Riktlinjer

EBA/GL/2019/04

den 28 november 2019

EBA:s riktlinjer för hantering av IKT-risker och säkerhetsrisker

Efterlevnad 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 ska de behöriga myndigheterna och finansinstituten med alla tillgängliga medel söka följa riktlinjerna.

2. Av riktlinjerna framgår EBA:s 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 institut.

Rapporteringskrav

3. Enligt artikel 16.3 i förordning (EU) nr 1093/2010 ska de behöriga myndigheterna meddela EBA att de följer eller tänker följa dessa riktlinjer, eller i annat fall, senast den [dd.mm.åååå], ange skälen till att de inte gör det. 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/2019/04”. Anmälningar ska lämnas in av personer som har befogenhet att rapportera om hur reglerna efterlevs på de behöriga myndigheternas vägnar. Eventuella förändringar av efterlevnadsstatus måste också rapporteras till EBA.

4. Anmälningarna kommer att offentliggöras på EBA:s webbplats i enlighet med artikel 16.3.

[1] Europaparlamentets och rådets förordning (EU) nr 1093/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska bankmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/78/EG (EUT L 331, 15.12.2010, s. 12).

Syfte, tillämpningsområde och definitioner

Syfte

5. Dessa riktlinjer utgår från bestämmelserna i artikel 74 i direktiv 2013/36/EU (CRD) om intern styrning och härrör från mandatet att utfärda riktlinjer enligt artikel 95. i direktiv (EU) 2015/2366 (PSD2).

6. Dessa riktlinjer anger de riskhanteringsåtgärder som ska vidtas av finansinstitut (enligt definitionen i avsnitt 9 nedan) i enlighet med artikel 74 i CRD-direktivet för att hantera sina IKT-risker och säkerhetsrisker för alla aktiviteter och som ska vidtas av betaltjänstleverantörer (enligt definitionen i avsnitt 9 nedan) i enlighet med artikel 95.1 i PSD2 för att hantera sina operativa risker och säkerhetsrisker (avsedda som 'IKT-risker och säkerhetsrisker') med avseende på de betaltjänster som de tillhandahåller. Dessa riktlinjer inkluderar krav på informationssäkerhet, bl.a. cybersäkerhet, i den mån informationen förvaras i IKT-system.

Tillämpningsområde

7. Dessa riktlinjer tillämpas på hantering av IKT-risker och säkerhetsrisker inom finansinstitut (enligt definitionen i avsnitt 9). I den mening som avses i dessa riktlinjer omfattar termen IKT-risker och säkerhetsrisker operativa risker och säkerhetsrisker enligt artikel 95 i PSD2 om tillhandahållande av betaltjänster.

8. För betaltjänstleverantörer (enligt definitionen i avsnitt 9) tillämpas dessa riktlinjer på deras tillhandahållande av betaltjänster i linje med den omfattning och det mandat som avses i artikel 95 i PSD2. För institut (enligt definitionen i avsnitt 9) tillämpas dessa riktlinjer på alla aktiviteter som de tillhandahåller.

Målgrupp

9. Dessa riktlinjer är avsedda för finansinstitut vilket i den mening som avses i dessa riktlinjer omfattar (1) betaltjänstleverantörer enligt definitionen i artikel 4.11 i PSD2 och (2) institut, det vill säga kreditinstitut och värdepappersföretag, enligt definitionen i punkt 3 av artikel 4.1 i förordning (EU) nr 575/2013. Dessa riktlinjer gäller även för behöriga myndigheter enligt definitionen i artikel 4.1.40 i förordning (EU) nr 575/2013, inbegripet Europeiska centralbanken med avseende på ärenden som rör de uppgifter som tilldelats den genom förordning (EU) nr 1024/2013, och för behöriga myndigheter enligt punkt i i artikel 4.2 i förordning (EU) nr 1093/2010.

Definitioner

10. Om inget annat anges har de termer som används och definieras i 2013/36/EU (CRD), förordning (EU) nr 575/2013 (CRR) och direktiv (EU) nr 2015/2366 (PSD2) samma innebörd i riktlinjerna. Dessutom gäller följande definitioner i dessa riktlinjer:

IKT-risk och säkerhetsrisk	Risk för förlust som beror på sekretessbrott, på att integriteten hos system och data inte fungerar, på att system och data är olämpliga eller otillgängliga, eller på oförmåga att ändra på det inom rimlig tid och till rimliga kostnader när miljö- eller verksamhetskraven förändras (dvs. smidighet).[2] Detta inkluderar säkerhetsrisker till följd av otillräckliga eller icke-funktionella interna processer eller externa händelser, bl.a. IT-attacker, eller otillräcklig fysisk säkerhet.
Ledningsorgan	a) För kreditinstitut och värdepappersföretag ska denna term ha samma betydelse som definitionen i punkt 7 av artikel 3.1 i direktiv 2013/36/EU. b) För betalinstitut eller institut för elektroniska pengar ska denna term avse direktörer eller personer som ansvarar för ledning av betalinstitut och institut för elektroniska pengar samt i förekommande fall personer som ansvarar för ledning av betaltjänstaktiviteter av betalinstitut och institut för elektroniska pengar. c) För betaltjänstleverantörer som avses i punkt c, e och f i artikel 1.1 i direktiv (EU) 2015/2366 ska denna term ha samma betydelse som i tillämplig unionslagstiftning eller nationell lagstiftning.
Operativa incidenter eller säkerhetsincidenter	En enskild händelse eller en serie av sammanhängande händelser som inte har planerats av finansinstitutet och som har eller sannolikt kommer att ha negativa effekter på tjänster vad gäller integritet, tillgänglighet, konfidentialitet och/eller autenticitet.
Verkställande ledning	a) För kreditinstitut och värdepappersföretag ska denna term ha samma betydelse som definitionen i punkt 9 av artikel 3.1 i direktiv 2013/36/EU. b) För betalningsinstitut och institut för elektroniska pengar avser denna term fysiska personer med beslutsfattande roller inom institutionen som är ansvariga mot ledningsorganet för institutets dagliga drift. c) För betaltjänstleverantörer som avses i punkt c, e och f i artikel 1.1 i direktiv (EU) 2015/2366 ska denna term ha samma

[2]Definition enligt EBA:s riktlinjer om gemensamma förfaranden och metoder för översyns- och utvärderingsprocessen av den 19 december 2014 (EBA/GL/2014/13) som har ändrats med EBA/GL/2018/03.

	betydelse som i tillämplig unionslagstiftning eller nationell lagstiftning.
Riskaptit	Den aggregerade risknivå och de risktyper som betaltjänstleverantörer och institut är villiga att ta inom ramen för sin riskkapacitet, i enlighet med sin affärsmodell, för att uppnå sina strategiska mål.
Revisionsfunktion	a) För kreditinstitut och värdepappersföretag följer revisionsfunktionen avsnitt 22 i EBA:s riktlinjer för intern styrning (EBA/GL/2017/11). b) För andra betaltjänstleverantörer utom kreditinstitut måste revisionsfunktionen vara oberoende inom eller av betaltjänstleverantören och den kan vara en intern och/eller en extern revisionsfunktion.
IKT-projekt	Ett projekt eller en del av ett projekt där IKT-system och -tjänster ändras, byts, avvecklas eller införs. IKT-projekt kan vara en del av bredare IKT- eller verksamhetsomvandlingsprogram.
Tredje part	En organisation som har ingått affärsförbindelser eller avtal med en enhet i syfte att tillhandahålla en produkt eller en tjänst[3].
Informationstillgång	En samling av information, antingen materiell eller immateriell, som är värd att skyddas.
IKT-tillgång	En programvaru- eller hårdvarutillgång som finns i affärsmiljön.
IKT-system[4]	IKT-struktur som en del av en mekanism eller ett sammanlänkat nät som stödjer ett finansinstituts verksamhet.
IKT-tjänster[5]	Tjänster som tillhandahålls av IKT-system till en eller flera interna eller externa användare. Detta omfattar till exempel inmatning av data, lagring av data, hantering av data och rapporteringstjänster, men även övervakning och tjänster för verksamhets- och beslutssupport.

[3]Definition enligt G7:s grunder för hantering av IT-risker för tredje part i finanssektorn.
[4]Definition enligt riktlinjer om IKT-riskbedömning inom ramen för översyns- och utvärderingsprocessen (ÖUP) (EBA/GL/2017/05).
[5]ibid.

Genomförande

Tillämpningsdatum

11. Dessa riktlinjer gäller från och med den 30 juni 2020.

Upphävande

12. Riktlinjerna för säkerhetsåtgärder för operativa risker och säkerhetsrisker (EBA/GL/2017/17) utfärdade 2017 upphävs av dessa riktlinjer från och med datumet för ikraftträdande av dessa riktlinjer.

Riktlinjer för hantering av IKT-risker och säkerhetsrisker

1.1. Proportionalitet

1. Alla finansinstitut ska efterleva bestämmelserna i dessa riktlinjer på ett sätt som är proportionerligt till och tar hänsyn till finansinstituts storlek, deras interna organisation samt karaktären, omfattningen, komplexiteten och risknivån av de tjänster och produkter som finansinstituten tillhandahåller eller avser att tillhandahålla.

1.2. Strategi och ledning

1.2.1. Styrning

2. Ledningsorganet ska tillse att finansinstitut har fastställt tillräcklig intern styrning och ett tillräckligt internt kontrollramverk för sina IKT-risker och säkerhetsrisker. Ledningsorganet ska fastställa tydliga roller och ansvarsområden för IKT-funktioner, hantering av informationssäkerhetsrisker och driftskontinuitet, inklusive för ledningsorganet och dess kommittéer.

3. Ledningsorganet ska tillse att finansinstituts personal är tillräckligt stor och kompetent för att kontinuerligt stödja finansinstitutens operativa IKT-behov och riskhanteringsprocesser för säkerhetsrisker samt för att säkerställa genomförande av deras IKT-strategi. Ledningsorganet ska tillse att den tilldelade budgeten är lämplig för att uppfylla kraven ovan. Vidare bör finansinstitut tillse att alla anställda, inklusive de som har nyckelbefattningar, årligen eller vid behov oftare får lämplig utbildning om IKT-risker och säkerhetsrisker, bl.a. om informationssäkerhet (se även avsnitt 1.4.7).

4. Ledningsorganet har det allmänna ansvaret för fastställande, godkännande och övervakning av finansinstituts IKT strategi som en del av deras allmänna affärsstrategi samt för framtagande av en effektiv riskhanteringsram för IKT-risker och säkerhetsrisker.

1.2.2. Strategi

5. IKT-strategin ska stämma överens med finansinstituts allmänna affärsstrategi och den ska definiera följande:

    a) Hur finansinstituts IKT ska utvecklas för att effektivt stödja och delta i deras affärsstrategi, bl.a. utveckling av den organisatoriska strukturen, ändringar i IKT-system och nyckelberoenden gentemot tredje parter.
    b) Den planerade strategin och utvecklingen av IKT-arkitekturen, bl.a. tredjepartsberoenden.
    c) Tydliga informationssäkerhetsmål som fokuserar på IKT-system, IKT-tjänster, personal och processer.

6. Finansinstitut bör ta fram uppsättningar av handlingsplaner som innehåller åtgärder som ska vidtas för att uppnå IKT-strategins mål. Dessa ska meddelas till all relevant personal (bl.a. uppdragstagare och tredjepartsleverantörer i tillämpliga och förekommande fall). Handlingsplanerna ska ses över periodiskt för att säkerställa att de är relevanta och lämpliga. Finansinstitut ska även ta fram processer för övervakning och mätning av effektiviteten av genomförandet av deras IKT-strategi.

1.2.3. Användning av tredjepartsleverantörer

7. Utan att det påverkar tillämpningen av EBA:s riktlinjer för outsourcing (EBA/GL/2019/02) och artikel 19 i PSD2 ska finansinstitut säkerställa effektiviteten hos de riskreducerande åtgärderna så som de definieras i respektive finansinstituts riskhanteringsramverk (inklusive åtgärder fastställda i dessa riktlinjer) när operativa funktioner för betaltjänster och/eller IKT-tjänster och IKT-system av någon aktivitet utkontrakteras, bl.a. till koncernenheter, eller vid användning av tredje parter.

8. För att säkerställa kontinuiteten av IKT-tjänster och IKT-system ska finansinstitut tillse att avtal och servicenivåavtal (både för normala förhållanden och vid störningar i tjänsten – se även avsnitt 1.7.2) med leverantörer (kontraktstagande leverantörer, koncernenheter eller tredjepartsleverantörer) inkluderar följande:

    a) Lämpliga och proportionerliga informationssäkerhetsrelaterade mål och åtgärder, bl.a. krav såsom minimikrav på cybersäkerhet; specifikationer för livscykelhantering av finansinstitutets data; eventuella krav på datakryptering, nätsäkerhet och säkerhetsövervakningsprocesser samt lokalisering av datacentraler.
    b) Hanteringsrutiner för operativa incidenter och säkerhetsincidenter, bl.a. eskalering och rapportering.

9. Finansinstituten bör kontrollera och erhålla intyg på dessa leverantörers efterlevnad av finansinstitutets säkerhetsmål, -mått och -resultatmått.

1.3. Ramverk för hantering av operativa risker och säkerhetsrisker

1.3.1. Organisation och mål

10. Finansinstitut bör identifiera och hantera sina IKT-risker och säkerhetsrisker. IKT-funktionen (-funktionerna) som ansvarar för IKT-system, IKT-processer och säkerhetsverksamhet ska ha fastställda lämpliga processer och kontroller för att säkerställa att alla risker identifieras, analyseras, mäts, övervakas, hanteras, rapporteras och hålls inom gränserna för finansinstitutets riskaptit och att de projekt och system som de tillhandahåller och de aktiviteter som de utför uppfyller externa och interna krav.

11. Finansinstitut bör tilldela ansvaret för hantering av och tillsyn över IKT-risker och säkerhetsrisker till en kontrollfunktion i enlighet med kraven i avsnitt 19 i EBA:s riktlinjer för intern styrning (EBA/GL/2017/11). Finansinstitut bör säkerställa kontrollfunktionens oberoende och objektivitet genom att på ett lämpligt sätt skilja av den från IKT-verksamhetsprocesser. Denna kontrollfunktion är direkt ansvarig mot ledningsorganet och ansvarar för övervakning och kontroll av efterlevnaden av ramverket för hantering av IKT-risker och säkerhetsrisker. Kontrollfunktionen ska tillse att IKT-risker och säkerhetsrisker identifieras, mäts, bedöms, övervakas och rapporteras. Finansinstitut bör tillse att denna kontrollfunktion inte ansvarar för någon internrevision.

    Enligt den riskbaserade metoden ska den interna revisionsfunktionen ha tillräcklig kapacitet för oberoende översyn och objektiv verifiering av att ett finansinstituts samtliga IKT- och säkerhetsrelaterade aktiviteter och enheter efterlever finansinstitutets policyer och rutiner och följer externa krav i enlighet med avsnitt 22 i EBA:s riktlinjer för intern styrning (EBA/GL/2017/11).

12. Finansinstitut bör definiera och tilldela nyckelroller och -ansvarsområden samt lämpliga rapporteringslinjer för att ramverket för hantering av IKT-risker och säkerhetsrisker ska vara effektivt. Detta ramverk bör fullständigt integreras i och bringas i överensstämmelse med finansinstitutets allmänna riskhanteringsprocesser.

13. Ramverket för hantering av IKT-risker och säkerhetsrisker ska inkludera fastställda processer för att,

    a) fastställa riskaptiten för IKT-risker och säkerhetsrisker i enlighet med finansinstitutets riskaptit,
    b) identifiera och bedöma de IKT-risker och säkerhetsrisker som ett finansinstitut utsätts för,
    c) definiera riskreduceringsåtgärder, bl.a. kontroller, för att reducera IKT-risker och säkerhetsrisker,
    d) övervaka effektiviteten av dessa åtgärder och antalet rapporterade incidenter, inklusive för betaltjänstleverantörer incidenter rapporterade i enlighet med artikel 96 i PSD2 som påverkar IKT-relaterade aktiviteter, samt att vid behov vidta åtgärder för att korrigera åtgärderna,
    e) rapportera till ledningsorganet om IKT-riskerna, säkerhetsriskerna och kontrollerna,

f) identifiera och bedöma om det finns några IKT-risker och säkerhetsrisker som härrör från en eventuell omfattande ändring i IKT-systemet eller IKT-tjänster, processer eller rutiner och/eller efter en eventuell betydande operativ incident eller säkerhetsincident.

14. Finansinstitut bör tillse att ramverket för hantering av IKT-risker och säkerhetsrisker dokumenteras och att den förbättras kontinuerligt utifrån tidigare erfarenheter från dess genomförande och övervakning. Ramverket för hantering av IKT-risker och säkerhetsrisker ska godkännas och minst en gång om året ses över av ledningsorganet.

1.3.2. Identifiering av funktioner, processer och tillgångar

15. Finansinstitut bör identifiera, ta fram och upprätthålla uppdaterad kartläggning av sina verksamhetsfunktioner, roller och stödprocesser för att identifiera vikten av var och en av dessa och deras inbördes beroenden avseende IKT-risker och säkerhetsrisker.

16. Vidare bör finansinstitut identifiera, ta fram och upprätthålla uppdaterad kartläggning av informationstillgångar som stödjer finansinstitutets verksamhetsfunktioner och stödprocesser såsom IKT-system, personal, uppdragstagare och tredje parter samt beroenden av andra interna och externa system och processer för att åtminstone kunna hantera de informationstillgångar som stödjer deras kritiska verksamhetsfunktioner och -processer.

1.3.3. Klassificering och riskbedömning

17. Finansinstitut bör klassificera de identifierade verksamhetsfunktioner, stödprocesser och informationstillgångar som anges i avsnitt 15 och 16 med avseende på kritikalitet.

18. För att definiera kritikaliteten hos dessa identifierade verksamhetsfunktioner, stödprocesser och informationstillgångar bör finansinstitut åtminstone ta hänsyn till konfidentialitets-, integritets- och tillgänglighetskraven. Det ska finnas ett tydligt tilldelat ansvar för informationstillgångarna.

19. Finansinstitut bör se över lämpligheten av klassificeringen av informationstillgångar och relevant dokumentation i samband med riskbedömning.

20. Finansinstitut bör identifiera sina IKT-risker och säkerhetsrisker som påverkar de identifierade och klassificerade verksamhetsfunktionerna, stödprocesserna och informationstillgångarna utifrån deras kritikalitet. Denna riskbedömning bör utföras och dokumenteras årligen eller vid behov oftare. Sådana riskbedömningar bör även utföras om eventuella omfattande ändringar i den infrastruktur, de processer eller de rutiner som påverkar verksamhetsfunktionerna, stödprocesserna eller informationstillgångarna och detta ska resultera i uppdatering av finansinstituts aktuella riskbedömning.

21. Finansinstitut bör tillse att de kontinuerligt övervakar de hot och den sårbarhet som är aktuell för deras affärsprocesser, stödfunktioner och informationstillgångar och regelbundet se över de riskscenarier som påverkar dessa.

1.3.4. Riskreducering

22. Med utgångspunkt i riskbedömningarna bör finansinstitut fastställa vilka åtgärder som krävs för att reducera de identifierade IKT-riskerna och säkerhetsriskerna till godtagbara nivåer och huruvida ändringar i befintliga affärsprocesser, kontrollåtgärder, IKT-system och IKT-tjänster är nödvändiga. Ett finansinstitut bör ta hänsyn till den nödvändiga tidsåtgången för att genomföra dessa ändringar och för att vidta lämpliga interimistiska riskreduceringsåtgärder för att minimera IKT-risker och säkerhetsrisker så att de förblir inom gränserna för finansinstitutets riskaptit för IKT-risker och säkerhetsrisker.

23. Finansinstitut bör definiera och införa åtgärder för att reducera identifierade IKT-risker och säkerhetsrisker samt skydda informationstillgångar i enlighet med deras klassificering.

1.3.5. Rapportering

24. Finansinstitut bör tydligt och i tid rapportera till ledningsorganet om riskbedömningens resultat. Sådan rapportering påverkar inte betaltjänstleverantörers skyldighet att lämna in en uppdaterad och övergripande riskbedömning till behöriga myndigheter i enlighet med artikel 95.2 i direktiv (EU) 2015/2366

1.3.6. Revision

25. Ett finansinstituts styrning samt dess system och processer för IKT-risker och säkerhetsrisker ska periodiskt granskas av revisorer med tillräckliga kunskaper och färdigheter samt tillräcklig sakkunskap inom IKT och säkerhetsrisker och (vid betaltjänstleverantörer) även inom betalningar för oberoende verifiering av deras effektivitet till ledningsorganet. Revisorerna ska vara oberoende inom eller av finansinstitutet. Intervall och fokus av sådana revisioner ska stämma överens med relevanta IKT-risker och säkerhetsrisker.

26. Ledningsorganet för ett finansinstitut ska godkänna revisionsplanen, bl.a. eventuella IKT-revisioner, och alla väsentliga ändringar i denna. Revisionsplanen och dess genomförande, bl.a. revisionsintervall, ska återspegla och vara proportionerlig med finansinstitutets inneboende IKT-risker och säkerhetsrisker och den ska uppdateras regelbundet.

27. En formell uppföljningsprocess, bl.a. bestämmelser om snabb verifiering och åtgärdande av kritiska resultat av IKT-revisionen, bör upprättas.

1.4. Informationssäkerhet

1.4.1. Informationssäkerhetspolicyn

28. Finansinstitut bör utarbeta och dokumentera en informationssäkerhetspolicy som ska definiera principer och regler med hög kravnivå för att skydda konfidentialiteten, integriteten för och tillgängligheten till finansinstitutets och deras kunders data och information. För betaltjänstleverantörer identifieras denna policy i säkerhetspolicydokumentet som ska antas i enlighet med artikel 5.1 j i direktiv (EU) 2015/2366. Informationssäkerhetspolicyn ska vara i

linje med finansinstitutets informationssäkerhetsmål och bygga på de relevanta resultaten av riskbedömningsprocessen. Policyn bör antas av ledningsorganet.

29. Policyn ska inkludera en beskrivning över informationssäkerhetsledningens viktigaste roller och ansvarsområden och den ska fastställa kraven på personal och uppdragstagare, processer och teknik i förhållande till informationssäkerhet och säkerställa att personalen och uppdragstagare på alla nivåer har sina ansvarsområden när det gäller finansinstitutets informationssäkerhet. Policyn ska säkerställa konfidentialitet, integritet och tillgänglighet av ett finansinstituts kritiska logiska och fysiska tillgångar, resurser och känsliga data, antingen i vila, vid transport eller vid användning. Informationssäkerhetspolicyn ska meddelas till alla anställda och uppdragstagare av finansinstitutet.

30. Med utgångspunkt i informationssäkerhetspolicyn bör finansinstitut ta fram och införa säkerhetsåtgärder för att reducera de IKT-risker och säkerhetsrisker som de utsätts för. Dessa åtgärder ska inkludera,

    a) organisation och styrning i enlighet med avsnitt 10 och 11,
    b) logisk säkerhet (avsnitt 1.4.2),
    c) fysisk säkerhet (avsnitt 1.4.3),
    d) säkerhet för IKT-verksamhet (avsnitt 1.4.4),
    e) säkerhetsövervakning (avsnitt 1.4.5),
    f) översyn, bedömning och testning av informationssäkerhet (avsnitt 1.4.6),
    g) utbildning i och medvetenhet om informationssäkerhet (avsnitt 1.4.7).

1.4.2. Logisk säkerhet

31. Finansinstitut bör definiera, dokumentera och införa rutiner för logisk åtkomstkontroll (identitets- och åtkomsthantering). Dessa rutiner bör införas, genomföras, övervakas och periodiskt ses över. Rutinerna ska även inkludera kontroller för övervakning av avvikelser. Dessa rutiner ska åtminstone implementera följande element där termen ’användare’ även inkluderar tekniska användare:

Behovsenlig behörighet, minsta möjliga behörighet och åtskillnad av ansvar: finansinstitut bör hantera åtkomsträttigheter till informationstillgångar och deras stödsystem utifrån behovsenlighet, bl.a. vid fjärråtkomst. Användare ska bara beviljas minimala åtkomsträttigheter som är absolut nödvändiga för att utföra arbetsuppgifterna (principen om minsta möjliga behörighet) för att förhindra obehörig åtkomst till information eller för att undvika att sådana kombinationer av åtkomsträttigheter beviljas som kan användas för att kringgå kontroller

(a) (principen om åtskillnad av ansvar).

(b) **Användaransvar**: finansinstitut bör i största möjliga mån begränsa användning av generiska och delade användarkonton samt säkerställa att användare kan identifieras vid åtgärder som utförs i IKT-systemen.

(c) **Privilegierade åtkomsträttigheter:** finansinstitut bör implementera strikta kontroller för privilegierad åtkomst till system genom att strikt begränsa och noggrant övervaka konton med höga behöriheter (t.ex. administratörskonton). För att säkerställa säker kommunikation och minska risk ska administrativ fjärråtkomst till kritiska IKT-system bara ges på en behovsenlig grund och starka autentiseringslösningar ska användas.

(d) **Loggning av användaraktiviteter:** åtminstone alla aktiviteter av privilegierade användare bör loggas och övervakas. Åtkomstloggar måste skyddas mot obehörig ändring eller radering och lagras under en period som motsvarar kritiskheten för de identifierade verksamhetsfunktionerna, stödprocesserna eller informationstillgångarna i enlighet med avsnitt 1.3.3, utan att detta påverkar tillämpningen av lagringskraven i unionslagstiftning och nationell lagstiftning. Ett finansinstitut bör använda denna information för att underlätta identifiering och utredning av avvikande aktiviteter som har upptäckts i tillhandahållandet av tjänster.

(e) **Åtkomsthantering:** åtkomsträttigheter bör tilldelas, tas bort eller ändras i tid i enlighet med på förhand definierade arbetsflöden för godkännande som omfattar verksamhetsägaren för den information som åtkomsten avser (ägaren av informationstillgången). Vid uppsägning av anställningsförhållandet bör åtkomsträttigheter upphävas omgående.

(f) **Omcertifiering av åtkomst:** åtkomsträttigheter bör ses över periodiskt för att säkerställa att användare inte har för omfattande rättigheter och att åtkomsträttigheter upphävs om de inte längre behövs.

(g) **Autentiseringsmetoder:** finansinstitut bör tillämpa autentiseringsmetoder som är tillräckligt tillförlitliga för att adekvat och effektivt säkerställa att policyer och rutiner för åtkomstkontroll följs. Autentiseringsmetoder ska stämma överens med kritikaliteten hos det IKT-system, den information eller den process som åtkomsten avser. Detta ska åtminstone inkludera komplexa lösenord eller starkare autentiseringsmetoder (t.ex. tvåfaktorsautentisering) med utgångspunkt i relevant risk.

32. Elektronisk åtkomst genom programvara till data och IKT-system måste hållas till det minimum som krävs för tjänsten i fråga.

1.4.3. Fysisk säkerhet

33. Finansinstituts fysiska säkerhetsåtgärder bör definieras, dokumenteras och införas för att skydda sina lokaler, datacentraler och känsliga områden från obehörig åtkomst och från miljöfaror.

34. Fysisk åtkomst till IKT-system får endast beviljas till behöriga personer. Behörighet bör tilldelas i enlighet med personens uppgifter och ansvarsområden och begränsas till personer som har lämplig utbildning och som övervakas på ett lämpligt sätt. Fysisk åtkomst bör ses över regelbundet för att säkerställa att onödiga åtkomsträttigheter snabbt tas bort om de inte längre behövs.

35. Tillräckliga åtgärder för att skydda mot miljöfaror bör motsvara byggnadernas betydelse och kritikaliteten för verksamheten eller IKT-systemen i dessa byggnader.

1.4.4. Säkerhet för IKT-verksamhet

36. Finansinstitut bör implementera processer för att förhindra säkerhetsincidenter i IKT-system och IKT-tjänster, samt att om de inträffar minimera effekten på IKT-leveransen. Dessa rutiner ska innehålla följande åtgärder:

a) identifiering av potentiella sårbarheter, som bör utvärderas och åtgärdas genom att säkerställa att programvara och firmware är uppdaterad, inklusive programvaran som tillhandahålls av finansiella institut till sina interna och externa användare, genom att distribuera kritiska säkerhetsuppdateringar eller genom att införa kompenserande kontroller.
b) implementering av säkra grundkonfigurationer för alla nätverkskomponenter
c) implementering av nätverkssegmentering, system för att förhindra av förlust av data och kryptering av nätverkstrafik (i enlighet med dataklassificeringen).
d) implementering av skydd för slutpunkter inklusive servrar, arbetsstationer och mobila enheter; finansinstitut bör utvärdera om slutpunkter uppfyller de säkerhetsstandarder som de definierat innan de ges tillgång till företagets nätverk.
e) Säkerställande att det finns mekanismer för verifiering av integriteten av programvara, firmware och data.
f) Kryptering av data i vila och under transitering (i enlighet med aktuell dataklassificering).

37. Vidare bör finansinstitut kontinuerligt fastställa huruvida ändringar i den befintliga verksamhetsmiljön påverkar de befintliga säkerhetsåtgärderna eller kräver införande av ytterligare åtgärder för lämplig reducering av relaterade risker. Sådana ändringar måste utgöra en del av finansinstitutens formella ändringshanteringsprocess som ska säkerställa att ändringar planeras, testas, dokumenteras, godkänns och tillämpas korrekt.

1.4.5. Säkerhetsövervakning

38. Finansinstitut bör ta fram och införa policyer och rutiner för att upptäcka avvikande aktiviteter som kan påverka finansinstituts informationssäkerhet och reagera på dessa händelser på ett lämpligt sätt. Som en del av denna kontinuerliga övervakning bör finansinstitut införa lämpliga och effektiva förmågor för att upptäcka och rapportera om fysiska eller logiska ingrepp samt överträdelser angående informationstillgångarnas konfidentialitet, integritet och tillgänglighet. Den kontinuerliga övervaknings- och upptäcktsprocessen måste inkludera

a) relevanta interna och externa faktorer, inklusive affärs- och IKT-administreringsfunktioner,
b) transaktioner för att upptäcka missbruk av tillgång till information från tredje part eller andra enheter och internt missbruk av åtkomst,
c) potentiella interna och externa hot.

39. Finansinstitut bör ta fram och införa processer och organisationsstrukturer för att identifiera och ständigt övervaka säkerhetshot som väsentligt kan påverka deras förmåga att tillhandahålla tjänster. Finansinstitut bör aktivt hålla sig uppdaterade om tekniska framsteg för att säkerställa att de är medvetna om alla säkerhetsrisker. Finansinstitut bör införa upptäckandeåtgärder, t.ex. för att identifiera eventuella informationsläckage, skadlig kod och andra säkerhetshot och även allmänt kända sårbarheter i programvara och hårdvara samt kontrollera motsvarande nya säkerhetsuppdateringar

40. Säkerhetsövervakningsprocessen ska även hjälpa ett finansinstitut att förstå karaktären av operativa incidenter eller säkerhetsincidenter, att identifiera trender och att stödja organisationens utredningar.

1.4.6. Översyn, bedömning och testning av informationssäkerhet

41. Finansinstitut bör utföra en mängd granskningar, bedömningar och tester av informationssäkerhet för att säkerställa effektiv identifiering av sårbarheter i sina IKT-system och IKT-tjänster. Till exempel kan finansinstitut utföra en gapanalys mot informationsäkerhetsstandarder, granskningar av överensstämmelse, interna och externa revisioner av informationssystem eller fysiska säkerhetsrevisioner. Vidare bör institutet ta hänsyn till god praxis såsom källkodsgranskningar, sårbarhetsbedömningar, penetrationstester och red team-tester.

42. Finansinstitut bör etablera och implementera ett testramverk för informationssäkerhet som validerar tillförlitligheten och effektiviteten hos deras informationssäkerhetsåtgärder och säkerställer att ramverket tar hänsyn till de hot och sårbarheter som har identifierats genom hotövervakning samt riskbedömningsprocessen för IKT-risker och säkerhetsrisker.

43. Testramverket för informationssäkerhet måste säkerställa att testerna

    a) utförs av oberoende testare med tillräckliga kunskaper och färdigheter samt tillräcklig sakkunskap inom testning av informationssäkerhetsåtgärder och som inte medverkar i utarbetandet av informationssäkerhetsåtgärderna,
    b) inkluderar sårbarhetsskanningar och penetrationstester (bl.a. hotbaserad penetrationstestning om nödvändigt och lämpligt) som motsvarar den risknivå som har identifierats för verksamhetsprocesserna och -systemen.

44. Finansinstitut bör utföra löpande och upprepade tester på de införda säkerhetsåtgärderna. För alla kritiska IKT system (avsnitt 17) bör dessa tester utföras minst en gång om året och för betaltjänstleverantörer utgör de en del av den övergripande bedömningen av säkerhetsrisker relaterade till de betaltjänster som de tillhandahåller, i enlighet med artikel 95(2) i PSD2. Icke-kritiska system måste testas regelbundet med hjälp av en riskbaserad metod, dock minst vart tredje år.

45. Finansinstitut bör säkerställa att tester av säkerhetsåtgärder utförs vid ändringar i infrastruktur, processer eller rutiner och om ändringar införs på grund av betydande operativa incidenter eller säkerhetsincidenter eller på grund av lansering av nya eller väsentligt modifierade internetanslutna kritiska applikationer.

46. Finansinstitut bör övervaka och utvärdera resultaten av säkerhetstesterna och uppdatera sina säkerhetsåtgärder därefter, för kritiska IKT-system utan dröjsmål.

47. För betaltjänstleverantörer måste testramverket även omfatta relevanta säkerhetsåtgärder för (1) betalningsterminaler och -enheter som används för att tillhandahålla betaltjänster, (2) betalningsterminaler och -enheter som används för att autentisera betaltjänstanvändare, och (3) de enheter och den programvara som tillhandahålls av betaltjänstleverantören till betaltjänstanvändaren för att generera/ta emot autentiseringskoder.

48. Beroende på de observerade säkerhetshoten och alla utförda ändringar måste testning inkludera scenarier med relevanta och kända potentiella attacker.

1.4.7. Utbildning i och medvetenhet om informationssäkerhet

49. Finansinstitut bör ta fram ett utbildningsprogram som även inkluderar periodiska säkerhetsmedvetenhetsprogram för all personal och alla uppdragstagare för att säkerställa att de är utbildade för de aktuella arbetsuppgifterna och skyldigheterna i enlighet med de relevanta säkerhetspolicyerna och -rutinerna i syfte att reducera mänskliga fel, stöld, bedrägeri, missbruk eller förlust samt för hantering av informationssäkerhetsrelaterade risker. Finansinstitut bör tillse att utbildningsprogrammet föreskriver utbildning för alla anställda och alla uppdragstagare minst en gång om året.

1.5. Hantering av IKT-verksamhet

50. Finansinstitut bör hantera sin IKT-verksamhet utifrån dokumenterade och införda processer och rutiner (som för betaltjänstleverantörer inkluderar säkerhetspolicydokumentet i enlighet med artikel 5.1 j i PSD2) som är godkända av ledningsorganet. Denna uppsättning av dokument ska definiera hur finansinstitut driver, övervakar och kontrollerar sina IKT-system och IKT-tjänster (bl.a. dokumentering av kritisk IKT-verksamhet) och möjliggöra för finansinstitut att upprätthålla en uppdaterad förteckning över IKT-tillgångar.

51. Finansinstitut bör säkerställa att kapaciteten av deras IKT-verksamhet är i linje med deras verksamhetskrav. Finansinstitut bör upprätthålla och vid möjlighet förbättra effektiviteten hos sin IKT-verksamhet, inklusive men inte begränsad till behovet att beakta hur man kan minimera eventuella fel till följd av manuella arbetsuppgifter.

52. Finansinstitut bör införa loggnings- och övervakningsrutiner för kritiska IKT-verksamheter för att möjliggöra upptäckt, analys och avhjälpande av fel.

53. Finansinstitut bör upprätthålla en uppdaterad förteckning över sina IKT-tillgångar (bl.a. IKT-system, nätenheter, databaser osv.). Förteckningen över IKT-tillgångar ska lagra konfigurationen av IKT-tillgångar samt länkar och inbördes beroenden mellan olika IKT-tillgångar för att möjliggöra en korrekt konfigurerings- och ändringshanteringsprocess.

54. Förteckningen över IKT-tillgångar ska vara tillräckligt detaljerad för att möjliggöra snabb identifiering av en IKT-tillgång och dess lokalisering, säkerhetsklassificering och ägarskap. Inbördes beroenden mellan olika tillgångar bör dokumenteras som hjälp vid hantering av säkerhetsincidenter och operativa incidenter, bl.a. IT-attacker.

55. Finansinstitut bör övervaka och hantera livscyklerna för IKT-tillgångar för att säkerställa att de även fortsättningsvis uppfyller och stödjer verksamhetskraven och riskhanteringskraven. Finansinstitut bör övervaka huruvida deras IKT-tillgångar stöds av deras externa eller interna leverantörer och utvecklare samt huruvida alla relevanta fixar och uppgraderingar tillämpas med utgångspunkt i dokumenterade processer. Risker som härrör från föråldrade eller icke-stödda IKT-tillgångar bör bedömas och genomgå riskreducering.

56. Finansinstitut bör införa kapacitetsplanerings- och övervakningsprocesser för att i tid förebygga, upptäcka och reagera på viktiga prestandaproblem i IKT-system och brister i IKT-kapacitet.

57. Finansinstitut bör definiera och införa rutiner för säkerhetskopiering och återställande av data och IKT-system för att säkerställa att de kan återställas efter behov. Omfattningen och intervallen av säkerhetskopiering bör planeras i linje med återställningskraven och kritikaliteten hos data och IKT-system samt utvärderas i enlighet med utförd riskbedömning. Säkerhetskopierings- och återställanderutiner bör testas regelbundet.

58. Finansinstitut bör säkerställa att säkerhetskopior på data och IKT-system lagras säkert och är på tillräckligt avstånd från det primära verksamhetsstället så att de inte utsätts för samma risker.

3.5.1 Hantering av IKT-incidenter och IKT-problem

59. Finansinstitut bör ta fram och införa en incident- och problemhanteringsprocess för att övervaka och logga operativa och säkerhetsrelaterade IKT-incidenter och för att möjliggöra för finansinstitut att i tid fortsätta eller återupprätta kritiska verksamhetsfunktioner och processer vid störningar. Finansinstitut bör fastställa lämpliga kriterier och tröskelvärden för att klassificera händelser som operativa incidenter eller säkerhetsincidenter (som anges i enlighet med definitionerna i dessa riktlinjer), liksom tidiga varningsindikatorer som bör fungera som varningar för att möjliggöra tidig upptäckt av dessa händelser. För betaltjänstleverantörer ska sådana kriterier och tröskelvärden inte påverka tillämpningen av klassificering av allvarliga incidenter i enlighet med artikel 96 i PSD2 och riktlinjerna för rapportering vid allvarliga incidenter enligt PSD2 (EBA/GL/2017/10).

60. För att minimera effekten av negativa händelser och möjliggöra snabbt återställande bör finansinstitut ta fram lämpliga processer och organisatoriska strukturer för att säkerställa en konsekvent och integrerad övervakning, hantering och uppföljning av operativa incidenter och säkerhetsincidenter samt för att säkerställa att de underliggande orsakerna identifieras och elimineras för att förebygga upprepade incidenter. Processen för incident- och problemhantering ska fastställa,

    a) rutinerna för identifiering, spårning, loggning, kategorisering och klassificering av incidenter i enlighet med en viss prioritet, som utgår från kritikaliteten för verksamheten,
    b) rollerna och ansvarsområdena för olika incidentscenarier (t.ex. fel, funktionsstörningar, IT-attacker),
    c) problemhanteringsrutiner för identifiering, analys och åtgärdande av den underliggande orsaken bakom en eller flera incidenter – ett finansinstitut bör analysera de operativa incidenter eller säkerhetsincidenter som sannolikt kan påverka finansinstitutet och som har identifierats eller förekommit inom och/eller utanför organisationen samt ta hänsyn till viktiga erfarenheter från dessa analyser och uppdatera säkerhetsåtgärderna därefter,

d) effektiva interna kommunikationsplaner, bl.a. rutiner för incidentrapportering och eskalering – vilket även omfattar säkerhetsrelaterade kundreklamationer – för att säkerställa
    i) att incidenter med potentiell stark negativ effekt på kritiska IKT-system och IKT-tjänster rapporteras till relevant verkställande ledning och verkställande IKT-ledning,
    ii) att ledningsorganet underrättas på ad hoc-basis vid väsentliga incidenter och åtminstone informeras om den aktuella effekten, hanteringen och de ytterligare kontroller som ska definieras till följd av incidenterna,
e) rutiner för incidenthantering i syfte att reducera effekter förknippade med incidenterna och att säkerställa att tjänsten blir funktionell och säker i tid,
f) specifika externa kommunikationsplaner för kritiska verksamhetsfunktioner och -processer för att
    i) samarbeta med relevanta intressenter för effektiv hantering av incidenten och effektiv återställning ,
    ii) i tid tillhandahålla information till externa parter (t.ex. kunder, andra marknadsaktörer, tillsynsmyndigheten) efter behov och i linje med en tillämplig förordning.

1.6. IKT-projektledning och ändringshantering

1.6.1. IKT-projektledning

61. Ett finansinstitut bör införa ett program och/eller en projektstyrningsprocess som definierar roller, skyldigheter och ansvarsområden för att effektivt stödja genomförandet av IKT strategin.

62. Ett finansinstitut bör på ett lämpligt sätt övervaka och reducera risker som härrör från finansinstitutets portfölj av IKT projekt (programhantering) med hänsyn även till de risker som kan följa av inbördes beroenden mellan olika projekt och från flera projekts beroenden av samma resurser och/eller samma sakkunskap.

63. Ett finansinstitut bör ta fram och införa en IKT-projektledningspolicy som åtminstone inkluderar

    a) projektets mål,
    b) roller och skyldigheter,
    c) en riskbedömning för projektet,
    d) en projektplan, tidsram och etapper,
    e) viktiga milstolpar,
    f) krav på ändringshantering.

64. IKT-projektledningspolicyn ska säkerställa att informationssäkerhetskraven analyseras och godkänns av en funktion som är oberoende av utvecklingsfunktionen.

65. Ett finansinstitut bör säkerställa att alla områden som påverkas av ett IKT-projekt är representerade i projektteamet och att projektteamet har de erforderliga kunskaperna för att säkerställa säkert och framgångsrikt genomförande av projektet.

66. Upprättande och utveckling av IKT-projekt och risker förknippade med dem bör regelbundet och på ad hoc-basis efter behov rapporteras till ledningsorganet antingen individuellt eller tillsammans, beroende på vikten och storleken av IKT-projekten. Finansinstitut bör inkludera projektrisken i sitt ramverk för riskhantering.

1.6.2. Anskaffning och utveckling av IKT-system

67. Finansinstitut bör utarbeta och införa en process som styr anskaffning, utveckling och underhåll av IKT-system. Denna process ska planeras med hjälp av en riskbaserad metod.

68. Ett finansinstitut bör tillse att de funktionella och icke-funktionella kraven (bl.a. säkerhetskraven) är tydligt definierade och godkända av behörig verksamhetsledning innan eventuell anskaffning eller utveckling av IKT-system sker.

69. Ett finansinstitut bör tillse att det finns fastställda åtgärder för att reducera risken för oavsiktlig ändring eller avsiktlig manipulering av IKT-systemen under deras utveckling och införande i produktionsmiljön.

70. Finansinstitut ska ha en fastställd metodik för testning och godkännande av IKT-system före första användning. Denna metodik ska ta hänsyn till kritikaliteten hos verksamhetsprocesser och tillgångar. Testning ska säkra att de nya IKT-systemen fungerar som planerat. De bör även använda sådana testmiljöer som korrekt återspeglar produktionsmiljön.

71. Finansinstitut bör testa IKT-system, IKT-tjänster och åtgärder för informationssäkerhet för att identifiera eventuella säkerhetssvagheter, överträdelser och incidenter.

72. Ett finansinstitut bör införa separata IKT-miljöer för att säkra korrekt åtskillnad av skyldigheter och för att reducera effekten av ej verifierade ändringar i produktionssystem. I synnerhet bör ett finansinstitut säkra åtskillnad av produktionsmiljöer från utvecklings- och testmiljöer och andra icke-produktionsmiljöer. Ett finansinstitut bör säkerställa integriteten och konfidentialiteten av produktionsdata i icke- produktionsmiljöer. Åtkomst till produktionsdata begränsas till behöriga användare.

73. Finansinstitut bör införa åtgärder för att skydda integriteten av källkoder för internt utvecklade IKT-system. De ska även fullständigt dokumentera utveckling, införande, drift och/eller konfigurering av IKT-systemen för att reducera eventuellt onödigt beroende av områdesexperter. Dokumentering av IKT-systemet ska (i tillämpliga fall) åtminstone inkludera användardokumentation, dokumentation av tekniska system och driftrutiner.

74. Ett finansinstituts processer för anskaffning och utveckling av IKT-system ska även tillämpas på IKT-system som utvecklas eller hanteras av verksamhetsfunktionens slutanvändare utanför IKT organisationen (t.ex. datorprogram för slutanvändare) med hjälp av en riskbaserad metod. Finansinstitutet bör upprätthålla ett register över dessa program som stödjer kritiska verksamhetsfunktioner eller -processer.

1.6.3. IKT-ändringshantering

75. Finansinstitut bör ta fram och införa en process för IKT-ändringshantering för att säkerställa att alla ändringar i IKT-system registreras, testas, bedöms, godkänns, införs och verifieras på ett kontrollerat sätt. Finansinstitut bör hantera ändringar vid nödsituationer (dvs. ändringar som ska införas snarast) i enlighet med rutiner som säkrar lämpliga skyddsåtgärder.

76. Finansinstitut bör avgöra om ändringar av den befintliga driftmiljön påverkar de befintliga säkerhetsåtgärderna eller kräver införande av fler åtgärder för att motverka riskerna i fråga. Dessa ändringar ska stämma överens med finansinstitutens formella process för ändringshantering.

1.7. Hantering av verksamhetens driftskontinuitet

77. Finansinstitut bör ta fram en sund process för kontinuitetshantering (BCM) för att maximera sin förmåga att tillhandahålla tjänster kontinuerligt och för att begränsa förluster vid allvarlig verksamhetsstörning i linje med artikel 85.2 i direktiv 2013/36/EU och rubrik VI i EBA:s riktlinjer för intern styrning (EBA/GL/2017/11).

1.7.1. Konsekvensanalys

78. Som en del av sund kontinuitetshantering bör finansinstitut utföra konsekvensanalys (BIA) genom att analysera sin exponering för allvarliga verksamhetsstörningar samt att kvantitativt och kvalitativt bedöma deras potentiella konsekvenser (bl.a. på konfidentialitet, integritet och tillgänglighet) med hjälp av interna och/eller externa data (t ex data från tredjepartsleverantörer som är relevant för en verksamhetsprocess eller offentligt tillgängliga data som kan vara relevant för konsekvensanalysen) och scenarieanalysen. Konsekvensanalysen ska även ta hänsyn till identifierade och klassificerade verksamhetsfunktioner, stödprocesser, tredje parter och informationstillgångar samt deras inbördes beroenden i enlighet med avsnitt 1.3.3.

79. Finansinstitut bör tillse att deras IKT-system och IKT-tjänster är planerade i enlighet med och stämmer överens med konsekvensanalysen, t ex med redundans av vissa kritiska komponenter för att förebygga störningar till följd av händelser som påverkar dessa komponenter.

1.7.2. Planering av driftskontinuitet

80. Utifrån sina konsekvensanalyser bör finansinstitut ta fram planer för att säkra driftskontinuitet (kontinuitetsplaner) som ska dokumenteras och godkännas av deras ledningsorgan. Planerna ska i synnerhet ta hänsyn till de risker som kan ha negativ effekt på IKT-system och IKT-tjänster. Planerna bör innehålla mål för att skydda och vid behov återupprätta konfidentialitet, integritet och tillgänglighet av deras affärsfunktioner, stödjande processer och informationstillgångar. Under framtagandet av dessa planer bör finansinstitut samordna med relevanta interna och externa intressenter efter behov.

81. Finansinstitut bör fastställa kontinuitetsplaner för att säkerställa att de kan hantera eventuella felscenarier på ett korrekt sätt och vid störningar återställa funktionen av sina kritiska affärsaktiviteter inom tidmålet (återställningstid (RTO), den maximala tiden inom vilken ett system eller en process ska återställas efter en incident) och återställningspunktmålet (återställningspunkt (RPO), den maximala tiden inom vilken dataförlust är acceptabel vid en incident). Vid allvarliga störningar i verksamheten som aktiverar specifika kontinuitetsplaner bör finansinstitut prioritera de kontinuitetsåtgärder som använder en riskbaserad metod som kan utgå från riskbedömningar utförda i enlighet med avsnitt 1.3.3. För betaltjänstleverantörer kan detta t.ex. inkludera underlättande av fortsatt hantering av kritiska transaktioner medan återställningsåtgärder pågår.

82. Ett finansinstitut bör överväga ett antal olika scenarier i sin kontinuitetsplan, bl.a. extrema men samtidigt möjliga sådana som finansinstitutet kan utsättas för, inklusive ett IT-attackscenario, och det bör bedöma den potentiella effekten av sådana scenarier. Utifrån dessa scenarier bör ett finansinstitut beskriva hur kontinuiteten av IKT-system och IKT-tjänster samt finansinstitutets informationssäkerhet säkerställs.

1.7.3. Hanterings- och återställningsplaner

83. Utifrån konsekvensanalyserna (avsnitt 78) och de möjliga scenarierna (avsnitt 82) bör finansinstitut utarbeta hanterings- och återställningsplaner. Dessa planer ska ange vilka förhållanden som kan föranleda aktivering av planerna och vilka åtgärder som ska vidtas för att säkra tillgänglighet, kontinuitet och återställande av åtminstone de kritiska IKT-systemen och IKT-tjänsterna av finansinstituten. Hanterings- och återställningsplanerna ska syfta till att stämma överens med återställningsmålen för finansinstitutens verksamhet.

84. Hanterings- och återställningsplanerna ska ta hänsyn till både kortsiktiga och långsiktiga återställningsmöjligheter. Planerna ska

    a) fokusera på återställande av driften av kritiska verksamhetsfunktioner, stödprocesser, informationstillgångar och deras inbördes beroenden för att undvika negativa effekter på funktionen av finansinstitut och på finanssystemet, bl.a. på betalsystem och betaltjänstanvändare, samt att säkra genomförande av pågående betaltransaktioner,
    b) dokumenteras och göras tillgängliga för verksamhets- och stödenheter samt vara lättillgängliga i nödfall, och
    c) uppdateras i enlighet med erfarenheter från incidenter, information från tester, nya identifierade risker och hot samt ändrade återställningsmål och –prioriteter.

85. Planerna ska även ta hänsyn till alternativa möjligheter i situationer där återställande på kort sikt kan vara omöjligt på grund av kostnader, risker, logistik eller oförutsedda omständigheter.

86. Som en del av hanterings- och återställningsplanerna bör ett finansinstitut även beakta och införa kontinuitetsåtgärder för att motverka fel hos tredjepartsleverantörer som har avgörande betydelse för kontinuiteten av ett finansinstituts IKT-tjänster (i linje med bestämmelserna om kontinuitetsplaner i EBA:s riktlinjer för outsourcing (EBA/GL/2019/02)).

1.7.4. Testning av planer

87. Finansinstitut bör periodiskt testa sina kontinuitetsplaner. I synnerhet bör de tillse att kontinuitetsplaner för deras kritiska verksamhetsfunktioner, stödprocesser, informationstillgångar och deras inbördes beroenden (bl.a. sådana som levereras av tredje parter i förekommande fall) testas minst en gång om året i enlighet med avsnitt 89.

88. Kontinuitetsplaner bör uppdateras minst en gång om året utifrån testresultaten, aktuella underrättelser om hot och erfarenheter från tidigare händelser. Eventuella ändringar av återställningsmål (bl.a. återställningstider och återställningspunkter) och/eller ändringar i verksamhetsfunktioner, stödprocesser och informationstillgångar bör i förekommande fall också beaktas som grund för uppdatering av kontinuitetsplanerna.

89. Finansinstituts testning av sina kontinuitetsplaner ska visa att de kan hålla företaget levande tills kritiska verksamheter kan återupprättas. I synnerhet bör de

    a) inkludera testning av en lämplig uppsättning av allvarliga men samtidigt möjliga scenarier, bl.a. sådana som tas i beaktande för utarbetandet av kontinuitetsplanerna (samt i förekommande fall testning av tjänster som tillhandahålls av tredje parter); detta ska inkludera byte av kritiska verksamhetsfunktioner, stödprocesser och informationstillgångar till katastrofmiljön samt demonstration av att de kan drivas på så sätt under en tillräckligt representativ tidsperiod och att normal funktion därefter kan återställas,
    b) vara utformade för att utmana förutsättningarna för kontinuitetsplanerna, inklusive styrnings- och kriskommunikationsplaner och
    c) inkludera rutiner för att verifiera förmågan hos personalen, uppdragstagarna, IKT-systemen och IKT-tjänsterna att hantera scenarier definierade i paragraf 89 a på ett lämpligt sätt.

90. Testresultat bör dokumenteras och eventuella brister som identifieras vid tester bör analyseras, hanteras och rapporteras till ledningsorganet.

1.7.5. Kriskommunikation

91. Vid en störning eller en nödsituation och under genomförande av kontinuitetsplanerna bör finansinstitut tillse att de har fastställda effektiva kriskommunikationsåtgärder så att alla relevanta interna och externa intressenter, bl.a. behöriga myndigheter (om så krävs enligt nationella bestämmelser) och relevanta leverantörer (outsourcingleverantörer), koncernenheter eller tredjepartsleverantörer) informeras i tid och på ett lämpligt sätt.

1.8. Hantering av relationer med betaltjänstanvändare

92. Betaltjänstleverantören bör ta fram och införa processer för att höja betaltjänstanvändarnas medvetenhet om säkerhetsrisker förknippade med betaltjänsterna genom att ge betaltjänstanvändarna information och vägledning.

93. Informationen och vägledningen till betaltjänstanvändarna bör uppdateras mot bakgrund av nya hot och sårbarheter och betaltjänstanvändarna bör underrättas om alla ändringar.

94. Om produktens funktioner tillåter bör betaltjänstleverantörerna ge betaltjänstanvändarna möjligheten att avaktivera specifika betalningsfunktioner för de betaltjänster som betaltjänstleverantören tillhandahåller betaltjänstanvändaren.

95. Om betaltjänstleverantören i enlighet med artikel 68.1 i direktiv (EU) 2015/2366 överenskommer med betalaren om beloppsgränser för betalningstransaktioner som utförs genom specifika betalningsinstrument bör betaltjänstleverantören ge betalaren möjligheten att justera dessa gränser upp till den högsta överenskomna gränsen

96. Betaltjänstleverantörerna bör ge betaltjänstanvändarna möjligheten att ta emot meddelanden om påbörjade och/eller misslyckade försök att utföra betalningstransaktioner för att låta dem upptäcka bedräglig eller skadlig användning av deras konton.

97. Betaltjänstleverantörerna bör informera betaltjänstanvändarna om uppdaterade säkerhetsprocedurer som påverkar betaltjänstanvändarens tillgång till betaltjänster.

98. Betaltjänstleverantörerna bör hjälpa betaltjänstanvändarna vid alla frågor, begäran om hjälp eller rapporter om avvikelser eller problem avseende betaltjänsternas säkerhet. Betaltjänstanvändarna bör underrättas om hur sådan hjälp kan erhållas.