance

28. I overensstemmelse med afsnit 5 i EBA's SREP-retningslinjer bør de kompetente myndigheder vurdere, om instituttet har en passende og gennemsigtig virksomhedsstruktur, der er "formålstjenlig", og har fastsat passende governance. Specifikt med hensyn til IKT-systemer og i overensstemmelse med EBA's retningslinjer vedrørende intern ledelse bør denne vurdering indeholde en vurdering af, om instituttet viser:

    a. en robust og gennemsigtig organisatorisk struktur med klare ansvarsområder for IKT, der omfatter både ledelsesorganet og dets udvalg, og at de vigtigste IKT-ansvarlige (f.eks. IT-direktøren, "CIO", den tekniske direktør, "COO" eller tilsvarende) har tilstrækkelig indirekte eller direkte adgang til ledelsesorganet for at sikre, at vigtige IKT-oplysninger eller -problemer rapporteres, drøftes eller besluttes af ledelsesorganet, og

    b. at ledelsesorganet kender og håndterer risici i forbindelse med IKT

29. I tillæg til afsnit 5.2 i EBA's SREP-retningslinjer bør de kompetente myndigheder vurdere, om instituttets IKT-outsourcingpolitik og strategi, hvor det er relevant, tager højde for, hvordan IKT-outsourcing påvirker instituttets forretning og forretningsmodel.

2.4 IKT-risiko i instituttets risikostyringsrammer

30. I vurderingen af instituttets risikostyring og interne kontrol som beskrevet i afsnit 5 i EBA's SREP-retningslinjer bør de kompetente myndigheder overveje, om instituttets rammer for risikostyring og intern kontrol i tilstrækkelig grad sikrer instituttets IKT-systemer på en måde, der svarer til instituttets størrelse og aktiviteter samt dets IKT-risikoprofil som defineret i afsnit 3. Navnlig bør de kompetente myndigheder fastslå, om:

    a. risikovilligheden og ICAAP dækker IKT-risiciene som led i en mere generel driftsrisikokategori med henblik på at definere den generelle risikostrategi og bestemme den interne kapital, og

    b. IKT-risiciene ligger inden for anvendelsesområdet for instituttets rammer for risikostyring og intern kontrol

31. De kompetente myndigheder bør foretage vurderingen i litra a) ovenfor under hensyntagen til både forventede og uforudsete scenarier, f.eks. scenarier i stresstest som led i tilsynsprocessen for instituttet.

32. Specifikt med hensyn til litra b) bør de kompetente myndigheder vurdere, om de uafhængige funktioner for kontrol og intern revision som beskrevet i pkt. 104, litra a), 104, litra d), 105, litra a), og 105, litra c), i EBA's SREP-retningslinjer er hensigtsmæssige i forhold til at sikre tilstrækkelig uafhængighed mellem IKT og kontrol- og revisionsfunktionerne i lyset af instituttets størrelse og IKT-risikoprofil.

2.5 Opsummering af observationer

33. Resultaterne bør afspejles i opsummeringen af observationerne under afsnit 5 i EBA's SREP-retningslinjer og bør udgøre en del af den enkelte score i overensstemmelse med betragtningerne i tabel 3 i EBA's SREP-retningslinjer.

34. Til vurdering af IKT-strategien bør følgende spørgsmål overvejes, når der skal drages en konklusion på ovenstående vurdering:

    a. Hvis de kompetente myndigheder konkluderer, at instituttets governance er utilstrækkelig med hensyn til at udvikle og implementere instituttets IKT-strategi under 2.2., bør dette indgå i vurderingen af instituttets interne ledelse i afsnit 5 i EBA's SREP-retningslinjer i pkt. 87, litra a).

    b. Hvis de kompetente myndigheder ud fra ovenstående vurderinger under 2.2 konkluderer, at der er en betydelig uoverensstemmelse mellem IKT-strategien og forretningsstrategien, som kan have en betydelig negativ indvirkning på instituttets langsigtede forretningsmæssige og/eller økonomiske mål, instituttets bæredygtighed og/eller forretningsmodel eller instituttets forretningsområder/-linjer, som er fastlagt som de vigtigste i stk. 62, litra a) i EBA's SREP-retningslinjer, bør dette indgå i vurderingen af forretningsmodellen i afsnit 4 i SREP-retningslinjerne under pkt. 70, litra b) og c).

    c. Hvis de kompetente myndigheder ud fra ovenstående vurderinger under 2.2 konkluderer, at instituttet muligvis ikke har tilstrækkelige IKT-ressourcer og IKT-implementeringsmuligheder til at gennemføre og støtte vigtige planlagte strategiske ændringer, bør dette indgå i vurderingen af forretningsmodellen i afsnit 4 i EBA's SREP-retningslinjer under punkt 70, litra b.

Afsnit 3 – Vurdering af instituttets IKT-risikoeksponering og kontrol

3.1 Generelle betragtninger

35. De kompetente myndigheder bør vurdere, om instituttet har identificeret, vurderet og mitigeret sine IKT-risici tilstrækkeligt. Denne proces bør være en del af de operationelle risikostyringsrammer og stemme overens med tilgangen til den operationelle risiko.

36. De kompetente myndigheder bør først og fremmest identificere de væsentlige iboende IKT-risici, som instituttet er eller kan være eksponeret for, efterfulgt af en vurdering af effektiviteten af instituttets IKT-risikostyringsrammer, procedurer og kontroller til at reducere disse risici. Resultatet af vurderingerne bør afspejles i en opsummering af observationerne, som indgår i scoren for den operationelle risiko i SREP-retningslinjerne. Hvis IKT-risikoen anses for at være væsentlig, og de kompetente myndigheder ønsker at tildele en individuel score, bør tabel 1 bruges til at tildele en score som en underrisiko af den operationelle risiko.

37. I forbindelse med vurderinger under dette afsnit bør de kompetente myndigheder trække på alle tilgængelige informationskilder som anført i pkt. 127 i afsnit 6 i EBA's SREP-retningslinjer, f.eks. instituttets risikostyringsaktiviteter, rapporter og resultater, som grundlag for identificeringen af deres tilsynsvurderingsprioriteter. De kompetente myndigheder bør desuden bruge andre informationskilder til at foretage denne vurdering, herunder følgende, hvor det er relevant:

    a. egenvurderinger af IKT-risiko og kontrol (hvis dette fremgår af ICAAP-oplysningerne)
    b. IKT-risikorelaterede ledelsesoplysninger, som fremsendes til instituttets ledelsesorgan, f.eks. periodisk og hændelsesorienteret IKT-risikorapportering (herunder databasen over operationelle tab), IKT-risikoeksponeringsdata fra instituttets risikostyringsfunktion
    c. IKT-relaterede interne og eksterne revisionsobservationer rapporteret til instituttets revisionsudvalg.

3.2 Identificering af væsentlige IKT-risici

38. De kompetente myndigheder bør identificere de væsentlige IKT-risici, som instituttet er eller kan blive eksponeret for, ved hjælp af følgende trin:

3.2.1 Gennemgang af instituttets IKT-risikoprofil

39. I forbindelse med gennemgangen af instituttets IKT-risikoprofil bør de kompetente myndigheder undersøge alle relevante oplysninger om instituttets IKT-risikoeksponering, herunder oplysningerne i pkt. 37 og de identificerede væsentlige mangler eller svagheder i IKT-organisationens og instituttets kontroller under afsnit 2 i disse retningslinjer og, hvor det er relevant, gennemgå disse oplysninger. Som led i denne gennemgang bør de kompetente myndigheder overveje:

a. den potentielle konsekvens, som en større afbrydelse af instituttets IKT-systemer kan få for det finansielle system, enten på nationalt eller internationalt niveau
b. om instituttet har forhøjede IKT-sikkerhedsrisici eller IKT-tilgængeligheds- og -kontinuitetsrisici som følge af internetbrug, omfattende anvendelse af innovative IKT-løsninger eller andre forretningsmæssige distributionskanaler, som kan gøre det til et mere sandsynligt mål for cyberangreb
c. om instituttet kan være mere eksponeret for IKT-sikkerhedsrisici, IKT-tilgængeligheds- og -kontinuitetsrisici, IKT-dataintegritetsrisici eller IKT-ændringer som følge af kompleksiteten (f.eks. som følge af opkøb eller fusioner) eller forældede IKT-systemer
d. om instituttet gennemfører væsentlige ændringer i sit IKT-system og/eller sin IKT-funktion (f.eks. som følge af fusioner, opkøb, frasalg eller udskiftning af det centrale IKT-system), som kan påvirke IKT-systemets stabilitet eller funktion negativt og kan medføre væsentlige IKT-tilgængeligheds- og -kontinuitetsrisici, IKT-sikkerhedsrisici, IKT-ændringsrisici eller IKT-dataintegritetsrisici
e. om instituttet har udliciteret IKT-tjenester eller IKT-systemer i eller uden for koncernen, som kan udgøre væsentlige IKT-outsourcingrisici
f. om instituttet gennemfører aggressive IKT-omkostningsbesparelser, som kan føre til en reduktion i de nødvendige IKT-investeringer, ressourcer og IT-ekspertise, og som kan øge eksponeringen for alle IKT-risikotyperne i klassificeringen
g. om placeringen af vigtige IKT-drifts-/datacentre (f.eks. regioner, lande) kan eksponere instituttet for naturkatastrofer (f.eks. oversvømmelser, jordskælv), politisk ustabilitet eller arbejdsmarkedskonflikter og civile uroligheder, som kan føre til en væsentlig forøgelse af IKT-tilgængeligheds- og -kontinuitetsrisici og IKT-sikkerhedsrisici.

3.2.2 Gennemgang af de kritiske IKT-systemer og -tjenester

40. Som led i processen med at identificere IKT-risici med potentielt væsentlig tilsynsmæssig påvirkning af instituttet bør de kompetente myndigheder gennemgå dokumentationen fra instituttet og danne sig en mening om de IKT-systemer og -tjenester, som er væsentlige for, at instituttets væsentlige aktiviteter kan fungere korrekt og er tilgængelige, kontinuerlige og sikre.

41. Til dette formål bør de kompetente myndigheder gennemgå de metoder og processer, som instituttet anvender til at identificere de IKT-systemer og tjenester, som er vigtige, under hensyntagen til, at visse IKT-systemer og -tjenester kan blive anset for at være kritiske for instituttet med hensyn til forretningskontinuitet og tilgængelighed samt sikkerhed (f.eks. forebyggelse af svig) og/eller fortrolighed. I forbindelse med gennemgangen bør de kompetente myndigheder tage højde for, at kritiske IKT-systemer og -tjenester bør opfylde mindst en af følgende betingelser:

a. De supporter instituttets centrale daglige drift og distributionskanaler (f.eks. betalingsautomater, internet- og mobilbank).

b. De støtter vigtige ledelsesprocesser og virksomhedsfunktioner, herunder risikostyring (f.eks. risikostyrings- og likviditetsstyringssystemer).

c. De hører ind under særlige (eventuelle) retlige eller reguleringsmæssige krav, der medfører øget tilgængelighed, modstandsdygtighed, fortrolighed eller sikkerhed (f.eks.

databeskyttelseslovgivning eller eventuelle mål for genoprettelsestid (Recovery Time Objectives, RTO, som er den maksimale tid, det må tage at genoprette systemet eller processen efter en hændelse) og mål for genoprettelsestidspunkt (Recovery Point Objective, RPO, som er den maksimale tid, hvor data kan mistes i tilfælde af en hændelse)) for visse systemisk vigtige tjenester (hvis sådanne er tilgængelige).

d. De behandler eller lagrer fortrolige eller følsomme data, hvor uautoriseret adgang i høj grad kan påvirke instituttets omdømme, finansielle resultater eller forretningens sundhed og kontinuitet (f.eks. databaser med følsomme kundeoplysninger) og/eller

e. De indeholder grundlæggende funktioner, som er vigtige for, at instituttet kan fungere korrekt (f.eks. telekommunikations- og netværkstjenester og IKT- og cybersikkerhedstjenester).

3.2.3 Identificering af væsentlige IKT-risici for vigtige IKT-systemer og -tjenester

42. Under hensyntagen til gennemgangen af instituttets IKT-risikoprofil og ovennævnte kritiske IKT-systemer og -tjenester bør de kompetente myndigheder danne sig en mening om de væsentlige IKT-risici, som efter deres vurdering kan have en væsentlig tilsynsmæssig påvirkning af instituttets kritiske IKT-systemer og -tjenester.

43. I forbindelse med vurderingen af den potentielle påvirkning, som IKT-risici kan have for et instituts kritiske IKT-systemer og -tjenester, bør de kompetente myndigheder overveje følgende:

a. den finansielle påvirkning, herunder (men ikke begrænset til) tab af midler eller aktiver, potentiel kundekompensation, rets- og afhjælpningsomkostninger, erstatning under kontrakt, mistede indtægter

b. muligheden for forretningsafbrydelser under hensyntagen (men ikke begrænset) til betydningen af de påvirkede finansielle tjenesteydelser, antallet af kunder og/eller afdelinger og potentielt berørte medarbejdere

c. den potentielle indvirkning på instituttets omdømme baseret på betydningen af banktjenesten eller driftsaktiviteten (f.eks. tyveri af kundedata), den eksterne profil/synlighed af de berørte IKT-systemer og -tjenester (f.eks. mobil- eller onlinebanksystemer, salgssteder, hæveautomater eller betalingssystemer)

d. den reguleringsmæssige indvirkning, herunder muligheden for offentlig censur fra regulatorens side, bøder eller endda ændring af tilladelser

e. den strategiske indvirkning på instituttet, f.eks. hvis det strategiske produkt eller forretningsplaner kompromitteres eller stjæles.

44. De kompetente myndigheder bør derefter kortlægge de identificerede IKT-risici, som anses for at være væsentlige, i følgende IKT-risikokategorier, som er beskrevet yderligere med eksempler i bilaget. De kompetente myndigheder bør reflektere over IKT-risiciene i bilaget som led i vurderingen i afsnit 3:

a. IKT-tilgængeligheds- og -kontinuitetsrisiko
b. IKT-sikkerhedsrisiko

c. IKT-ændringsrisiko
d. IKT-dataintegritetsrisiko
e. IKT-outsourcingrisiko.

Kortlægningen skal hjælpe de kompetente myndigheder med at bestemme, hvilke (eventuelle) risici som er væsentlige og derfor bør underkastes en nøjere og/eller dybere gennemgang i følgende vurderingstrin.

3.3 Vurdering af kontrollerne til reduktion af væsentlige IKT-risici

45. For at vurdere instituttets rest-IKT-risikoeksponering bør de kompetente myndigheder gennemgå, hvordan instituttet identificerer, overvåger, vurderer og reducerer de væsentlige risici, som de kompetente myndigheder har identificeret i ovennævnte vurdering.

46. Til dette formål bør de kompetente myndigheder for de identificerede væsentlige IKT-risici gennemgå gældende:

    a. IKT-risikostyringspolitik, -processer og -risikotolerance
    b. organisationsstyring og løbende overvågning
    c. intern revision og observationer og
    d. IKT-risikokontrol, som er specifik for den identificerede væsentlige IKT-risiko.

47. I vurderingen bør der tages højde for resultatet af analysen i rammerne for den overordnede risikostyring og de interne kontrolrammer i afsnit 5 i EBA's SREP-retningslinjer samt instituttets governance og strategi i afsnit 2 i disse retningslinjer, eftersom betydelige mangler på disse områder kan påvirke instituttets evne til at styre og reducere dets IKT-risikoeksponeringer. Hvor det er relevant, bør de kompetente myndigheder også gøre brug af informationskilderne i pkt. 37 i disse retningslinjer.

48. De kompetente myndigheder bør gennemgå følgende vurderingstrin på en måde, som står i forhold til arten, omfanget og kompleksiteten af instituttets aktiviteter og ved at anvende en tilsynsgennemgang, som svarer til instituttets IKT-risikoprofil.

3.3.1 IKT-risikostyringspolitik, -processer og -tolerance

49. De kompetente myndigheder bør gennemgå, om instituttet har passende risikostyringspolitikker, -processer og risikotolerance for de identificerede væsentlige IKT-risici. Disse kan indgå i rammerne for operationel risikostyring eller i et særskilt dokument. De kompetente myndigheder bør i forbindelse med denne vurdering tage hensyn til:

    a. om risikostyringspolitikken er formaliseret og godkendt af ledelsen og indeholder tilstrækkelig vejledning om instituttets IKT-risikovillighed og de vigtigste forfulgte IKT-risikostyringsmålsætninger og/eller anvendte IKT-risikotolerancetærskler. Den relevante IKT-risikostyringspolitik bør ligeledes formidles til alle relevante interessenter
    b. om den gældende politik dækker alle betydelige elementer for risikostyring af de identificerede væsentlige IKT-risici

c. om instituttet har implementeret en proces og underliggende procedurer til identificering (f.eks. egenvurdering af risikokontrol (RCSA), analyser af risikoscenarier) og overvågning af de involverede væsentlige IKT-risici og
d. om instituttet har en IKT-risikostyringsrapportering, der giver den daglige ledelse og ledelsesorganet rettidige oplysninger, og som lader den daglige ledelse og/eller ledelsesorganet vurdere og overvåge, om instituttets planer og foranstaltninger for IKT-risikoreduktion stemmer overens med den godkendte risikovillighed og/eller -tolerance (hvor dette er relevant) og overvåge ændringer af væsentlige IKT-risici.

3.3.2 Organisationsstyring og løbende overvågning

50. De kompetente myndigheder bør vurdere, hvordan de gældende risikostyringsroller og -ansvarsområder er indlejret og integreret i den interne organisation til styring og overvågning af de identificerede væsentlige IKT-risici. I denne henseende bør de kompetente myndigheder vurdere, om instituttet udviser:

a. tydelige roller og ansvarsområder for identificering, vurdering, overvågning, reduktion, rapportering og tilsyn med den involverede væsentlige IKT-risiko
b. at risikoansvar og -roller kommunikeres tydeligt, fordeles og indlejres i de relevante dele (f.eks. forretningslinjer, IT) og organisationsprocesser, herunder roller og ansvarsområder i forbindelse med indsamling og sammenlægning af risikooplysninger og rapportering til den daglige ledelse og/eller ledelsesorganet
c. at IKT-risikostyringsaktiviteter gennemføres med tilstrækkelige og kvalitative hensigtsmæssige menneskelige og tekniske ressourcer. For at vurdere troværdigheden af de gældende risikoreduktionsplaner bør de kompetente myndigheder også vurdere, om instituttet har tildelt tilstrækkelige finansielle budgetter og/eller andre krævede ressourcer til gennemførelsen deraf
d. en tilstrækkelig opfølgning på og svar fra ledelsesorganet med hensyn til vigtige observationer af de uafhængige kontrolfunktioner vedrørende IKT-risici under hensyntagen til eventuel uddelegering af visse aspekter til et udvalg, hvor et sådan findes, og
e. at undtagelser fra de gældende IKT-regler og -politikker registreres og underkastes en dokumenteret gennemgang og rapportering i den uafhængige kontrolfunktion med fokus på relevante risici.

3.3.3 Intern revision og observationer

51. De kompetente myndigheder bør overveje, om den interne revisionsfunktion er effektiv med hensyn til at revidere de gældende IKT-risikokontrolrammer ved at gennemgå, om:

a. IKT-risikokontrolrammerne revideres med den krævede kvalitet, dybde og hyppighed og står i forhold til instituttets størrelse, aktiviteter og IKT-risikoprofil
b. revisionsplanen omfatter revisioner af de kritiske IKT-risici identificeret af instituttet
c. de vigtige IKT-revisionsresultater, herunder aftalte foranstaltninger, rapporteres til ledelsesorganet og

d. IKT-revisionsresultater, herunder aftalte foranstaltninger, følges op, og statusrapporter løbende gennemgås af den daglige ledelse og/eller revisionsudvalget.

3.3.4 IKT-risikokontrol, som er specifik for de identificerede væsentlige IKT-risici

52. For de identificerede væsentlige IKT-risici bør de kompetente myndigheder vurdere, om instituttet har indført specifikke kontroller til at tage hånd om disse risici. Følgende afsnit indeholder en ikke-udtømmende liste over de specifikke kontroller, som skal overvejes, når de væsentlige risici identificeret under pkt. 3.2.2, som blev kortlagt til følgende IKT-risikokategorier, vurderes:

a. IKT-tilgængeligheds- og -kontinuitetsrisici
b. IKT-sikkerhedsrisici
c. IKT-ændringsrisici
d. IKT-dataintegritetsrisici
e. IKT-outsourcingrisici.

a) Kontroller til styring af væsentlige IKT-tilgængeligheds- og -kontinuitetsrisici

53. Ud over kravene i EBA's SREP-retningslinjer (pkt. 279-281) bør de kompetente myndigheder vurdere, om instituttet har passende rammer på plads til at identificere, forstå, måle og reducere IKT-tilgængeligheds- og -kontinuitetsrisici.

54. De kompetente myndigheder bør i forbindelse med denne vurdering navnlig tage hensyn til, om rammerne:

a. identificerer de kritiske IKT-processer og de relevante understøttende IKT-systemer, som bør være en del af de driftsmæssige genopretning- og beredskabsplaner med:

i. en omfattende analyse af afhængigheden mellem kritiske forretningsprocesser og støttesystemer

ii. bestemmelse af genopretningsmål for de understøttende IKT-systemer (som f.eks. typisk bestemmes af virksomheden og/eller lovgivningen med hensyn til RTO og RPO)

iii. passende beredskabsplaner, der sikrer tilgængelighed, kontinuitet og genopretning af kritiske IKT-systemer og -tjenester for at minimere afbrydelser i instituttets drift inden for en acceptabel grænse

b. har politikker, standarder og operationelle kontroller for genopretning og beredskab, som inkluderer:

i. sikringsforanstaltninger til at undgå, at et enkelt scenario, en enkelt hændelse eller en katastrofe kan påvirke både IKT-produktionen og -genoprettelsessystemerne

ii. IKT-systembackup og -genopretningsprocedurer for kritisk software og data, der sikrer, at disse backups lagres på en sikker og tilstrækkelig fjern placering, så en hændelse eller en katastrofe ikke kan ødelægge disse kritiske data

iii. overvågning af løsninger til rettidig sporing af IKT-tilgængeligheds- eller -kontinuitetshændelser

iv. en dokumenteret incident- og eskaleringsproces, der også indeholder vejledning om de forskellige incident- og eskaleringsroller og -ansvarsområder, medlemmerne af kriseudvalget eller -udvalgene og kommandokæden i hastetilfælde

v. fysiske sikringsforanstaltninger, der både beskytter instituttets kritiske IKT-infrastruktur (f.eks. datacentre) mod miljømæssige risici (f.eks. oversvømmelser og andre naturkatastrofer) og sikrer et stabilt driftsmiljø for IKT-systemer (f.eks. ventilation)

vi. processer, roller og ansvar, der sikrer, at også outsourcede IKT-systemer og -tjenester er omfattet af passende driftsmæssige genopretnings- og beredskabsløsninger og -planer

vii. IKT-performance- og -kapacitetsplanlægnings- og -overvågningsløsninger for kritiske IKT-systemer og -tjenester med definerede tilgængelighedskrav, der sporer vigtige performance- og kapacitetsbegrænsninger rettidigt

viii. løsninger, der skal beskytte kritiske internetvendte aktiviteter og tjenester (f.eks. netbanktjenester), mod "denial of service" og andre cyberangreb fra internettet, og som derved har til formål beskytte og styre adgangen til disse aktiviteter og tjenester.

c. teste IKT-tilgængeligheds- og -beredskabsløsninger mod en række realistiske scenarier, herunder cyberangreb, fail-over-test og test af backup til kritisk software og data, som:

i. planlægges, formaliseres og dokumenteres, og hvor testresultaterne anvendes til at styrke effektiviteten af IKT-tilgængelighed og beredskabsløsninger

ii. omfatter interessenter og funktioner i organisationen såsom styring af forretningslinjer, herunder forretningsberedskab, incident-- og krisehåndteringsteams samt relevante eksterne interessenter i økosystemet

iii. ledelsesorganet og den daglige ledelse er involveret i (f.eks. som en del af krisehåndteringsteams) og underrettes om testresultater.

b) Kontrol til styring af væsentlige IKT-sikkerhedsrisici

55. Kompetente myndigheder bør vurdere, om instituttet har effektive rammer på plads til at identificere, måle og reducere IKT-sikkerhedsrisici. De kompetente myndigheder bør i forbindelse med denne vurdering navnlig tage hensyn til, om rammerne tager højde for:

a. klart definerede roller og ansvarsfordeling vedrørende:

i. den eller de personer eller udvalg, som er ansvarlige for og/eller står til regnskab for den daglige IKT-sikkerhedsstyring og udarbejdelsen af de generelle IKT-sikkerhedspolitikker med opmærksomhed på deres uafhængighed
ii. udformning, implementering , styring og overvågning af IKT-sikkerhedskontroller
iii. beskyttelse af kritiske IKT-systemer og -tjenester gennem vedtagelse af f.eks. en sårbarhedsvurdering, styring af softwarepatches, endpointbeskyttelse (f.eks. malwarevirus) og værktøjer til sporing og forebyggelse af hændelser

iv. overvågning, klassificering og håndtering af eksterne eller interne IKT-sikkerhedshændelser, herunder hændelseshåndtering og genopretning af IKT-systemer og -tjenester
v. løbende og proaktive trusselsvurderinger til opretholdelse af passende sikkerhedskontroller

b. en IKT-sikkerhedspolitik, der tager højde for og, hvor det er relevant, opfylder internationalt anerkendte IKT-sikkerhedsstandarder og sikkerhedsprincipper (f.eks. princippet om sidste privilegium ("principle of last privilege"), dvs. begrænset adgang til det minimumsniveau, der giver mulighed for normal funktionalitet ved styring af adgangsrettigheder og princippet om forsvar i dybden ("principle of defence in depth"), dvs. design af sikkerhedsarkitektur, hvor lagdelte sikkerhedsmekanismer øger systemsikkerheden)

c. en proces til identificering af IKT-systemer og tilsvarende sikkerhedskrav, der afspejler potentiel risiko for svindel, misbrug og/eller forkert anvendelse af fortrolige data, samt dokumenterede sikkerhedsforventninger som knyttes til disse identificerede IKT-systemer og data, og som sammenholdes med instituttets risikotolerance og løbende overvågning for implementering

d. en dokumenteret proces for incidenthåndtering og eskalering, der vejleder om de forskellige incident- og eskaleringsroller og ansvarsområder, medlemmerne af kriseberedskabet eller -udvalgene og kommandokæden i tilfælde af hasteændringer relateret til sikkerhed

e. log over adgange for at sikre en effektiv overvågning og rettidig sporing af uautoriseret aktivitet og for at bidrage til eller gennemføre kriminaltekniske undersøgelser af sikkerhedshændelser. Instituttet bør indføre logpolitikker, der definerer de logs, der skal føres, og hvor længe de skal opbevares

f. awarenesskampagner eller -initiativer skal indgå i alle niveauer i instituttet omhandlende sikker brug og beskyttelse af instituttets IKT-systemer og de vigtigste IKT-sikkerhedsrisici (og andre risici), som de skal være opmærksomme på, navnlig vedrørende eksisterende og nye cybertrusler (f.eks. computervirusser, mulige interne eller eksterne misbrug eller angreb, cyberangreb) og deres rolle med hensyn til at mindske sikkerhedsbrud

g. passende fysiske sikkerhedsforanstaltninger (f.eks. CCTV, tyverialarm, sikkerhedsdøre), der forebygger uautoriseret fysisk adgang til kritiske og følsomme IKT-systemer (f.eks. datacentre)

h. sikkerhedsforanstaltninger til beskyttelse af IKT-systemerne mod angreb fra internettet (dvs. cyberangreb) eller andre eksterne netværk (f.eks. traditionelle telekomforbindelser eller forbindelser til betroede partnere). De kompetente myndigheder bør undersøge, om instituttets rammer tager højde for:

    i. en proces og løsninger, der fastholder en fuldstændig og ajourført lagerliste og oversigt over alle de udadvendte netværksforbindelsespunkter (f.eks. websteder, internetapplikationer, WIFI, fjernadgang), hvorigennem tredjeparter kan bryde ind i de interne IKT-systemer

    ii. nøje styrede og overvågede sikkerhedsforanstaltninger (f.eks. firewalls, proxyservere, mailtransmissioner, virus- og indholdsscannere), som skal sikre ind- og udgående netværkstrafik (f.eks. e-mail) og udadgående netværksforbindelser, hvorigennem tredjeparter kan bryde ind i de interne IKT-systemer

iii. processer og løsninger, der sikrer websider og applikationer, der kan angribes direkte fra internettet og/eller uden for, som kan tjene som adgangspunkt til de interne IKT-systemer. Generelt omfatter dette en kombination af anerkendte, sikre udviklingsprocesser, IKT-systemhardening og sårbarhedsscanning og/eller implementering af yderligere sikkerhedsløsninger som f.eks. applikationsfirewalls og/eller systemer til intrusion detection (IDS) og/eller intrusion prevention (IPS)

iv. periodiske sikkerhedspenetrationstest for at vurdere effektiviteten af de implementerede cyber- og interne IKT-sikkerhedsforanstaltninger og -processer. Disse test skal gennemføres af medarbejdere og/eller eksterne eksperter med den nødvendige ekspertise, med dokumenterede testresultater og konklusioner, som indberettes til den daglige ledelse og/eller ledelsesorganet. Hvor det er nødvendigt og anvendeligt, bør instituttet af disse test lære, hvor de kan forbedre sikkerhedskontroller og -processer yderligere og/eller opnå bedre sikring af deres effektivitet.

c) Kontrol til styring af væsentlige IKT-ændringsrisici

56. De kompetente myndigheder bør vurdere, om instituttet har effektive rammer på plads til at identificere, forstå, måle og mindske IKT-ændringsrisici, som står i forhold til arten, omfanget og kompleksiteten af instituttets aktiviteter og instituttets IKT-risikoprofil. Instituttets rammer bør omfatte risici forbundet med udvikling, test og godkendelse af IKT-systemændringer, herunder udvikling eller ændring af software, inden de migreres til produktionsmiljøet samt sikre en passende styring af IKT-livscyklussen. De kompetente myndigheder bør i forbindelse med denne vurdering navnlig tage hensyn til, om rammerne tager højde for:

a. dokumenterede processer for forvaltning og kontrol af ændringer til IKT-systemer (f.eks. konfiguration og patchstyring) og data (f.eks. fejlretning eller datarettelser), sikring af passende inddragelse af IKT-risikostyringsfunktionen i forbindelse med vigtige IKT-ændringer, som kan påvirke instituttets risikoprofil og -eksponering

b. specifikationer vedrørende funktionsadskillelse (”segregation of duties”, SoD) i de forskellige faser af de implementerede IKT-ændringsprocesser (f.eks. udformning og udvikling af løsninger, test og godkendelse af ny software og/eller ændringer, migration og implementering i produktionsmiljøet og fejlretning) med fokus på de implementerede løsninger og funktionsadskillelse til styring og kontrol af ændringer i produktions-IKT-systemer og -data for IKT-medarbejdere (f.eks. udviklere, IKT-systemadministratorer, databaseadministratorer) eller andre parter (f.eks. brugere, leverandører)

c. testmiljøer, der på passende vis afspejler produktionsmiljøet

d. en fortegnelse over eksisterende applikationer og IKT-systemer i produktionsmiljøet samt test- og udviklingsmiljøet, så de pågældende ændringer (f.eks. versionsopdateringer eller opgraderinger, systemrettelser, konfigurationsændringer) kan styres, gennemføres og overvåges rigtigt for de involverede IKT-systemer

e. en proces til overvågning og styring af IKT-systemers livscyklus for at sikre, at de fortsat opfylder og støtter de faktiske forretnings- og risikostyringskrav, og for at sikre, at de anvendte IKT-løsninger og

-systemer fortsat støttes af leverandøren, og at dette ledsages af passende procedurer til softwareudviklingscyklussen (SDLC)

f. kontrol af softwarekildekode og passende procedurer til at forebygge uautoriserede ændringer i kildekoden til software som udvikles internt

g. en proces for sikkerheds- og sårbarhedsscreening af nye eller væsentlige ændrede IKT-systemer og -software, inden de frigives til produktion og eksponeres for mulige cyberangreb

h. en proces og løsninger, der forebygger uautoriseret eller utilsigtet frigivelse af fortrolige oplysninger ved udskiftning, arkivering, kassering eller ødelæggelse af IKT-systemer

i. en uafhængig gennemgangs- og valideringsproces, der skal mindske risikoen for menneskelige fejl, når der foretages ændringer til IKT-systemerne, som kan have en stor negativ indvirkning på instituttets tilgængelighed, kontinuitet eller sikkerhed (f.eks. vigtige ændringer til firewallkonfigurationen) eller instituttets sikkerhed (f.eks. ændringer til firewalls).

d) Kontrol til styring af væsentlige IKT-dataintegritetsrisici

57. De kompetente myndigheder bør vurdere om instituttet har effektive rammer på plads til at identificere, forstå, måle og mindske IKT-dataintegritetsrisici, som står i forhold til arten, omfanget og kompleksiteten af instituttets aktiviteter og IKT-risikoprofil. Instituttets rammer bør tage højde for risici relateret til bevarelse af integriteten af de data, som er lagret og behandles i IKT-systemerne. De kompetente myndigheder bør i forbindelse med denne vurdering navnlig tage hensyn til, om der i rammerne tages højde for:

a. en politik, der definerer roller og ansvar for styring af dataintegriteten i IKT-systemerne (f.eks. dataarkitekter, dataansvarlige[6], databeskyttere[7], dataejere/-forvaltere[8]) og vejleder om, hvilke data som er kritiske ud fra et dataintegritetsperspektiv og hvilke data der bør være underlagt specifikke IKT-kontroller (f.eks. kontroller for automatiserede inputvalideringer, dataoverførsler, afstemninger mv.) eller -gennemgange (f.eks. kontrol af kompatibilitet med dataarkitekturen) i de forskellige faser af IKT-dataenes livscyklus

b. en dokumenteret dataarkitektur, datamodel og/eller datarelationer/-strukturer, som er valideret med relevante forretnings- og it-interessenter i forhold til at støtte den nødvendige datakonsistens på tværs af IKT-systemer og sikre, at dataarkitekturen, datamodellen og/eller datarelationerne/-strukturerne fortsat er tilpasset forretnings- og risikostyringsbehov

c. en politik vedrørende tilladt brug af slutbrugercomputere, navnlig vedrørende identifikation, registrering og dokumentation af vigtige computerløsninger for slutbrugere (f.eks. ved behandling af vigtige data) og de forventede sikkerhedsniveauer med hensyn til at forebygge uautoriserede ændringer, både i selve værktøjet samt af de data, der er lagret i det

[6] En dataansvarlig er ansvarlig for databehandling og -brug.

[7] En databeskytter er ansvarlig for sikker opbevaring, transport og lagring af data.

[8] En dataforvalter er ansvarlig for forvaltningen og egnetheden af dataelementer – både indhold og metadata.

d. dokumenterede processer til håndtering af undtagelser med hensyn til at løse identificerede IKT-dataintegritetsproblemer efter deres alvor og følsomhed.

58. Med hensyn til institutter, der er underlagt tilsyn under BCBS 239-principperne for effektiv indsamling af risikodata og risikorapportering[9], bør de kompetente myndigheder gennemgå instituttets risikoanalyse af risikorapporteringen og dataindsamlingsmulighederne sammenlignet med principperne og den udarbejdede dokumentation under hensyntagen til gennemførelsestiden og overgangsordningerne i disse principper.

e) Kontrol til styring af væsentlige IKT-outsourcingrisici

59. De kompetente myndigheder bør vurdere, om instituttets outsourcingstrategi i overensstemmelse med kravene i CEBS's outsourcingretningslinjer (2006) og i tillæg til kravene i pkt. 85, litra d), i EBA's SREP-retningslinjer på passende vis finder anvendelse på IKT-outsourcing, herunder intern outsourcing af IKT-tjenester i koncernen. I forbindelse med vurderingen af IKT-outsourcingrisici bør de kompetente myndigheder tage højde for, at IKT-outsourcingrisici også kan dækkes som en del af vurderingen af iboende operationelle risici i pkt. 240, litra j), i EBA's SREP-retningslinjer for at undgå dobbeltarbejde eller dobbelttælling.

60. De kompetente myndigheder bør navnlig vurdere, om instituttet har effektive rammer på plads til at identificere, forstå og måle IKT-outsourcingrisici og navnlig kontroller og et kontrolmiljø til reduktion af risici i forbindelse med væsentlige outsourcede IKT-tjenester, som står i forhold til instituttets størrelse, aktiviteter og IKT-risikoprofil og omfatter:

a. en vurdering af IKT-outsourcingens indvirkning på instituttets risikostyring i forbindelse med brug af leverandører (dvs. leverandører af cloudservices) og deres tjenester i indkøbsprocessen, som den daglige ledelse eller ledelsesorganet har dokumenteret og taget højde for i beslutningen om at outsource tjenester. Instituttet bør gennemgå leverandørens IKT-risikostyringspolitikker og IKT-kontroller og -kontrolmiljø for at sikre, at de opfylder instituttets interne risikostyringsmål og risikovillighed. Denne gennemgang bør ajourføres løbende i outsourcingperioden under hensyntagen til kendetegnene ved de outsourcede tjenester

b. overvågning af IKT-risiciene ved de outsourcede tjenester i outsourcingperioden som led i instituttets risikostyring, der indgår i instituttets IKT-risikostyringsrapportering (f.eks. rapportering om den forretningsmæssige kontinuitet, sikkerhedsrapportering)

c. overvågning og sammenligning af de modtagne serviceniveauer og de aftalte serviceniveauer, som bør indgå i outsourcingkontrakten eller serviceniveauaftalen (SLA) og

d. tilstrækkelige medarbejdere, ressourcer og kompetencer til at overvåge og styre IKT-risici fra de outsourcede tjenester.

[9] Basel Committee on Banking Supervision, Principles for effective risk data aggregation and risk reporting, januar 2013, findes online: http://www.bis.org/publ/bcbs239.pdf.

3.4 Opsummering af observationer og scoring

61. Efter ovennævnte vurdering bør de kompetente myndigheder danne sig en mening om instituttets IKT-risiko. Denne mening bør afspejles i en opsummering af observationer, som de kompetente myndigheder bør tage højde for, når de fastsætter en score for operationel risiko i tabel 6 i EBA's SREP-retningslinjer. De kompetente myndigheder bør basere deres mening på væsentlige IKT-risici under hensyntagen til følgende betragtninger, som skal indgå i den operationelle risikovurdering:

a. Risikobetragtninger

   i. Instituttets IKT-risikoprofil og eksponeringer
   ii. de identificerede kritiske IKT-systemer og -tjenester og
   iii. væsentligheden af IKT-risiko vedrørende kritiske IKT-systemer.

b. Betragtninger om styring og kontrol

   i. Om der er overensstemmelse mellem instituttets IKT-risikostyringspolitik og -strategi og dets generelle strategi og risikovillighed.
   ii. Om den organisatoriske struktur for IKT-risikostyring er robust og baseret på klare ansvarsområder og en klar opgavefordeling mellem risikoejere og styrings- og kontrolfunktioner.
   iii. Om systemerne til IKT-risikomåling, -overvågning og -rapportering er passende.
   iv. Om kontrolrammerne for væsentlige IKT-risici er forsvarlige.

62. Hvis de kompetente myndigheder vurderer, at IKT-risikoen er væsentlig, og de kompetente myndigheder beslutter at vurdere og score denne risiko som en underkategori af operationel risiko, indeholder nedenstående tabel (tabel 1) betragtninger vedrørende IKT-risikoscore.

Tabel 1: Tilsynsmæssige betragtninger vedrørende fastsættelse af IKT-risikoscore

Risikoscore	Tilsynsmæssig vurdering	Betragtninger om iboende risiko	Betragtninger om tilstrækkelig styring og kontrol
1	Der er ingen mærkbar risiko for væsentlig tilsynsmæssig påvirkning af instituttet som følge af den iboende risiko samt risikostyringen og -kontrollen.	• De informationskilder, som skal overvejes i pkt. 37, afslørede ingen betydelige IKT-risikoeksponeringer. • Arten af instituttets IKT-risikoprofil sammen med gennemgangen af de kritiske IKT-systemer og væsentlige IKT-risici for IKT-systemer og -tjenester har ikke afsløret væsentlige IKT-risici.	
2	Der er en lav risiko for væsentlig	• De informationskilder, som skal overvejes i pkt. 37, afslørede	

	tilsynsmæssig påvirkning af instituttet som følge af den iboende risiko samt risikostyringen og -kontrollen.	ingen betydelige IKT-risikoeksponeringer. • Arten af instituttets IKT-risikoprofil sammen med gennemgangen af de kritiske IKT-systemer og væsentlige IKT-risici for IKT-systemer og -tjenester afslørede en begrænset IKT-risikoeksponering (f.eks. ikke mere end to ud af fem af de foruddefinerede IKT-risikokategorier).	• Instituttets IKT-risikopolitik og -strategi stemmer overens med den overordnede strategi og risikovillighed. • Den organisatoriske struktur i relation til IKT-risici er robust og baseret på klare ansvarsområder og en klar opgavefordeling mellem risikoejere og styrings- og kontrolfunktioner. • Systemerne til måling, overvågning og rapportering af IKT-risici er passende. • Kontrolrammerne for IKT-risici er forsvarlige.
3	Der er en mellemhøj risiko for væsentlig tilsynsmæssig påvirkning af instituttet som følge af den iboende risiko samt risikostyringen og -kontrollen.	• De informationskilder, som skal overvejes i pkt. 37, afslørede tegn på mulige væsentlige IKT-risikoeksponeringer. • Arten af instituttets IKT-risikoprofil sammen med gennemgangen af de kritiske IKT-systemer og væsentlige IKT-risici for IKT-systemer og -tjenester afslørede en forhøjet IKT-risikoeksponering (f.eks. tre eller flere ud af fem af de foruddefinerede IKT-risikokategorier).	
4	Der er en høj risiko for væsentlig tilsynsmæssig påvirkning af instituttet som følge af den iboende risiko samt risikostyringen og -kontrollen.	• De informationskilder, som skal overvejes i pkt. 37, afslørede flere tegn på væsentlige IKT-risikoeksponeringer. • Arten af instituttets IKT-risikoprofil sammen med gennemgangen af de kritiske IKT-systemer og væsentlige IKT-risici for IKT-systemer og -tjenester afslørede en høj IKT-risikoeksponering (f.eks. fire eller fem ud af fem af de foruddefinerede IKT-risikokategorier).	

Bilag – IKT-risikoklassificering

5 IKT-risikokategorier med en ikke-udtømmende liste over IKT-risici med potentielt høj alvorlighed og/eller påvirkning af drift, omdømme eller økonomi

IKT-risikokategorier	IKT-risici (ikke-udtømmende[10])	Risikobeskrivelse	Eksempler
IKT-tilgængelighed og beredskabsrisici	Utilstrækkelig kapacitetsstyring	Mangel på ressourcer (f.eks. hardware, software, medarbejdere, leverandører) kan medføre, at tjenesten ikke i tilstrækkelig grad opfylder de forretningsmæssige behov, og kan forårsage systemafbrydelser, nedbrud og/eller operationelle fejl.	• Kapacitetsmangel kan påvirke transmissionshastigheder og netværkstilgængelighed (internettet) for tjenesten som f.eks. netbank. • Mangel på medarbejdere (interne eller hos tredjeparter) kan medføre systemafbrydelser og/eller operationelle fejl.
	IKT-systemfejl	Manglende tilgængelighed på grund af hardwarefejl.	• Fejl/funktionsfejl i lagerplads (harddisk), server eller andet IKT-udstyr som følge af f.eks. manglende vedligeholdelse.
		Manglende tilgængelighed på grund af softwarefejl eller andre fejl.	• Uendeligt loop i anvendelsen af software forhindrer gennemførelse af transaktioner. • Afbrydelser som følge af fortsat brug af forældede IKT-systemer og løsninger, der ikke længere opfylder nuværende krav til tilgængelighed og modstandsdygtighed, understøttes ikke længere af sælgerne.
	Utilstrækkelig IKT-beredskabs- og -katastrofeberedskabsplaner.	Fejl i planlagt IKT-tilgængelighed og/eller kontinuitetsløsninger og/eller katastrofeberedskab (f.eks. datacenter til fallback), som aktiveres i forbindelse med en hændelse.	• Konfigurationsforskelle mellem det primære og sekundære datacenter kan medføre manglende kapacitet for fallback-datacentret med hensyn til at levere den planlagte kontinuitet i tjenesten.
	Ødelæggende og	Angreb med forskellige formål (f.eks. aktivisme,	• Distribuerede "denial of service"-angreb udføres

[10] IKT-risici fremgår under den risikokategori, som de påvirker mest, men de kan også påvirke andre risikokategorier

IKT-risikokategorier	IKT-risici (ikke-udtømmende[10])	Risikobeskrivelse	Eksempler
	destruktive cyberangreb	afpresning), som medfører en overbelastning af systemer og netværk og forhindrer brugerne i at få adgang til onlinetjenester på computeren.	også ved hjælp af en lang række computersystemer på internettet, som kontrolleres af en hacker, der sender store mængder tilsyneladende lovlige anmodninger til internetbaserede tjenester (f.eks. netbank).
IKT-sikkerhedsrisici	Cyberangreb og andre eksterne IKT-baserede angreb	Angreb gennemført fra internettet eller uden for netværk med forskellige formål (f.eks. svig, spionage, aktivisme/sabotage, cyberterrorisme) ved hjælp af forskellige teknikker (f.eks. social manipulation, indtrængningsangreb gennem udnyttelse af sårbarheder, anvendelse af skadelig software), der overtager kontrollen med interne IKT-systemer.	Forskellige typer angreb: • APT (Advanced Persistent Threat), hvor der tages kontrol med interne systemer, eller der stjæles oplysninger (f.eks. oplysninger vedrørende identitetstyveri, kreditkortoplysninger). • Skadelig software (f.eks. ransomware), som krypterer data med henblik på afpresning. • Inficering af interne it-systemer med trojanske heste med henblik på at skjule skadelige systemaktioner. • Udnyttelse af IKT-system og/eller (web)applikationssårbarheder (f.eks. SQL-injektion ...) for at få adgang til det interne IKT-system.
		Hacking af svigagtige betalingstransaktioner ved indbrud i eller omgåelse af sikkerheden i netbank- eller betalingstjenester og/eller ved at angribe og udnytte sikkerhedssårbarheder i et instituts interne betalingssystemer.	• Angreb mod netbank- eller betalingstjenester med det formål at foretage uautoriserede transaktioner. • Oprettelse og udsendelse af svigagtige betalingstransaktioner fra et instituts interne betalingssystemer (f.eks. svigagtige SWIFT-meddelelser).
		Hacking af svigagtige sikkerhedstransaktioner ved indbrud i eller omgåelse af sikkerheden i netbanktjenester, der også giver adgang til kundernes sikkerhedskonti.	• "Pump and dump"-angreb, hvor angriberne får adgang til kundernes værdipapirkonti via netbank og placerer svigagtige købs- eller salgsordrer for at påvirke markedspriserne og/eller få en gevinst baseret på tidligere etablerede værdipapirpositioner.
		Angreb på kommunikationsforbindelser og alle former for samtaler eller IKT-systemer med det formål at	• Aflytning/indsamling af ubeskyttede transmissioner af ægthedskontroldata i tekstform.

IKT-risikokategorier	IKT-risici (ikke-udtømmende[10])	Risikobeskrivelse	Eksempler
		indsamle oplysninger og/eller begå svig.	
	Utilstrækkelig intern IKT-sikkerhed	Uautoriseret adgang til kritiske IKT-systemer internt i instituttet til forskellige formål (f.eks. svig, gennemføre og skjule svindelaktiviteter, datatyveri, aktivisme/sabotage) med en række forskellige teknikker (f.eks. misbrug og/eller eskalerende privilegier, identitetstyveri, social manipulation, udnyttelse af sårbarheder i IKT-systemer, anvendelse af skadelig software).	• Installation af keylogger (til registrering af tastaturanslag) med henblik på at stjæle bruger-ID og adgangskoder for at få uautoriseret adgang til fortrolige data og/eller begå svig. • Bryde/gætte svage adgangskoder for at opnå ulovlige eller højere adgangsrettigheder. • Systemadministrator bruger operativsystemer eller databasefunktioner (til direkte databaseændringer) til at begå svig.
		Uautoriserede IKT-manipulationer som følge af utilstrækkelig IKT-adgangsstyringsprocedurer og -praksis.	• Manglende deaktivering eller sletning af unødvendige konti, som giver uautoriseret adgang til IKT-systemer, f.eks. konti tilhørende personale, som har fået nye funktioner og/eller har forladt instituttet, herunder gæster og leverandører, som ikke længere har behov for adgang. • For omfattende adgangsrettigheder og privilegier, der giver uautoriseret adgang og/eller gør det muligt at skjule svindelaktiviteter.
		Sikkerhedstrusler som følge af manglende opmærksomhed på sikkerhed, hvorved medarbejderne ikke forstår, undlader eller undgår at følge IKT-sikkerhedspolitikker og -procedurer.	• Medarbejdere, der forledes til at yde bistand til et angreb (f.eks. social manipulation). • Dårlig praksis med hensyn til brugeridentifikation: deling af adgangskoder, brug af adgangskoder, som er lette at gætte, brug af samme adgangskode til mange forskellige formål mv. • Lagring af ikke-krypterede fortrolige oplysninger på bærbare pc'er og andre datalagringsløsninger (f.eks. USB-nøgler), som kan mistes eller blive stjålet.
		Uautoriseret lagring eller overførsel af fortrolige oplysninger uden for instituttet.	• Personer, der stjæler eller bevidst lækker eller smugler fortrolige oplysninger ud til uautoriserede personer eller offentligheden.
	Utilstrækkelig	Misbrug eller tyveri af IKT-aktiver via fysisk adgang, der	• Fysisk indbrud i kontorbygninger og/eller

IKT-risikokategorier	IKT-risici (ikke-udtømmende[10])	Risikobeskrivelse	Eksempler
	fysisk IKT-sikkerhed	forårsager skader, tab af aktiver eller data eller muliggør andre trusler.	datacentre for at stjæle IKT-udstyr (f.eks. computere, bærebare pc'er, lagringsløsninger) og/eller kopiere data ved fysisk at tilgå IKT-systemer.
		Bevidst eller tilfældig beskadigelse af fysiske IKT-aktiver som følge af terrorisme, ulykker eller utilsigtet/fejlagtig håndtering fra instituttets medarbejderes og/eller tredjeparters (leverandører, reparatører) side.	• Fysisk terrorisme (f.eks. terrorbomber) eller sabotage af IKT-aktiver. • Ødelæggelse af datacentre på grund af brand, vandskade eller andre faktorer.
		Utilstrækkelig fysisk beskyttelse mod naturkatastrofer, som medfører hel eller delvis ødelæggelse af IKT-systemer/datacentre.	• Jordskælv, ekstrem varme, orkaner, voldsomme snestorme, oversvømmelser, brand, lynnedslag.
IKT-ændringsrisici	Utilstrækkelig kontrol med IKT-systemændringer og IKT-udvikling	Hændelser som følge af uopdagede fejl eller sårbarheder som følge af en ændring (f.eks. uventede virkninger af en ændring eller en dårligt håndteret ændring som følge af manglende test eller forkert ændringsstyringspraksis) i f.eks. software, IKT-systemer og data.	• Utilstrækkeligt testet software, der ligges i produktionsløjet, eller konfigurationsændringer med uventede skadelige virkninger på data (f.eks. ødelæggelse, sletning) og/eller på IKT-systemets ydeevne (f.eks. nedbrud, dårligere ydeevne). • Ukontrollerede ændringer i IKT-systemer eller data i produktionsmiljøet. • Dårligt sikrede IKT-systemer og internetapplikationer, der ligges i produktionsmiljøet, og som giver hackere mulighed for at angribe internettjenesterne og/eller bryde ind i interne IKT-systemer. • Ukontrollerede ændringer i kildekoden i internt udviklet software. • Utilstrækkelig test på grund af utilstrækkelige testmiljøer.
	Utilstrækkelig IKT-arkitektur	En svag IKT-arkitektur ved design, opbygning og vedligeholdelse af IKT-systemer (f.eks. software, hardware, data) kan over tid føre til komplekse, svære, omkostningstunge og stive IKT-systemer, der ikke længere er tilstrækkeligt tilpasset de	• Utilstrækkeligt styrede ændringer i IKT-systemer, software og/eller data over en længere periode, der medfører, at komplekse, heterogene IKT-systemer og arkitekturer er vanskelige at styre, og som har mange skadelige virkninger på forretningsdriften og

IKT-risikokategorier	IKT-risici (ikke-udtømmende[10])	Risikobeskrivelse	Eksempler
		forretningsmæssige behov og har mangler i forhold til de faktiske risikostyringskrav.	risikostyringen (f.eks. manglende fleksibilitet og smidighed, IKT-hændelser og -fejl, store driftsomkostninger, ringere IKT-sikkerhed og -modstandsdygtighed, dårligere datakvalitet og rapporteringsmuligheder). • Overdreven tilpasning og udvidelse af kommercielle softwarepakker med internt udviklet software, som gør det umuligt senere hen at frigive og opgradere den kommercielle software og medfører risiko for, at sælger ikke længere understøtter den.
	Utilstrækkelig livscyklus og patchstyring	Manglende vedligeholdelse af fortegnelse over alle IKT-aktiver til støtte for og kombineret med forsvarlige livscyklus- og patchstyringspraksisser. Dette medfører utilstrækkelig patchning (og dermed mere sårbare) og forældede IKT-systemer, der muligvis ikke støtter forretnings- og risikostyringsbehovene.	• Ikke-patchede og forældede IKT-systemer, der kan have en negativ virkning på forretnings- og risikostyringen (f.eks. manglende fleksibilitet og smidighed, IKT-nedbrud, svag IKT-sikkerhed og modstandsdygtighed).
IKT-dataintegritetsrisici	Dysfunktionel IKT-databehandling eller -håndtering	På grund af system-, kommunikations- og/eller applikationsfejl eller fejlagtigt gennemførte datatransaktions-, overførsels- og belastningsprocesser (ETL) kan data blive ødelagt eller gå tabt.	• IT-systemfejl i batchbehandling, der giver ubalancer i kundernes bankkonti. • Forkert udførte forespørgsler. • Datatab på grund af fejl ved datareplikation (backup).
	Dårligt designede datavalideringskontroller i IKT-systemer.	Fejl i forbindelse med manglende eller ineffektive automatiske datainput- og acceptkontroller (f.eks. til anvendte tredjepartsdata), dataoverførsels-, behandlings- og outputkontroller i IKT-systemerne (f.eks. inputvaliditetskontrol, dataafstemninger).	• Utilstrækkelig eller ugyldig formatering/validering af datainput i applikationer og/eller brugergrænseflader. • Manglende dataafstemningskontrol af produceret output • Manglende kontrol med gennemførte dataudtrækningsprocesser (f.eks. databasesøgninger), der medfører fejlbehæftede data. • Brug af fejlbehæftede eksterne data.
	Dårligt	Datafejl som følge af manglende kontrol med, om	• Udviklere eller databaseadministratorer, der direkte

IKT-risikokategorier	IKT-risici (ikke-udtømmende[10])	Risikobeskrivelse	Eksempler
	kontrollerede dataudvekslinger i produktions-IKT-systemer.	datamanipulationer udført i forbindelse med produktionen af IKT-systemer er korrekte og berettigede.	tilgår og ændrer data i produktions-IKT-systemer på en ikke-kontrolleret måde, f.eks. i tilfælde af en IKT-hændelse.
	Dårligt designet og/eller styret dataarkitektur, datastrømme, datamodeller eller data struktur/relationer.	Dårligt styret dataarkitektur, datamodeller, datastrømme eller datastruktur/-relationer kan medføre flere versioner af samme data på tværs af IKT-systemerne, som ikke længere er konsekvente på grund af forskelligt anvendte datamodeller eller datadefinitioner og/eller forskelle i den underliggende datagenererings- og ændringsproces.	• Forskellige kundedatabaser pr. produkt eller forretningsenhed med forskellige datadefinitioner og -områder, som medfører uafstemte og vanskeligt sammenlignelige kundedata i hele det finansielle institut eller koncernen.
IKT-outsourcingrisici	Utilstrækkelig modstandsdygtighed hos tredjeparter eller andre koncernenheder.	Manglende tilgængelighed af kritisk outsourcede IKT-tjenester, telekommunikationstjenester og forsyningsvirksomheder. Tabte eller ødelagte kritiske/følsomme data, som var betroet leverandøren	• Manglende tilgængelighed af centrale tjenester som følge af fejl i leverandørers (outsourcede) IKT-systemer eller -applikationer. • Afbrydelse af telekommunikationsforbindelser. • Manglende strømforsyning.
	Utilstrækkelig styring af outsourcing.	Større nedbrud eller fejl i tjenester som følge af ineffektive beredskabs- eller kontrolprocesser hos den outsourcede leverandør. Ineffektiv forvaltning af outsourcing kan medføre manglende færdigheder og muligheder for fuldt ud at identificere, vurdere, mindske og overvåge IKT-risici og kan begrænse institutternes operationelle kapacitet.	• Dårlige procedurer for håndtering af hændelser, kontraktlige kontrolmekanismer og garantier indbygget i leverandøraftalen, som øger afhængigheden af tredjeparter og sælgere. • Utilstrækkelige ændringsstyringskontroller vedrørende leverandørens IKT-miljø kan medføre en kraftig forringelse af tjenesten, eller at de helt bryder ned.
	Utilstrækkelig sikkerhed hos tredjeparter eller andre koncernenheder.	Hacking af tredjepartsleverandørers IKT-systemer, som direkte påvirker de outsourcede tjenester eller kritiske/fortrolige data lagret hos leverandøren. Leverandørens medarbejdere får uautoriseret adgang til kritiske/følsomme data lagret hos leverandøren.	• Kriminelle eller terroristers hacking af leverandører som indgangspunkt til instituttets IKT-systemer eller for at få adgang til/ødelægge kritiske eller følsomme data, som er lagret hos leverandøren. • Ansatte hos leverandører, der i ond hensigt forsøger at stjæle og sælge følsomme oplysninger.