Föreskrifter och anvisningar 8/2014

Hantering av operativa risker i företag under tillsyn inom finanssektorn

Dnr
FIVA 8/01.00/2014

Utfärdade
4.11.2014

Gäller från
1.2.2015

Upplysningar
Digitalisering och analys /
Digitalisering och banktjänster

FINANSINSPEKTIONEN
telefon 09 183 51
fornamn.efternamn@fiva.fi
finansinspektionen.fi

FIN-FSA
FINANSINSPEKTIONEN

Den juridiska karaktären av föreskrifter och anvisningar

Föreskrifter

I Finansinspektionens föreskrifter och anvisningar presenteras föreskrifterna under rubriken "Föreskrift". Föreskrifterna är bindande rättsregler, som måste följas.

Finansinspektionen meddelar föreskrifter endast med stöd av och inom ramen för rättsliga bestämmelser som ger Finansinspektionen behörighet att ge ut föreskrifter.

Anvisningar

I Finansinspektionens föreskrifter och anvisningar presenteras under rubriken "Anvisning" Finansinspektionens tolkningar av innehållet i lagar eller andra bindande bestämmelser.

Under denna rubrik presenteras också rekommendationer och andra verksamhetsanvisningar som inte är bindande. Vidare upptas här Finansinspektionens rekommendationer om hur internationella riktlinjer och rekommendationer ska följas.

Av formuleringen av anvisningen framgår när det är fråga om en tolkning och när det är fråga om en rekommendation eller annan verksamhetsanvisning. Formuleringen av anvisningarna och den juridiska karaktären av föreskrifterna och anvisningarna förklaras närmare på Finansinspektionens webbplats.

Finansinspektionen.fi > Regelverk > Den juridiska karaktären av föreskrifter och anvisningar

Innehåll

1 Tillämpningsområde och definitioner 5

1.1 Riskhantering 5

1.2 Beredskap för undantagsförhållanden 6

1.3 Proportionalitetsprincipen 6

1.4 Definitioner 6

2 Regelverk och internationella rekommendationer 8

2.1 Lagstiftning 8

2.2 Europeiska unionens förordningar 8

2.3 Europeiska unionens direktiv 9

2.4 Finansinspektionens rätt att meddela föreskrifter 9

2.5 Internationella rekommendationer 10

3 Syfte 12

4 Allmänna principer för hantering av operativa risker 13

4.1 Hantering av operativ risk 13

4.2 Organisation av den operativa riskhanteringen 13

4.3 Identifiering och bedömning av operativa risker 13

4.4 Övervakning av operativa risker och rapportering av skador 15

5 Delområden i hanteringen av operativa risker 18

5.1 Processer 18

5.2 Legal risk 18

5.3 Personal 19

6 IT-system och informationssäkerhet 21

6.1 IT-system ... 21

6.2 Informationssäkerhet ... 22

6.2.1 Definition av informationssäkerhet och grundläggande krav ... 22

6.2.2 Hantering av informationssäkerhetsrisker och incidenthantering ... 23

6.2.3 Regler och utbildning om informationssäkerhet ... 23

6.2.4 Informationssäkerheten i datanätet ... 24

6.2.5 Utveckling av säkra onlinetjänster ... 24

7 Betalningssystem och betalningsförmedling ... 26

8 Kontinuitets- och beredskapsplanering ... 28

8.1 Regelverk ... 28

8.2 Kontinuitetsplanering ... 29

8.3 Beredskap för undantagsförhållanden ... 30

8.4 Beredskapsplan ... 31

9 Rapportering till Finansinspektionen ... 32

9.1 Anmälan om störningar och fel i verksamheten ... 32

9.2 Årsanmälan om förluster på grund av operativa risker ... 33

9.3 Årlig bedömning av de operativa riskerna och säkerhetsriskerna som gäller betaltjänster (Utfärdats 29.1.2018, gäller från 1.3.2018) ... 34

9.4 Rapportering av svikliga förfaranden i anslutning till betaltjänster (Utfärdats 23.9.2019, gäller från 1.1.2020) ... 35

9.5 Ansökan om undantag från kravet på beredskapsmekanism för PSD2-specialgränssnittet (Utfärdats 23.9.2019, gäller från 1.1.2020) ... 35

10 Upphävda föreskrifter och anvisningar ... 37

11 Ändringshistorik ... 38

1 Tillämpningsområde och definitioner

1.1 Riskhantering

Kapitel 4–7 samt avsnitt 8.2, 9.1 och 9.2 i dessa föreskrifter och anvisningar tillämpas på följande företag under tillsyn enligt lagen om Finansinspektionen: (Utfärdats 29.12018, gäller från 1.3.2018)

- kreditinstitut
- filialer i Finland till kreditinstitut i tredjeländer
- värdepappersföretag som i enlighet med 6 kap. 2 § i lagen om investeringstjänster omfattas av bestämmelserna i 9, 10 och 11 kap. i kreditinstitutslagen
- fondbolag som bedriver sådan verksamhet som avses i 5 § 2 mom. i lagen om placeringsfonder
- förvaltare av alternativa investeringsfonder (AIF-förvaltare) som tillhandahåller investeringstjänster
- kreditinstituts och värdepappersföretags holdingföretag samt konglomerats holdingsammanslutning enligt lagen om tillsyn över finans- och försäkringskonglomerat
- centralinstitut för sammanslutningar av inlåningsbanker
- betalningsinstitut

Kapitel 4–6 samt avsnitt 8.2 och 9.1 (2) i dessa föreskrifter och anvisningar tillämpas på följande företag under tillsyn:

- börsen

Vidare rekommenderar Finansinspektionen att filialer i Finland till värdepappersföretag från tredjeländer följer kapitel 4–7 samt avsnitten 8.2, 9.1 och 9.2 i dessa föreskrifter och anvisningar. (Utfärdats 29.1.2018, gäller från 1.3.2018)

Kapitel 7 om betalningssystem tillämpas endast på företag under tillsyn som bedriver betalningsförmedling.

På personer som utan auktorisation tillhandahåller betaltjänster, inklusive personer som tillhandahåller kontoinformationstjänster, tillämpas kapitel 7 och avsnitt 9.1, vilka tillämpas till de delar som närmare framgår av det aktuella kapitlet eller avsnittet. (Utfärdats 29.1.2018, gäller från 1.3.2018)

Avsnitt 9.3 (årlig bedömning av operativa risker och säkerhetsrisker för betaltjänster) och 9.4 (rapportering av uppgifter om svikliga förfaranden i anslutning till betaltjänster) tillämpas på tillsynsobjekt som tillhandahåller betaltjänster och på personer som utan auktorisation tillhandahåller betaltjänster samt på inhemska kreditinstitut som tillhandahåller betaltjänster och på filialer till utländska kreditinstitut som tillhandahåller betaltjänster i Finland. (Utfärdats 23.9.2019, gäller från 1.1.2020)

Avsnitt 9.5 (ansökan om undantag från kravet på beredskapsmekanism för PSD2-gränssnittet) tillämpas på kredit- eller betalinstitut som upprätthåller betalkonton. (Utfärdats 23.9.2019, gäller från 1.1.2020)

1.2 Beredskap för undantagsförhållanden

Avsnitt 8.3 i dessa föreskrifter och anvisningar tillämpas på följande företag under tillsyn och utländska företag under tillsyn som är skyldiga att skapa beredskap för undantagsförhållanden enligt beredskapslagen (1552/2011).

- kreditinstitut
- betalningsinstitut
- värdepappersföretag som tillhandahåller förvaring av finansiella instrument som sidotjänst (Utfärdats 29.1.2018, gäller från 1.3.2018)
- fondbolag
- AIF-förvaltare som tillhandahåller investeringstjänster
- filialer i Finland till utländska kreditinstitut
- filialer i Finland till utländska betalningsinstitut
- filialer i Finland till utländska värdepappersföretag
- värdepapperscentralen.

Finansinspektionen rekommenderar också att börsen följer anvisningarna i avsnitt 8.3 om beredskap för undantagsförhållanden. (Utfärdats 29.1.2018, gäller från 1.3.2018)

1.3 Proportionalitetsprincipen

Dessa föreskrifter och anvisningar tillämpas på olika företag under tillsyn och olika styrningsmodeller. Vid tillämpningen av föreskrifterna och anvisningarna får företaget ta hänsyn till verksamhetens art, omfattning och mångfald, riskerna i verksamheten och eventuella andra motsvarande omständigheter som påverkar dess bedömning, när det avgör hur det så ändamålsenligt och effektivt som möjligt följer föreskrifterna och anvisningarna.

1.4 Definitioner

Med *tillsynsobjekt och institut* avses sådana företag under tillsyn och utländska företag under tillsyn enligt lagen om Finansinspektionen som omfattas av tillämpningsområdet enligt avsnitt 1.1 ovan.

Med *operativ risk* avses risk för förluster på grund av
- otillräckliga eller misslyckade interna processer
- personalen
- systemen
- externa faktorer.

Operativa risker inkluderar legala risker, men exkluderar strategiska risker.

Med *kontroller* avses rutiner för att säkerställa att en verksamhet når sitt mål. Kontroller är alla åtgärder i syfte att förebygga, upptäcka och reducera störningar, brister, fel och missbruk.

Exempel på kontroller är avstämningar, principen att "fyra ögon ser mer än två" och jämförelser av motparternas bekräftelser med företagets egen avtalsdokumentation.

Med *verkställande ledning* avses verkställande direktören och alla de personer som rapporterar direkt till verkställande direktören och har ledningsuppgifter i företaget eller leder dess verksamhet

2 Regelverk och internationella rekommendationer

2.1 Lagstiftning

Dessa föreskrifter och anvisningar har samband med följande lagar och beslut:
(Utfärdats 23.9.2019, gäller från 1.1.2020)

- kreditinstitutslagen (610/2014, nedan även KIL)
- lagen om investeringstjänster (747/2012, nedan även ITL)
- lagen om placeringsfonder (48/1999, nedan även PlacFL)
- lagen om förvaltare av alternativa investeringsfonder (162/2014, nedan även AIFML)
- lagen om en sammanslutning av inlåningsbanker (599/2010)
- lagen om betalningsinstitut (297/2010, nedan även BIL)
- lagen om tillsyn över finans- och försäkringskonglomerat (699/2004)
- lagen om handel med finansiella instrument (1070/2017)
- lagen om värdeandelssystemet och om clearingverksamhet (348/2017)
- betaltjänstlagen (290/2010)
- beredskapslagen (1552/2001)
- statsrådets beslut om målen med försörjningsberedskapen (857/2013).

2.2 Europeiska unionens förordningar

Dessa föreskrifter och anvisningar har nära samband med följande EU-förordningar:
(Utfärdats 23.9.2019, gäller från 1.1.2020)

- Kommissionens delegerade förordning (EU) nr 231/2013 (32013R0231) av den 19 september 2012 om komplettering av Europaparlamentets och rådets direktiv 2011/61/EU vad gäller undantag, allmänna verksamhetsvillkor, förvaringsinstitut, finansiell hävstång, öppenhet och tillsyn, EUT L 83, 22.3.2013, s. 1–95 (nedan delegerad förordning)
- Europeiska centralbankens förordning (EU) nr 795/2014 (32014R0795) av den 3 juli 2014 om krav på övervakning av systemviktiga betalningssystem (ECB/2014/28), EUT L 217, 23.7.2014, s. 16–30.
- Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)
- Kommissionens delegerade förordning (EU) 2018/389 av den 27 november 2017 om komplettering av Europaparlamentets och rådets direktiv (EU) 2015/2366 vad gäller tekniska tillsynsstandarder för sträng kundautentisering och gemensamma och säkra öppna kommunikationsstandarder (nedan SCA delegerad förordning).

2.3 Europeiska unionens direktiv

Dessa föreskrifter och anvisningar har nära samband med följande EU-direktiv:
(Utfärdats 23.9.2019, gäller från 1.1.2020)

- Europaparlamentets och rådets direktiv 2013/36/EU (32013L0036) av den 26 juni 2013 om behörighet att utöva verksamhet i kreditinstitut och om tillsyn av kreditinstitut och värdepappersföretag, om ändring av direktiv 2002/87/EG och om upphävande av direktiv, 2006/48/EG och 2006/49/EG; EUT L 176, 27.6.2013, s. 338
- Europaparlamentets och rådets direktiv 2014/65/EU av den 15 maj 2014 om marknader för finansiella instrument och om ändring av direktiv 2002/92/EG och av direktiv 2011/61/EU, EUT L 173, 12.6.2014, s. 349.
- Europaparlamentets och rådets direktiv (EU) 2015/2366 av den 25 november 2015 om betaltjänster på den inre marknaden, om ändring av direktiven 2002/65/EG, 2009/110/EG och 2013/36/EU samt förordning (EU) nr 1093/2010 och om upphävande av direktiv 2007/64/EG, EUT L 319, 23.12.2015
- Europaparlamentets och rådets direktiv 2002/87/EG (32002L0087) av den 16 december 2002 om extra tillsyn över kreditinstitut, försäkringsföretag och värdepappersföretag i ett finansiellt konglomerat och om ändring av rådets direktiv 73/239/EEG, 79/267/EEG, 92/49/EEG, 92/96/EEG, 93/6/EEG och 93/22/EEG samt Europaparlamentets och rådets direktiv 98/78/EG och 2000/12/EG, EUT L 35, 11.2.2003, s. 1–27
- Kommissionens direktiv 2006/73/EG (32006L0073) av den 10 augusti 2006 om genomförandet av Europaparlamentets och rådets direktiv 2004/39/EG vad gäller organisatoriska krav och villkor för verksamheten i värdepappersföretag, och definitioner för tillämpning av det direktivet, EUT L 241, 2.9.2006, s. 26–58
- Europaparlamentets och rådets direktiv 2009/65/EG (32009L0065) av den 13 juli 2009 om samordning av lagar och andra författningar som avser företag för kollektiva investeringar i överlåtbara värdepapper (fondföretag), EUT L 302, 17.11.2009, s. 32–96
- Europaparlamentets och rådets direktiv 2011/61/EU (32011L0061) av den 8 januari 2011 om förvaltare av alternativa investeringsfonder samt om ändring av direktiv 2003/41/EG och 2009/65/EG och förordningarna (EG) nr 1060/2009 och (EU) nr 1095/2010, EUT L 174, 1.7.2011, s. 1–73.
- Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.

2.4 Finansinspektionens rätt att meddela föreskrifter

Finansinspektionens rätt att meddela föreskrifter bygger på följande bestämmelser:

- 18 § 2 mom. i lagen om Finansinspektionen (878/2008), som föreskriver att Finansinspektionen kan meddela föreskrifter om regelbunden rapportering av uppgifter om tillsynsobjekts internkontroll och riskhantering till Finansinspektionen.

- Enligt 9 kap. 24 § i KIL kan Finansinspektionen meddela närmare föreskrifter om operativa risker enligt 9 kap. 16 § i lagen.
- Enligt 19 § 6 mom. i lagen om en sammanslutning av inlåningsbanker kan Finansinspektionen meddela närmare föreskrifter om riskhanteringen i företag som hör till en sammanslutning.
- Av 6 kap. 2 § 1 mom. i lagen om investeringstjänster och 6 § 5 mom. i PlacFL följer att de föreskrifter som Finansinspektionen meddelar med stöd av 9 kap. 24 § i KIL också är bindande för sådana värdepappersföretag och fondbolag som avses i lagrummen.
- Enligt 6 kap. 2 § 6 mom. i lagen om förvaltare av alternativa investeringsfonder ska en AIF-förvaltare som tillhandahåller tjänster som avses i 3 kap. 2 § 2 mom. och 3 kap. 3 § 1 mom. alltid uppfylla de krav som föreskrivs i 6 kap. 2 § 1 mom. i lagen om investeringstjänster. Av 6 kap. 2 § 1 mom. i lagen om investeringstjänster följer att de föreskrifter som Finansinspektionen meddelar med stöd av 9 kap. 24 § i kreditinstitutslagen även är bindande för sådana förvaltare av alternativa investeringsfonder som avses i lagrummen. (Utfärdats 29.1.2018, gäller från 1.3.2018)
- Med stöd av 30 a § 3 mom. i PlacFL meddelar Finansinspektionen närmare föreskrifter om kraven för ett fondbolags riskhanteringssystem och övriga interna kontroll.
- Med stöd av 19 § 3 mom. i BIL kan Finansinspektionen meddela närmare föreskrifter om organisation av verksamheten för genomförande av betaltjänstdirektivet, samt med stöd av 19 a och 19 b § i nämnda lag om hanteringen av operativa risker och säkerhetsrisker samt om anmälan av incidenter och bedrägerier Föreskrifter som Finansinspektionen meddelar med stöd av 19 a och 19 b § i betaltjänstlagen är även bindande för personer som utan auktorisation tillhandahåller betaltjänster samt för kreditinstitut som tillhandahåller betaltjänster med stöd av 9 kap. 16 § i kreditinstitutslagen. (Utfärdats 29.1.2018, gäller från 1.3.2018)
- Med stöd av 16 § 3 mom. lagen om tillsyn över finans- och försäkringskonglomerat meddelar Finansinspektionen närmare föreskrifter om uppläggningen av den interna kontrollen och riskhanteringen till konglomeratets moderföretag och holdingsammanslutning.
- Med stöd av 3 kap. 36 § 1 mom. 1 punkten i lagen om handel med finansiella instrument meddelar Finansinspektionen närmare föreskrifter om organisationen av verksamheten i en börs enligt 3 kap. 1 § i lagen.

2.5 Internationella rekommendationer

Dessa föreskrifter och anvisningar beaktar följande internationella rekommendationer:

- Baselkommitténs rekommendation Revisions to the Principles for the Sound Management of Operational Risk (BIS mars 2021) (Utfärdats 16.2.2022, gäller från 1.3.2022)
- Europeiska bankmyndighetens riktlinje Management of Operational Risks in Market-related Activities (CEBS oktober 2010)
- Europeiska bankmyndighetens riktlinjer för intern styrning Guidelines on Internal Governance (EBA/GL/2021/05) (Utfärdats 16.2.2022, gäller från 1.3.2022)

- Baselkommitténs rekommendation High level principles for business continuity (BIS augusti 2006)
- Baselkommitténs rekommendation Risk Management Principles for Electronic Banking (BIS juli 2003)
- Europeiska värdepappers- och marknadsmyndighetens riktlinjer ”System och kontroller i en automatiserad handelsmiljö för handelsplattformar, värdepappersföretag och behöriga myndigheter” (ESMA februari 2012)
- “Committee on Payment and Settlement Systems”, som sorterar under Baselkommittén, och IOSCOs tekniska kommitténs, “Technical Committee” rekommendation Principles for financial market infrastructures (BIS/IOSCO april 2012)
- Europeiska bankmyndighetens riktlinjer om IKT-riskbedömning inom ramen för översyns- och utvärderingsprocessen (ÖUP) Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP) (EBA/GL/2017/05) (Utfärdats 6.11.2017, gäller från 1.3.2018)
- Europeiska bankmyndighetens riktlinjer om rapportering av allvarliga incidenter Revised Guidelines on major incident reporting under PSD2 (EBA/GL/2021/03) (Utfärdats 16.2.2022, gäller från 1.3.2022))
- Europeiska bankmyndighetens riktlinjer för hantering av IKT och säkerhetsrisker Guidelines on ICT and security risk management (EBA/GL/2019/04) (Utfärdats 16.2.2022, gäller från 1.3.2022)
- De europeiska övervakningsmyndigheternas gemensamma kommittés ställningstagande Joint Position on Manufacturers’ Product Oversight and Governance Processes (november 2013)
- Europeiska bankmyndighetens riktlinjer om krav för rapportering av statistiska uppgifter om svikliga förfaranden enligt artikel 96.6 i det andra betaltjänstdirektivet (Guidelines on fraud reporting under the Payment Services Directive 2 (PSD2) (EBA/GL/2018/05) (Utfärdats 23.9.2019, gäller från 1.1.2020)
- Europeiska bankmyndighetens riktlinjer för villkoren att utnyttja undantaget från beredskapsmekanismen enligt artikel 33.6 i förordning EU 2018/389 (tekniska tillsynsstandarder för sträng kundautentisering och gemensamma och säkra öppna kommunikationsstandarder) (Utfärdats 23.9.2019, gäller från 1.1.2020).

3 Syfte

(1) Dessa föreskrifter och anvisningar redogör för principerna för hantering av operativa risker och för riskhanteringens uppläggning. Särskild uppmärksamhet ägnas områden som har samband med processhantering, personal, IT- och betalningssystem, informationssäkerhet, kontinuitetsplanering och legala risker.

(2) Den tekniska utvecklingen, utvecklingen av produkter och tjänster, nya riskhanteringsmetoder, utläggningar, strukturaffärer och globalisering har gjort omvärlden allt mer komplex och ökat de operativa riskerna vid produktion av finansiella tjänster.

(3) Det är viktigt att betalnings- och avvecklingssystemen är välfungerande, eftersom största delen av betalningarna i ekonomin förmedlas och avvecklas i systemen. Avbrott och störningar försvårar kundernas betalningar och kan därigenom medföra långtgående ekonomiska problem.

(4) Syftet med dessa föreskrifter och anvisningar är att se till att följande uppfylls:

- Tillsynsobjekten lägger upp hanteringen av operativa risker så att den är tillfredsställande i förhållande till verksamhetens art och omfattning.
- Vid behov kan riskhanteringsuppgifter läggas ut på entreprenad enligt Finansinspektionens föreskrifter och anvisningar 1/2012.
- Tillsynsobjekten tillämpar adekvata rutiner för informationsförvaltning, informationssäkerhet och kontinuiteten i verksamheten.
- Tillsynsobjekten informerar Finansinspektionen om betydande störningar och fel i sin verksamhet och andra skador och förluster på grund av operativa risker.

4 Allmänna principer för hantering av operativa risker

4.1 Hantering av operativ risk

(1) Den förlust som operativ risk resulterar i är inte alltid mätbar. Risken kan också realiseras med fördröjning och ge utslag indirekt t.ex. genom försämrat rykte eller minskad respekt.

(2) Hanteringen av operativa risker fokuserar på åtgärder för att avhjälpa observerade brister och fel i processer och riskhantering och andra riskbegränsningsåtgärder, såsom personella och datatekniska reservsystem och tecknande av försäkringsskydd.

(3) I kreditinstitutslagen finns detaljerade bestämmelser om hantering av operativa risker. Enligt 9 kap. 16 § 1 mom. i KIL ska ett kreditinstitut införa metoder för att identifiera, bedöma och hantera exponeringen för operativa risker. Institutet ska ha beredskap åtminstone för modellrisk och för extrema händelser med stor inverkan på institutets verksamhet. Institutet ska tydligt ange vad det betraktar som operativa risker. Det ska ha skriftliga riktlinjer och processer för hantering av operativa risker

4.2 Organisation av den operativa riskhanteringen

(4) Med stöd av avsnitt 2.4 om rätten att meddela föreskrifter meddelar Finansinspektionen följande föreskrift om organisation av riskhanteringen.

Föreskrift (styckena 5-6)

(5) Tillsynsobjektets styrelse ska godkänna principerna för hantering av operativa risker, som omfattar metoderna och processerna för identifiering, bedömning, uppföljning och begränsning av operativa risker. Principerna ska ses över med jämna mellanrum så att de speglar förändringarna i omvärlden och i tillsynsobjektets egen verksamhet.

(6) Tillsynsobjekten ska i sin definition av operativa risker utgå från den egna verksamheten och beakta verksamhetens särdrag.

Anvisning (styckena 7-8)

(7) Finansinspektionen rekommenderar att den verkställande ledningen sörjer för att principerna för hantering av operativa risker omsätts i praktiken i tillsynsobjektets samtliga verksamheter och i alla koncernföretag. Dessutom bör det säkerställas att varje anställd kan identifiera de operativa riskerna i sin egen verksamhet och känner till rutinerna för att hantera dessa risker.

(8) Finansinspektionen rekommenderar att styrelsen säkerställer att hanteringen av operativa risker regelbundet är föremål för en effektiv och täckande internrevision.

4.3 Identifiering och bedömning av operativa risker

(9) Med stöd av avsnitt 2.4 om rätten att meddela föreskrifter meddelar Finansinspektionen följande föreskrifter om organisation av riskhanteringen.

(10) Närmare bestämmelser om processer för produktgodkännande i värdepappersföretag finns i de föreskrifter och anvisningar som getts med stöd av 7 kap. 7 och 16 § i lagen om investeringstjänster. (Utfärdats 23.9.2019, gäller från 1.1.2020)

Föreskrift (styckena 11-15)

(11) Tillsynsobjekten ska kunna identifiera de operativa riskerna i alla sina viktigaste produkter, tjänster, funktioner, processer och system som kan ha en väsentlig inverkan på måluppfyllelsen för verksamheten.

(12) Tillsynsobjekten ska bedöma riskerna i nya produkter och tjänster innan de tas i bruk. Motsvarande bedömning ska också göras när en ny tjänstemodell introduceras om produkter och tjänster har kombinerats på nytt sätt, om inte tillsynsobjektet bedömer att de tidigare bedömningarna fångar upp riskerna i den nya tjänstemodellen.

(13) Vid den löpande kartläggningen av riskerna ska sannolikheten för och verkningarna av en förlusthändelse bedömas. I planeringen av riskhanteringen ska tillsynsobjekten fastställa nödvändiga riskreduceringsmetoder och övriga korrigeringsåtgärder som verksamheten kräver.

(14) Tillsynsobjekten ska fatta beslut om den godtagbara nivån på risktagandet för de viktigaste funktionerna och sätta upp limiter eller andra gränser för de viktigaste riskerna.

(15) Tillsynsobjekten ska ta fram alternativa scenarier som ska beakta effekten av en lamslagning av åtminstone de viktigaste processerna, systemen och personerna, samt effekten av externa faktorer.

Anvisning (styckena 16-22)

(16) Finansinspektionen rekommenderar att tillsynsobjekten i fråga om de viktigaste identifierade operativa riskerna bedömer hur riskerna ska kontrolleras, om de ska begränsas eller accepteras, eller om verksamheten ska avvecklas helt.

(17) Finansinspektionen rekommenderar att riskbedömningen analyserar skadliga interna och externa faktorer. Exempel på interna faktorer är företagets juridiska struktur, organisationsförändringar, komplexiteten av produkter och tjänster, de anställdas kompetens, personalomsättningen och läget för IT-systemen. Externa faktorer är exempelvis tekniska framsteg och internationalisering.

(18) Finansinspektionen rekommenderar att tillsynsobjekten inför förebyggande rutiner och mått för identifiering av operativa risker. För detta ändamål kan exempelvis användas formbundna självutvärderingar som utförs av bankens organisation, statistik om skador på grund av riskerna, användning av kritiska variabler (KRI) som beskriver verksamheten och genomgång av skador som drabbat tillsynsobjektet självt eller någon kollegial grupp.

(19) Finansinspektionen rekommenderar att tillsynsobjekten tecknar en försäkring mot de ekonomiska effekterna av operativa risker. Den verkställande ledningen bör sörja för att försäkringsskyddet och kostnaderna för försäkringen ses över regelbundet med beaktande av förändringar i tillsynsobjektets verksamhet. Dessutom bör motpartsriskerna på grund av försäkringsavtal och avtalsbolagets solvens bedömas.

(20) Finansinspektionen rekommenderar att tillsynsobjekten inför rutiner för godkännande av nya produkter och tjänster.

(21) Finansinspektionen rekommenderar att godkännandeprocessen för en ny produkt eller tjänst innehåller åtminstone följande uppgifter:

- beskrivning av produkten eller tjänsten
- bedömning av produktens eller tjänstens överensstämmelse med verksamhetsstrategin
- geografiskt marknadsområde eller målgrupp
- kartläggning av riskerna (bedömning av vilka risker som är förknippade med produkten eller tjänsten)
- beskrivning av hur internkontrollen och riskhanteringen av en ny produkt eller tjänst är organiserad
- genomgång av de processer som hänför sig till produkten eller tjänsten (exempelvis offertstadiet, identifiering av kunden, försäljning, produktion, clearing och avveckling samt betalningar)
- juridiska frågor och avtalsbefogenheter
- beskrivning av IT-systemen, informationssäkerheten och kontinuiteten i tjänsterna
- kraven från den externa och interna redovisningen
- beskrivning av prissättning, eventuella värderingar och användning av prissättningsmodeller
- bedömning av effekterna på lönsamhet och kapitaltäckning
- beräknade skatteeffekter
- beskrivning av den utbildning och vägledning som behövs.

(22) Finansinspektionen rekommenderar att tillsynsobjekten presenterar en viktig ny produkt eller tjänst för Finansinspektionen i god tid innan den introduceras.

4.4 Övervakning av operativa risker och rapportering av skador

(23) Kapitel 9 innehåller anvisningar om den anmälan som ska lämnas till Finansinspektionen om störningar och fel i verksamheten och om årsanmälan om viktiga förlusthändelser på grund av operativa risker.

(24) Med stöd av avsnitt 2.4 om rätten att meddela föreskrifter meddelar Finansinspektionen följande föreskrifter om organisation av riskhanteringen.

Föreskrift (styckena 25-26)

(25) Tillsynsobjektet ska regelbundet bedöma arten av operativa risker och sannolikheten för att de realiseras och övervaka realiserade förluster och deras storlek. Bidragande faktorer och konsekvenser av skadehändelsen ska undersökas.

(26) Styrelsen och verkställande ledningen ska informeras om de viktigaste operativa riskerna inom företagets olika affärsområden. Som en del av internkontrollen ska styrelsen regelbundet få rapporter om de viktigaste operativa riskerna och skadehändelserna.

Anvisning (styckena 27-30)

(27) Finansinspektionen rekommenderar att rapporterna innehåller till exempel en beskrivning av förlusthändelsen, orsakerna till händelsen, uppskattning av direkta och indirekta kostnader och åtgärder för att förebygga liknande skador. Dessutom rekommenderas att uppgifter lämnas om vilka åtgärder som har vidtagits med anledning av skadan, vem som ansvarar för dem och tidsplanen för de korrigerande åtgärderna.

(28) Finansinspektionen rekommenderar att den verkställande ledningen regelbundet verifierar tidsenligheten, riktigheten och relevansen av rutinerna och rapporteringssystemen. Rapporternas innehåll och detaljrikedom, målgruppen för rapporterna och rapporteringsfrekvensen bör regelbundet ses över.

(29) För att säkerställa en tillfredsställande övervakning och rapportering rekommenderar Finansinspektionen att det fastställs en beloppsgräns för rapportering av transaktioner. Även små skador och s.k. nära ögat-situationer bör rapporteras om de är av principiell betydelse för riskhanteringens funktion.

(30) Finansinspektionen rekommenderar att övervakningen av förluster på grund av operativa risker läggs upp enligt följande tabell.

Förlusttyp	**Exempel**
Interna oegentligheter	förskingring, bedrägeri, tagande av muta, värdepappersmarknadsbrott eller -förseelse, skadegörelse, avsaknad av befogenheter (eller överskridande av dem), missbruk av kunduppgifter, avsiktlig felrapportering av positioner, yppande av affärshemlighet, utpressning
Extern brottslighet	stöld, rån, bedrägeri (t.ex. med betalningsmedel), förfalskning, penningtvätt, intrång i IT-system, spridning av skadliga program, överbelastningsattack mot IT-system, bombhot, hot mot personalen, utpressning
Arbetsmiljö och arbetarskydd	brott mot arbetsavtalslagen (bl.a. arbetstid, arbetarskydd), ersättningsanspråk med anledning av diskriminering, löne-, ersättnings- eller uppsägningstvister, arbetsmarknadskonflikter

Förluster på grund av affärspraxis	marknadsföring och tillhandahållande av tjänster som strider mot lag och god sed eller annars är vilseledande, missbruk av konfidentiella kunduppgifter (t.ex. för marknadsföring), försummelse av informationsskyldigheten gentemot en kund, försummelse av tystnadsplikten, försummelse av utredningsplikten, uppdragsutförande som strider mot bestämmelserna, regelvidrig hantering av kundmedel, värdepappersmarknadsbrott eller - förseelse, penningtvätt
Egendomsskada	eldsvåda, vattenskada, översvämning
Störningar och avbrott i IT-system	programfel, störning i datakommunikationen, driftavbrott, apparathaveri, elavbrott, störning hos en extern tjänsteproducent
Processproblem	rapporteringsfel, fel i kunduppgifterna, inmatningsfel i IT-systemet, prissättningsfel, ogiltigt avtal, bristfällig dokumentation, försvunna dokument, brister i säkerhetshanteringen, misslyckat utförande av kunduppdrag, störning i utlagd verksamhet, tvist med utomstående leverantör, redovisningsfel

5 Delområden i hanteringen av operativa risker

5.1 Processer

(1) Med process avses i detta kapitel en helhet av verksamheter och resurser som skapats i syfte att framställa en viss tjänst eller produkt. I hanteringen av processerna ingår aspekter som gäller kundtillfredsställelse, effektivitet, lönsamhet och verksamhetens pålitlighet och kvalitet. Kartläggning av de operativa risker som hänför sig till olika processfaser hjälper tillsynsobjekten att identifiera och reducera de operativa riskerna.

(2) Med stöd av avsnitt 2.4 om rätten att meddela föreskrifter meddelar Finansinspektionen följande föreskrift om organisation av riskhanteringen.

Föreskrift (stycke 3)

(3) Tillsynsobjekten ska identifiera de processer som är viktigast för verksamheten. Kontroller ska byggas in i de olika faserna av processerna och kvaliteten på dem utvärderas regelbundet, särskilt när verksamhetens omfattning eller innehåll förändras eller processerna ändras.

Anvisning (styckena 4-6)

(4) Finansinspektionen rekommenderar att tillsynsobjektet lägger särskild vikt vid gränssnitten mellan olika organisatoriska enheter och företag, eventuella avbrott i processerna, gränsöverskridande verksamhet och betalningar.

(5) Finansinspektionen rekommenderar att processer som är viktigast för verksamheten dokumenteras så enhetligt som möjligt med beskrivningar av de uppgifter som hänför sig till processen, processens olika faser och deras samband och riskställen. Vidare ska data- och materialflöden, rapportering och processens intressegrupper och IT-system dokumenteras. Särskild vikt ska fästas vid dokumentationen av och rutinerna för hantering av stora transaktionsvolymer. Processbeskrivningarna bör uppdateras regelbundet.

(6) Finansinspektionen rekommenderar att så samordnade principer som möjligt tillämpas vid genomförandet av olika projekt. För viktiga projekt bör riskbedömningar göras på förhand.

5.2 Legal risk

(7) Legal risk kan uppstå på grund av externa faktorer såsom förändringar i omvärlden men också på grund av tillsynsobjektens egen verksamhet. Legala risker kan ingå i all verksamhet. I tolkningen, räckvidden och giltigheten av de regelverk och föreskrifter som gäller tillsynsobjektens verksamhet ingår osäkerhetsfaktorer som kan leda till betydande förluster och som kan inverka på tillsynsobjektets juridiska ansvar och eventuella ersättningsskyldighet.

(8) Tvister om avtalens giltighet och innehåll kan skada tillsynsobjektets verksamhet. Att lösgöra sig från ogynnsamma avtal och ingå ersättande avtal kan medföra risk för förlust. Detta gäller särskilt avtal med standardvillkor. Också dokument som tillsynsobjekten har offentliggjort, exempelvis broschyrer och reklam kan vara förknippade med risk för skadestånd eller försämrat rykte och minskad respekt.

(9) Med stöd av avsnitt 2.4 om rätten att meddela föreskrifter meddelar Finansinspektionen följande föreskrift om organisation av riskhanteringen.

Föreskrift (stycke 10)

(10) Styrelsen måste vara medveten om de viktigaste legala riskerna i verksamheten och säkerställa en tillfredsställande hantering av legala risker.

Anvisning (styckena 11-15)

(11) Finansinspektionen rekommenderar att den verkställande ledningen lägger upp rutiner för hantering av den legala risken och tilldelar tillräckligt med resurser för identifiering, övervakning och reducering av den legala risken inom olika affärsområden.

(12) Finansinspektionen rekommenderar att tillsynsobjekten ser till att de har den sakkunskap som behövs för hantering av den legala risken i samband med avtal och andra rättshandlingar. Tillsynsobjekten bör se till att den som företräder avtalsparten har rätt att underteckna avtalet.

(13) Finansinspektionen rekommenderar att tillsynsobjektet arkiverar avtalsdokumentationen på lämpligt sätt och följer upp avtalens giltighet och eventuella tolkningstvister eller processer.

(14) Finansinspektionen rekommenderar att tillsynsobjekten bevakar förändringar av såväl lagstiftning som internationella regelverk för att på förhand kunna förbereda sig för de krav som nya lagar och föreskrifter ställer. Tillsynsobjekten bör känna till rättspraxis inom den egna branschen.

(15) Finansinspektionen rekommenderar att finans- och försäkringskonglomeratets moderbolag sörjer för att samtliga företag som hör till konglomeratet har tillräcklig sakkunskap om de bestämmelser och föreskrifter som gäller för båda sektorerna. Företag med verksamhet i flera stater bör beakta att viktiga rättsprinciper och rättspraxis kan variera betydligt mellan olika stater.

5.3 Personal

(16) Med stöd av avsnitt 2.4 om rätten att meddela föreskrifter meddelar Finansinspektionen följande föreskrift om organisation av riskhanteringen.

Föreskrift (styckena 17-20)

(17) Tillsynsobjektet ska se till att de anställda och personer som rekryteras till företaget har tillräcklig kompetens i förhållande till arbetsuppgifterna och företagets storlek och till verksamhetens omfattning och art.

(18) Tillsynsobjektet ska lägga upp rutiner för att säkerställa att de anställda kontinuerligt uppfyller kompetenskraven, dvs. har formell kompetens och tillräcklig utbildning och erfarenhet. Särskild vikt ska fästas vid nyanställdas anseende och bakgrund.

(19) Den verkställande ledningen ska se till att det finns tillräckligt med personal för att klara av uppgifterna. För att kontinuiteten ska kunna säkerställas ska särskilt personer i nyckelställning ha ersättare för den händelse att anställningsförhållandet plötsligt upphör eller avbryts.

(20) Tillsynsobjektet ska genom att lägga upp nödvändiga rutiner säkerställa att företagets anställda inte yppar detaljer om en kunds eller annan med företagets verksamhet förknippad persons

ekonomiska ställning eller privata förhållanden eller affärs- eller yrkeshemligheter. Yppande av dessa detaljer kan ske enbart då de i lag stadgade förutsättningarna uppfylls.

6 IT-system och informationssäkerhet

6.1 IT-system

(1) Enligt 9 kap. 16 § 2 mom. i KIL ska ett kreditinstitut ha adekvata, trygga och funktionssäkra betalnings- och värdepapperssystem och andra datasystem.

(2) Med stöd av avsnitt 2.4 om rätten att meddela föreskrifter meddelar Finansinspektionen följande föreskrifter om organisation av riskhanteringen.

Föreskrift (styckena 3-6)

(3) Styrelsen ska säkerställa att institutets IT-system är tillräckliga och lämpliga i förhållande till verksamhetens art och omfattning. Detta ska avgöras utgående från institutets verksamhet, styrelsens krav och det faktum att systemen ska stödja verksamheten enligt styrelsens riktlinjer.

(4) Tillsynsobjekten ska ha den kompetens, organisation och internkontroll som behövs för att registrera, överföra, behandla och arkivera data elektroniskt. Om dessa verksamheter läggs ut på entreprenad, ska tillsynsobjektet se till att leverantören av databehandlingstjänster följer de principer som fastställs i detta kapitel.

(5) Styrelsen ska anta en IT-strategi för att säkerställa en IT-miljö som är lämplig för tillsynsobjektets nuvarande och beräknade framtida behov och se över strategin med jämna mellanrum. Styrelsen ska också följa upp IT-kostnaderna.

(6) Standardrutiner ska också finnas för driftsättning, ändringshantering och testning av systemen. Systemen ska noggrant testas innan de sätts i drift. Systemen ska vid behov belastnings- och kapacitetstestas.

Anvisning (styckena 7-10)

(7) Finansinspektionen rekommenderar att tillsynsobjektet tar fram ett handlingsmönster som säkerställer samarbetet mellan verksamhetsenheterna och de enheter som tillhandahåller IT-tjänster. Tillsynsobjekten bör dock hålla i sär systemutveckling och datadrift.

(8) Finansinspektionen rekommenderar att tillsynsobjekten tar fram metoder för systemutveckling och kvalitetssäkring som säkerställer att systemen fungerar såsom planerat. Vidare bör systemen dokumenteras i sådan form att de går att använda och utveckla i framtiden även om exempelvis nyckelpersoner byts ut.

(9) Finansinspektionen rekommenderar att tillsynsobjekten beskriver rutinerna för köp av viktig program- och maskinvara eller kontraktering till externa tjänsteproducenter. Instituten bör säkerställa att nyanskaffningar och avtal motsvarar dess behov och kvalitetsmålen för verksamheten och garanterar fortlöpande service.

(10) Finansinspektionen rekommenderar att tillsynsobjekten beaktar Europeiska bankmyndighetens riktlinjer om IKT-riskbedömning inom ramen för översyns- och utvärderingsprocessen (ÖUP) i hanteringen av sina IT-risker. (Utfärdats 6.11.2017, gäller från 1.3.2018)

6.2 Informationssäkerhet

6.2.1 Definition av informationssäkerhet och grundläggande krav

(11) Informationssäkerhet innebär att företagets data, tjänster, system och datakommunikationer är skyddade och säkerställda under både normala och exceptionella förhållanden genom administrativa, tekniska och andra åtgärder.

(12) Med stöd av avsnitt 2.4 om rätten att meddela föreskrifter meddelar Finansinspektionen följande föreskrifter om organisation av informationssäkerheten.

Föreskrift (styckena 13-17)

(13) Tillsynsobjektens allmänna informationssäkerhet och de olika IT-systemens säkerhetsnivåer ska vara tillfredsställande i förhållande till verksamhetens art och omfattning, hoten mot systemen och den allmänna tekniska utvecklingsnivån.

(14) Styrelsen svarar för att tillsynsobjektets informationssäkerhet är tillfredsställande. Den allmänna nivån på informationssäkerheten ska fastställas och godkännas av styrelsen. Tillsynsobjektet ska tilldela tillräckliga resurser och delegera ansvaret för att informationssäkerheten håller tillräckligt hög nivå. Tillsynsobjektet ska regelbundet bedöma informationssäkerheten. Konstaterade brister i säkerheten ska omedelbart åtgärdas.

(15) Tillsynsobjekten ska fastställa ägarna till den information som företaget förvarar och hanterar och de system som företaget använder. Ägarna ska svara för principerna för användning av informationen och systemen, behörigheter och säkerhet. Tillsynsobjekten ska klassificera den information som förvaras och hanteras enligt säkerhetskraven och utarbeta hanteringsregler för olika säkerhetsklasser.

(16) Tillsynsobjekten ska bevilja behörighet att använda information, program och system samt övervaka användningen av systemen enligt samordnade principer som godkänts av ledningen. Tilldelningen av användarbehörigheter ska basera sig på användarens arbetsuppgifter. Tillsynsobjekten ska begränsa tillträdet till data, program och system med tekniska metoder. Överskridningar av användarbehörigheterna ska undersökas och rapporteras till de systemansvariga inom organisationen.

(17) Systemen ska ha en åtkomstkontroll. Också oavvisligheten av de transaktioner som utförs samt identifieringen och autentiseringen av de kommunicerande parterna ska vara säkerställd. Vidare ska de transaktioner som hanteras i systemen kunna spåras.

Anvisning (styckena 18-19)

(18) Finansinspektionen rekommenderar att tillsynsobjekten i tillämpliga delar utnyttjar den allmänna anvisning som ledningsgruppen för datasäkerheten inom statsförvaltningen har gett ut.[1]

[1] *Anvisning om verkställighet av förordningen om informationssäkerheten inom statsförvaltningen, VAHTI 2/2010*

(19) Finansinspektionen rekommenderar att det vid utvecklingen av tjänsterna säkerställs att transaktionerna loggförs på behörigt sätt. Vidare ska avseende fästas vid åtkomstkontroll och identifiering och autentisering av användarna.

6.2.2 Hantering av informationssäkerhetsrisker och incidenthantering

(20) Med incident avses en händelse eller åtgärd som strider mot företagets informationssäkerhetsprinciper, exempelvis virusattack, intrång i IT-system eller informationsläckage.

(21) Med stöd av avsnitt 2.4 om rätten att meddela föreskrifter meddelar Finansinspektionen följande föreskrifter om organisation av hanteringen av informationssäkerhetsrisker.

Föreskrift (styckena 22-24)

(22) Rutiner för bedömning av informationssäkerhetsriskerna ska byggas in i riskhanteringen för att styrelsen och verkställande ledningen ska kunna bilda sig en uppfattning om samverkan mellan alla väsentliga risker i verksamheten.

(23) Bedömningen av informationssäkerhetsnivån ska basera sig på regelbunden analys av riskerna i informationssäkerheten. Riskanalyserna ska fastställa tillsynsobjektets viktigaste verksamheter och resurser och hotbilderna mot dem och verksamheternas och resursernas sårbarhet för hoten. Vidare ska uppskattas eventuella effekter på institutets verksamhet om hoten realiseras. För hantering av identifierade risker ska tillräckliga kontroller byggas in. Också riskerna med nya system, tekniker och tjänster ska bedömas före introduktionen.

(24) Incidenter som gäller bristande informationssäkerhet ska identifieras, analyseras, arkiveras och rapporteras till namngivna ansvariga inom organisationen.

6.2.3 Regler och utbildning om informationssäkerhet

(25) Till informationssäkerhetsreglerna hör bland annat bestämmelser om fastställande av behörigheter, bekämpning av skadliga program samt användningen av Internet och e-post.

(26) Med stöd av avsnitt 2.4 om rätten att meddela föreskrifter meddelar Finansinspektionen följande föreskrifter.

Föreskrift (styckena 27-28)

(27) Tillsynsobjekten ska ha uppdaterade informationssäkerhetsprinciper som är godkända av styrelsen och andra informationssäkerhetsregler, som företagets anställda ska få kännedom om.

(28) Tillsynsobjekten ska klart fastställa informationssäkerhetsansvaret för varje anställd och ge de anställda regelbunden informationssäkerhetsutbildning. Informationssäkerheten ska kontinuerligt utvecklas och ansvaret för detta ska klart fastställas på chefsnivå.

6.2.4 Informationssäkerheten i datanätet

(29) Onlinetjänsternas informationssäkerhet beror bland annat på hur säkra de handlingsmönster, tillämpningar, tekniska system och datakommunikationer som används för tjänsterna är.

(30) Med stöd av avsnitt 2.4 om rätten att meddela föreskrifter meddelar Finansinspektionen följande föreskrift.

Föreskrift (styckena 31-32)

(31) Tillsynsobjekten ska bedöma om tjänsterna är lämpliga att tillhandahålla över datanätet innan existerande eller nya tjänster introduceras i nätet. De största riskerna med tjänsterna och riskhanteringsmetoderna ska dokumenteras och nödvändiga kontroller byggas in i systemet. Riskhanteringen och internkontrollen av online-verksamhet, IT-system och interna processer ska planeras och läggas upp så att verksamhetens art och omfattning och hoten mot verksamheten beaktas.

(32) Tillsynsobjekten ska på löpande basis analysera och utveckla sina IT-system och informationssäkerheten samt på ett tillfredsställande sätt skydda sig mot olika störningar och eventuellt missbruk.

6.2.5 Utveckling av säkra onlinetjänster

(33) Med stöd av avsnitt 2.4 om rätten att meddela föreskrifter meddelar Finansinspektionen följande föreskrift.

Föreskrift (stycke 34)

(34) Tillsynsobjektet ska bedöma informationssäkerhetsriskerna när det utvecklar nya tjänster. Tillsynsobjektet ska vidta de riskhanteringsåtgärder som föranleds av riskanalysen.

Anvisning (stycke 35)

(35) Finansinspektionen rekommenderar att tillsynsobjekten för att trygga informationssäkerheten ser till att åtminstone följande kriterier uppfylls både innan de lanserar en tjänst och fortlöpande därefter:

- Testning och besiktning av informationssäkerheten har genomförts i alla system och fortlöpande bevakning och rapportering av säkerhetsnivån och eventuella störningar i systemen finns på plats. Med besiktning av informationssäkerheten avses systematisk granskning av säkerhetsnivån i ett system, en tjänst eller en verksamhet för att säkerställa att den målsatta säkerhetsnivån har uppnåtts.
- För att säkerställa tjänstens användbarhet och kontinuitet har reservrutinerna beskrivits i förväg och återställningsplaner tagits fram för systemen.
- Systemen är försedda med nödvändiga mekanismer för bekämpning av virus och andra skadliga program.

- Systemen och datakommunikationerna är tillräckligt skyddade till exempel för överbelastningsattacker. Systemen är försedda med en mekanism för behörighetskontroll och tillsynsobjekten har sörjt för att behörighetshanteringen har ordnats på behörigt sätt.
- Det externa nätet har skiljts åt från tillsynsobjektens interna nät med säkerhetsanordningar.
- Systemen testas regelbundet och särskilt efter systemändringar. Identifierade säkerhetsbrister åtgärdas omedelbart.
- Innan ibruktagning av webbtjänster utförs auditering av informationssäkerheten, detta utförs även regelbundet under den tid som webbtjänster erbjuds.
- Tillsynsobjekten har säkerställt att dataöverföringen i internettjänsten mellan tjänstemottagaren och tjänsteleverantören och databehandlingen i tjänsteleverantörens system uppfyller kraven på konfidentialitet, integritet och oavvislighet. Också identifieringen och autentiseringen av sinsemellan kommunicerande parter bör vara tillförlitlig.
- Tillsynsobjekten har försett IT-systemen med kontrollmekanismer och spårningskedjor som säkerställer in- och utdatas riktighet och integritet. De transaktioner som handläggs i systemet bör kunna spåras.
- Systemen har inbyggda kontroller som möjliggör avstämning av transaktioner som har utförts i olika system.
- Med tanke på störningar och avbrott i verksamheten eller i systemet har reservsystem med alternativa verksamhetsmodeller eller system lagts upp när tjänsterna byggts upp. Reservsystem är exempelvis dubblering av viktiga komponenter som behövs i databehandlingen och datakommunikationen samt säkerhetskopiering.
- Eventuella lösenord för kunder har krypterats inom systemet och vid överföring mellan systemen.
- Vid uppläggning, behandling och överlämning till kunden av dennes identifikationsuppgifter (användaridentitet och lösenord) har extra aktsamhet iakttagits och s.k. farliga arbetskombinationer undvikits.
- Systemen har fört en logg över inloggning, försök till inloggning och användning av tjänsten. Loggarna och loggrapporterna gås igenom regelbundet.
- Kunden får tillräckligt med information om tjänsteleverantören, den tjänst som marknadsförs, om ansvarsfördelningen mellan den som tillhandahåller och den som utnyttjar tjänsten och om hur kunden tryggt kan utnyttja tjänsten.

7 Betalningssystem och betalningsförmedling

(1) Enligt 9 kap. 16 § 2 mom. i KIL ska ett kreditinstitut ha adekvata, trygga och funktionssäkra betalnings- och värdepapperssystem och andra datasystem.

(2) Enligt 19 a och 19 b § i betaltjänstlagen ska tillsynsobjekt som tillhandahåller betaltjänster och personer utan auktorisation som tillhandahåller betaltjänster ha tillräckliga riskhanteringssystem för att hantera operativa risker och säkerhetsrisker i anslutning till de betaltjänster som de tillhandahåller samt för uppföljning och rapportering av incidenter och bedrägerier. (Utfärdats 29.1.2018, gäller från 1.3.2018)

(3) Med betalningssystem avses i regel ett system

- där överenskomna betalningsmedel används
- där deltagarna är kreditinstitut, betalningsinstitut och clearingorganisationer
- där deltagarna kommer överens om olika betalningsförmedlings- och riskhanteringsrutiner
- som möjliggör förmedling av transaktioner från betalaren till mottagaren.

(4) Avvecklingssystemet fungerar som förmedlare av betalningstransaktioner i överföringen av medel mellan bankerna och kan också tillhandahålla tjänster för avveckling av betalningstransaktioner.

(5) Med betalningsmedel avses betalkort, annat personligt instrument eller förfarande eller en kombination av dem som enligt överenskommelse mellan användaren och tjänsteleverantören får användas för att utföra betalningsorder.

(6) Med stöd av avsnitt 2.4 om rätten att meddela föreskrifter meddelar Finansinspektionen följande föreskrifter.

Föreskrift (styckena 7-11)

(7) Styrelsen ska godkänna principer för betalningsförmedling för de betalnings- och avvecklingssystem i vilka institutet deltar och för de betaltjänster som institutet tillhandahåller för sina kunder. Betalningsförmedlingsprinciperna ska omfatta den nuvarande verksamheten och de ska ta hänsyn till den beräknade utvecklingen under de närmaste åren. Styrelsen ska uppställa mål för verksamheten i syfte att säkerställa en effektiv, högklassig och säker betalningsförmedling och övervaka verksamheten. Tillsynsobjektets avvecklingssystem ska också uppfylla dessa mål.

(8) Den verkställande ledningen svarar för att det finns tillfredsställande kompetens, resurser och internkontroll för en effektiv och säker betalningsförmedling. Tillsynsobjekten ska kartlägga riskerna med de betalningssystem och betaltjänster som används och regelbundet uppdatera kartläggningarna.

(9) Tillsynsobjektens betalningssystem ska vara välfungerande, funktionssäkra och stabila. Tillsynsobjekten ska sörja för att det förekommer så få störningar och dröjsmål som möjligt i betalningsförmedlingen. Det ska finnas tillräckliga reservsystem för hantering av betalningsförmedlingen mellan bankerna.

(10) Tillsynsobjekt som tillhandahåller betaltjänster och personer som utan auktorisation tillhandahåller betaltjänster ska ha tillräckliga riskhanteringsmetoder i anslutning till de

betaltjänster som de tillhandahåller för att hantera operativa risker och säkerhetsrisker. (Utfärdats 29.1.2018, gäller från 1.3.2018)

(11) Tillsynsobjekt som tillhandahåller betaltjänster och personer utan auktorisation som tillhandahåller betaltjänster ska upprätta en bedömning av operativa risker och säkerhetsrisker för betaltjänster, vilken även inkluderar en bedömning av om deras riskhanteringsåtgärder och kontrollmekanismer är tillräckliga. Bedömningen ska inlämnas till Finansinspektionen varje år enligt avsnitt 9.3. (Utfärdats 29.1.2018, gäller från 1.3.2018)

Anvisning (styckena 12-16)

(12) Finansinspektionen rekommenderar att tillsynsobjekten lämnar riskanalyser om nya tjänster, system och tekniker för betalningsförmedlingen till Finansinspektionen innan de introduceras. Riskanalyser bör likaså lämnas in till Finansinspektionen före introduktionen av betydande ändringar i betalningsförmedlingen eller avvecklingssystemen.

(13) Finansinspektionen rekommenderar att tillsynsobjekten underrättar Finansinspektionen om nya betaltjänster och betydande ändringar i existerande tjänster i god tid på förhand innan de introduceras.

(14) Finansinspektionen rekommenderar att företag under tillsyn beaktar Europeiska bankmyndighetens riktlinjer för hantering av IKT- och säkerhetsrisker (EBA/GL/2019/04) (30 June 2020) när de tillhandahåller och utvecklar betalningstjänster. (Utfärdats 16.2.2022, gäller från 1.3.2022)

(15) Finansinspektionen rekommenderar att tillsynsobjekt som tillhandahåller betaltjänster och personer utan auktorisation som tillhandahåller betaltjänster följer Europeiska bankmyndighetens riktlinjer för hantering av IKT- och säkerhetsrisker **(**EBA/GL/2019/04) **(**30 June 2020) när de tillhandahåller betaltjänster. (Utfärdats 16.2.2022, gäller från 1.3.2022)

(16) Finansinspektionen rekommenderar att tillsynsobjekt som deltar i systemviktiga betalnings- eller avvecklingssystem i tillämpliga delar följer ECB:s förordning ECB/2014/28, som genomför CPSS-kommitténs och IOSCOs gemensamma rekommendation Principles for financial market infrastructures.

8 Kontinuitets- och beredskapsplanering

8.1 Regelverk

(1) Enligt 9 kap. 16 § 3 mom. i KIL ska ett kreditinstitut ha beredskaps- och kontinuitetsplaner för att bereda sig för allvarliga störningar i affärsverksamheten samt säkerställa sin förmåga att fortlöpande bedriva verksamhet och begränsa förlusterna i störningssituationer.

(2) Enligt 5 kap. 16 § i KIL ska kreditinstitut genom deltagande i beredskapsplanering på finansmarknaden och genom förberedelser för undantagsförhållanden samt genom andra åtgärder säkerställa att deras uppgifter kan skötas så störningsfritt som möjligt också under undantagsförhållanden.

(3) Enligt 18 kap. 5 § i KIL gäller vad som föreskrivs i 5 kap. 17 § om beredskap för undantagsförhållanden också filialer till utländska kreditinstitut. Detta gäller inte filialer till utländska EES-kreditinstitut till den del filialen med stöd av lagstiftningen i kreditinstitutets hemstat har säkerställt att dess uppgifter under undantagsförhållanden sköts i överensstämmelse med 18 kap. 5 § i KIL och presenterat en tillräcklig utredning om detta för Finansinspektionen.

(4) Enligt 41 a § i BIL ska betalningsinstitut genom deltagande i beredskapsplanering på finansmarknaden och genom förberedelser för undantagsförhållanden samt genom andra åtgärder säkerställa att deras uppgifter kan skötas så störningsfritt som möjligt också under undantagsförhållanden. Motsvarande beredskapsskyldighet gäller också utländska betalningsinstituts filialer.

(5) Enligt 7 kap. 8 § i lagen om investeringstjänster ska värdepappersföretag vilka såsom sidotjänster tillhandahåller förvaring av finansiella instrument genom deltagande i beredskapsplanering på finansmarknaden och genom förberedelser för undantagsförhållanden samt genom andra åtgärder säkerställa att deras uppgifter kan skötas så störningsfritt som möjligt också under undantagsförhållanden. Enligt 1 kap. 4 § 2 mom. i ITL tillämpas bestämmelserna om beredskapsplanering på AIF-förvaltare som tillhandahåller investeringstjänster. (Utfärdats 29.1.2018, gäller från 1.3.2018).

(6) Enligt 7 kap.15 § i lagen om investeringstjänster gäller det som föreskrivs om beredskap i 8 § på motsvarande sätt utländska EES-värdepappersföretags filialer. Enligt 1 kap. 7 § i lagen om investeringstjänster ska på tredjelandsföretag som tillhandahåller investeringstjänster eller bedriver investeringsverksamhet i Finland via filialer i fråga om dessa tjänster tillämpas vad som föreskrivs i 7 kap. 15 § i lagen om investeringstjänster. (Utfärdats 29.1.2018, gäller från 1.3.2018).

(7) Enligt 4 a § i PlacFL ska fondbolag genom deltagande i beredskapsplanering på finansmarknaden och förberedelser av verksamhet under undantagsförhållanden samt genom andra åtgärder säkerställa att deras uppgifter kan skötas så störningsfritt som möjligt också under undantagsförhållanden. Enligt 1 kap. 6 § 2 mom. i lagen om förvaltare av alternativa investeringsfonder tillämpas beredskapsskyldigheten enligt 7 kap. 8 § i ITL på AIF-förvaltare som tillhandahåller investeringstjänster enligt 3 kap. 2 § i lagen. (Utfärdats 29.1.2018, gäller från 1.3.2018).

(8) Enligt 2 kap. 12 § i lagen om värdeandelssystemet och om clearingverksamhet ska värdepapperscentralen säkerställa att uppgifterna i värdeandelssystemet kan förvaras så störningsfritt som möjligt också under undantagsförhållanden. Detta ska ske genom tillräckligt

omfattande IT-system i Finland eller genom andra arrangemang som är tillräckliga för att verksamheten inte ska avbrytas, genom deltagande i beredskapsplanering på finansmarknaden och förberedelser av verksamhet under undantagsförhållanden samt genom andra motsvarande åtgärder. (Utfärdats 29.1.2018, gäller från 1.3.2018).

8.2 Kontinuitetsplanering

(9) Med kontinuitetsplanering avses säkerställande av förmågan att upprätthålla verksamheten och begränsa förluster i händelse av olika slag av störningar i verksamheten. Hit hör till exempel skador eller avsiktliga handlingar som drabbar personalen, lokalerna, IT-systemen eller datakommunikationerna samt vattenskador, eldsvådor och avbrott i exempelvis el-, värme- eller vattenförsörjningen. Inom ramen för kontinuitetsplaneringen upprättas kontinuitetsplaner för viktiga verksamheter för att upprätthålla verksamheten i händelse av eventuella störningar.

(10) Med stöd av avsnitt 2.4 om rätten att meddela föreskrifter meddelar Finansinspektionen följande föreskrifter om kontinuitetsplaneringen.

Föreskrift (styckena 11-18)

(11) Styrelsen svarar för att det finns uppdaterade och tillräckliga kontinuitetsplaner för företagets centrala verksamheter. Den verkställande ledningen ska fastställa ansvaret för kontinuitetsplaneringen. Tillsynsobjekten ska ha ett tydligt handlingsmönster för upprättande, underhåll och testning av kontinuitetsplaner och för uppföljning av kontinuitetsplaneringen.

(12) Tillsynsobjekten ska kartlägga och prioritera de viktigaste verksamhetsprocesserna och fastställa återställningstider för dem, dvs. det längsta tillåtna avbrottet som inte stör verksamheten. För de prioriterade processerna ska alternativa handlingsmönster och återställningsrutiner läggas upp för eventuella avbrott. Extra uppmärksamhet bör ges möjligheten att återställa information som är nödvändig för att verksamheten ska kunna återupptas.

(13) IT-system och tillämpningar ska rangordnas efter det hur snabbt de ska kunna återställas efter olika typer av störningar. För IT-systemen ska det upprättas återställningsplaner med beskrivningar av hur systemen kan fås funktionsdugliga efter allvarliga störningar eller katastrofer.

(14) Säkerhetskopiorna och en eventuell reservanläggning ska placeras så långt bort från den egentliga datacentralen att data och säkerhetskopior inte kan förstöras samtidigt.

(15) Kontinuitetsplanerna ska grunda sig på risk- och sårbarhetsanalyser, dvs. på en utredning om de hot, sårbarheter och risker som riktar sig mot data, system, funktioner och tjänster.

(16) Kontinuitetsplanerna ska beakta olika hotbilder avseende verksamheten och funktionernas sårbarhet. Kontinuitetsplanerna ska dimensioneras efter verksamhetens art, omfattning och komplexitet. De ska styra verksamheten och informationsgivningen vid olika typer av störningar.

(17) Tillsynsobjekten ska bereda sig på störningar i externa tjänsteleverantörers verksamhet. Kontinuitetsplanerna ska beskriva åtgärderna för att förebygga effekterna av störningar i externa tjänsteleverantörers verksamhet och hur tillsynsobjekten övervakar externa tjänsteleverantörers kontinuitetsplanering. I avtalen med externa tjänsteleverantörer ska förutsättas att de utvärderar, uppdaterar och testar sina system för störningar.

(18) Kontinuitetsplanerna ska revideras regelbundet och anpassas till förändringar i verksamhet, tjänster eller strategier. Kontinuitetsplanerna ska testas och regelbundna övningar ordnas. Ansvariga ska utses för att övervaka uppdateringen och testningen av kontinuitetsplanerna.

8.3 Beredskap för undantagsförhållanden

(19) Kraven på beredskap för undantagsförhållanden grundar sig på beredskapslagen och andra myndighetsdirektiv om beredskap för undantagsförhållanden. Med undantagsförhållanden avses situationer enligt 3 § i beredskapslagen. Beredskapen för undantagsförhållanden bygger på kontinuitetssystemen för normala förhållanden.

(20) En störning under undantagsförhållanden varar i typiska fall längre än situationer för vilka det finns beredskap i kontinuitetsplanen för normala förhållanden. Hot under undantagsförhållanden är vidare i regel allvarligare än de hot för vilka kontinuitetsplaner upprättas.

(21) Dessa anvisningar om beredskap för undantagsförhållanden kan också tillämpas på andra allvarliga störningar och kriser än undantagsförhållanden enligt beredskapslagen. Allvarliga störningar och kriser kan uppstå till exempel vid allvarliga hot mot personalens handlingsförmåga eller förstörelse av tillsynsobjektets lokaler eller datormiljö.

(22) Statsrådet har i sitt beslut av den 5 december 2013 ställt upp allmänna mål för försörjningsberedskapen. I finansförsörjningspoolens beredskapsanvisningar från 2009 ställs noggrannare beredskapsmål och lämnas mer detaljerade anvisningar om beredskap för undantagsförhållanden.

Föreskrift (styckena 23-30)

(23) Finansinspektionen rekommenderar att tillsynsobjektet genomför en riskanalys för att fastställa om de driftssystem som används för produktion av viktiga tjänster och den kompetens som behövs för deras styrning, underhåll, systemhantering och tekniska stöd ska bevaras helt eller delvis i Finland eller om det räcker att de kan återtas till Finland enligt förhandsplanerade rutiner.

(24) Finansinspektionen rekommenderar att tillsynsobjekten sörjer för reservsystem som säkerställer betalningsförmedlingen mellan bankerna, clearing, avveckling och förvaring av värdepapper och utbetalningar av pensioner och andra återkommande betalningar också när kritiska system för dessa funktioner i eller utanför Finland inte är tillgängliga. Vidare ska tillsynsobjekten säkerställa en välfungerande infrastruktur för kortbetalningar och kortautentisering i Finland.

(25) Finansinspektionen rekommenderar att tillsynsobjektet ser till att inte hela systemet lamslås om en enskild funktion slås ut eller de IT-system eller datakommunikationssystem som behövs för produktion av viktiga tjänster skadas. Tillsynsobjekten bör lägga upp reservsystem för att förbereda sig för störningar i internationella och nationella datakommunikationer.

(26) Finansinspektionen rekommenderar att IT-system och datalager som behövs för produktion av viktiga tjänster sprids geografiskt till minst två platser med olika riskprofiler. Viktiga uppgifter och funktioner kan överföras till EU-området förutsatt att deras lagenlighet, säkerhet och användbarhet för uppfyllande av servicemålen i denna anvisning har tryggats.

(27) Finansinspektionen rekommenderar att tillsynsobjektet sörjer för tillgången till de viktigaste uppgifterna för produktion av tjänsterna så att uppgifter som är väsentliga för verksamhetens kontinuitet kan återkallas om de egentliga databehandlingscentralerna eller information och

säkerhetskopior i dem förstörs. Sådana basfakta är åtminstone basfakta om kunder och kundavtal (bl.a. personuppgifter) och uppgifter om kundernas tillgångar och skulder. Räddning av data från särskild säkerhetskopia till allmänt läsbart elektroniskt format bör testas.

(28) Finansinspektionen rekommenderar att tillsynsobjekten utsträcker beredskapen också till utlagda verksamheter i den utsträckning som detta krävs för att trygga de kärnfunktioner och kärntjänster som ska upprätthållas under undantagsförhållanden. Beredskapskraven bör beaktas när uppdragsavtal upprättas. De beredskapsskyldiga bör bedöma tjänsteleverantörens beredskap och sörja för att den motsvarar kraven. De beredskapsskyldiga bör bedöma tjänsteleverantörens beredskap till exempel genom att hålla gemensamma beredskapsövningar med leverantören.

(29) Finansinspektionen rekommenderar att de beredskapsskyldiga säkerställer att de har tillräckliga resurser och kapacitet för att upprätthålla verksamheten under undantagsförhållanden och vid allvarliga störningar. Tillgången till personella resurser och reservlokaler bör också planeras i förväg. Tillgången på resurser bör säkerställas genom förhandsåtgärder för sådana situationer då en stor del av personalen inte är tillgänglig, en del av de viktigaste lokalerna, utrustning och system har förstörts eller annars inte finns tillgängliga eller verksamheten har lamslagits på ett brett område.

(30) Finansinspektionen rekommenderar att de beredskapsskyldiga instituten sörjer för myndighetsrapporteringen även under undantagsförhållanden.

8.4 Beredskapsplan

(31) Med beredskapsplan avses en förhandsbeskrivning av de åtgärder som de beredskapsskyldiga vidtar för att säkerställa kontinuiteten i verksamheten vid allvarliga störningar under normala förhållanden och under undantagsförhållanden.

Beredskapsplanen kan ingå i kontinuitetsplanen, förutsatt att den i tillräcklig mån beaktar behoven av beredskap för undantagsförhållanden.

Föreskrift (styckena 32-33)

(32) Finansinspektionen rekommenderar att tillsynsobjekten har en beredskapsplan som uppdateras regelbundet. De beredskapsskyldiga tillsynsobjekten bör testa och regelbundet öva beredskapsplanen självständigt och tillsammans med andra marknadsaktörer.

(33) Finansinspektionen rekommenderar att tillsynsobjekten utser en eller flera personer som är ansvariga för att uppdatera och ge information om beredskapsplanen.

9 Rapportering till Finansinspektionen

9.1 Anmälan om störningar och fel i verksamheten

(1) Med stöd av rätten att meddela föreskrifter enligt avsnitt 2.4 meddelar Finansinspektionen följande föreskrifter om rapportering av uppgifter om internkontroll, riskhantering och störningar till Finansinspektionen. (Utfärdats 23.9.2019, gäller från 1.1.2020)

Föreskrift (styckena 2-7)

(2) Tillsynsobjektet ska utan dröjsmål göra en första anmälan till Finansinspektionen om betydande störningar och fel i tjänster som tillhandahålls för kunderna och i betalnings- och IT-systemen omedelbart när de yppat sig. En betydande störning i betalningsförmedlingen eller vid kortbetalningar är till exempel en störning eller ett dröjsmål som gäller ett stort antal kunder. En betydande störning är också en störning eller avvikelse i nätverks- och informationssäkerheten samt en störning där kundinformation har hamnat i händerna på utomstående. Finansinspektionen ska omedelbart underrättas också om sådana störningar och fel som skadar eller äventyrar tillsynsobjektets förmåga att fortsätta sin verksamhet eller svara för sina åtaganden. (Utfärdats 23.9.2019, gäller från 1.1.2020)

(3) I anmälan ska som kod anges ”informationssäkerhet”, om det är fråga om en avvikelse i informationssäkerheten och ”informationsskydd”, om det är fråga om en dataskyddskränkning. (Utfärdats 23.9.2019, gäller från 1.1.2020)

(4) Tillsynsobjektet ska lämna in en kompletterande anmälan till Finansinspektionen om de närmare detaljerna i störningen så snabbt som möjligt efter den första anmälan och en slutrapport efter att den egentliga orsaken till störningen har utretts. (Utfärdats 23.9.2019, gäller från 1.1.2020).

(5) Anmälan ska lämnas åtminstone om följande kategorier av störningar: (Utfärdats 23.9.2019, gäller från 1.1.2020).

- intrång i IT-system
- uppgifter har avslöjats för utomstående
- kränkning av informationssäkerheten
- spridning av fientliga program i IT-systemet
- överbelastningsattack.

Anmälan ska lämnas till Finansinspektionen endast för sådana fall då uppgifter har avslöjats för utomstående, som också måste rapporteras till dataombudsmannen. Anmälan kan lämnas till Finansinspektionen med samma rapport, som man använder till dataombudsmannen, om tillsynsobjektet så väljer.

För överbelastningsattack rapporteras endast sådana, som påverkar tjänsternas tillgänglighet eller brukbarhet.

(6) Anmälan ska också lämnas om följande störningar om de påverkar tjänsterna till kunden:

- programfel

- störning i datakommunikationen
- driftavbrott i systemet
- apparathaveri
- dröjsmål i betalningsförmedlingen.

(7) Tillsynsobjekt som tillhandahåller betaltjänster och person som utan auktorisation tillhandahåller betaltjänster ska rapportera om allvarliga operativa incidenter och säkerhetsincidenter som gäller betaltjänster till Finansinspektionen med iakttagande av Europeiska bankmyndighetens riktlinjer för rapportering om allvarliga incidenter.[3] Rapporteringen ska omfatta alla de uppgifter som nämns i riktlinjerna och rapporteringen ska följa de tidsfrister för klassificering och rapportering av incidenter som ges i riktlinjerna. (Utfärdats 29.1.2018, gäller från 1.3.2018)

Anvisning (styckena 8-10)

(8) Anmälan, en kompletterande anmälan och slutrapporten ska inlämnas på den blankettmall och enligt de instruktioner som finns på Finansinspektionens webbplats. (Utfärdats 1.12.2022, gäller från 1.1.2023)

(9) Betydande operativa störningar som gäller betaltjänsterna och säkerhetsstörningar ska rapporteras enligt Europeiska bankmyndighetens riktlinjer. Anmälan, en kompletterande anmälan och slutrapporten ska inlämnas på den blankettmall och enligt de instruktioner som finns på Finansinspektionens webbplats. För en dylik störning behövs ingen separat anmälan på Finansinspektionens blankettmall för störningsanmälan enligt stycke 8. (Utfärdats 1.12.2022, gäller från 1.1.2023)

(10) Anmälan till Finansinspektionen upphäver inte heller tillsynsobjektets skyldighet att rapportera om att uppgifter avslöjats för utomstående i enlighet med rapporteringsskyldigheterna i dataskyddsförordningen. (Utfärdats 23.9.2019, gäller från 1.1.2020).

9.2 Årsanmälan om förluster på grund av operativa risker

(11) Anmälan om förluster på grund av operativa risker till Finansinspektionen görs enligt tillsynsobjektets interna rapportering av förlustuppgifter. Anvisningar för rapportering av skador på grund av operativa risker finns i avsnitt 4.4.

(12) Med stöd av rätten att meddela föreskrifter enligt avsnitt 2.4 meddelar Finansinspektionen följande föreskrift om regelbunden rapportering av uppgifter om internkontroll och riskhantering till Finansinspektionen. (Utfärdats 29.1.2018, gäller från 1.3.2018)

[3] *Europeiska bankmyndighetens riktlinjer om rapporteringen av allvarliga incidenter (Revised Guidelines on major incident reporting under PSD2 (EBA/GL/2021/03)*

Anvisning (styckena 13-16)

(13) Tillsynsobjektet ska lämna in en årsanmälan till Finansinspektionen om förluster på grund av operativa risker som identifierats under föregående år. Anmälan ska lämnas in till Finansinspektionen före den 28 februari.

(14) Årsanmälan ska lämnas om de till beloppet fem största förlusthändelserna på grund av operativa risker under kalenderåret. Om skador under tiotusen euro (10 000) behövs dock ingen anmälan.

(15) Anmälan ska innehålla åtminstone följande uppgifter:

- beskrivning av händelsen och typ av skada enligt klassificeringen i avsnitt 4.4
- redogörelse för åtgärder som vidtagits på grund av händelsen
- redogörelse för förlustbeloppet och försäkringsersättning eller andra återbetalningar.

(16) Årsanmälan ska inlämnas på den blankettmall och enligt de instruktioner som finns på Finansinspektionens webbplats. (Utfärdats 1.12.2022, gäller från 1.1.2023)

Anvisning (styckena 17-18)

(17) Finansinspektionen rekommenderar att centralinstitutet för en sammanslutning av inlåningsbanker lämnar in en anmälan om förluster som drabbat tillsynsobjekt inom sammanslutningen och att Lokalandelsbanksförbundet lämnar in en anmälan om förluster som drabbat andelsbanker inom förbundet.

(18) Finansinspektionen rekommenderar att årsanmälan även görs i det fallet att ingen förlust uppstått. (Utfärdats 23.9.2019, gäller från 1.1.2020).

9.3 Årlig bedömning av de operativa riskerna och säkerhetsriskerna som gäller betaltjänster (Utfärdats 29.1.2018, gäller från 1.3.2018)

(19) Med stöd av rätten att meddella föreskrifter enligt avsnitt 2.4 meddelar Finansinspektionen följande föreskrift.

Föreskrift (stycke 20)

(20) Ett tillsynsobjekt som tillhandahåller betaltjänster och en person som tillhandahåller betaltjänster utan auktorisation ska lämna in en bedömning av de operativa riskerna och säkerhetsriskerna samt av riskhanteringsåtgärderna till Finansinspektionen varje år. En fritt formulerad riskbedömning ska inlämnas senast den 28 februari enligt de instruktioner som finns på Finansinspektionens webbplats. (Utfärdats 1.12.2022, gäller från 1.1.2023)

9.4 Rapportering av svikliga förfaranden i anslutning till betaltjänster (Utfärdats 23.9.2019, gäller från 1.1.2020)

(21) Enligt 3 kap. 19 § 4 mom. i lagen om betalningsinstitut ska betalningsinstitut och personer som utan auktorisation tillhandahåller betaltjänster till Finansinspektionen lämna in statistiska uppgifter om bedrägerier i samband med betalningsinstrument. Finansinspektionen får enligt 3 kap. 19 b § 4 mom. meddela närmare föreskrifter om rapporteringsskyldigheten. Lagrummet gäller med stöd av 9 kap. 16 § 4 mom. i kreditinstitutslagen även kreditinstitut som tillhandahåller betaltjänster.

(22) Europeiska bankmyndigheten har med stöd av artikel 16 i Europaparlamentets och rådets förordning (EU) nr 1093/2010 utfärdat riktlinjer om krav för rapportering av statistiska uppgifter om svikliga förfaranden enligt artikel 96.6 i det andra betaltjänstdirektivet. (EBA/GL/2018/05) Rapportering enligt dessa riktlinjer sker den sista gången för året 2021. För svikliga förfaranden under året 2022 kommer att rapporteras till Finlands Bank enligt riktlinjer från Europas Centralbank.

Föreskrift (styckena 23-26)

(23) Tillsynsobjekt som tillhandahåller betaltjänster och person som utan auktorisation tillhandahåller betaltjänster samt inhemska kreditinstitut som tillhandahåller betaltjänster och filialer till utländska kreditinstitut som tillhandahåller betaltjänster i Finland ska lämna in uppgifter till Finansinspektionen om svikliga förfaranden i anslutning till betalningsinstrument på MF-blanketten som finns att få via Jakelu-distributionstjänst. (Utfärdats 23.9.2019, gäller från 1.1.2020).

(24) Betalningsinstitut och kreditinstitut som tillhandahåller betalningstjänster ska lämna in uppgifterna varje halvår före den 28 februari och den 31 augusti. (Utfärdats 23.9.2019, gäller från 1.1.2020).

(25) Personer som utan auktorisation tillhandahåller betaltjänster ska lämna in uppgifterna varje år före den 28 februari. (Utfärdats 23.9.2019, gäller från 1.1.2020).

(26) En filial till ett utländskt betalnings- eller kreditinstitut som tillhandahåller betaltjänster i Finland ska lämna in uppgifterna till Finansinspektionen varje halvår den 28 februari och den 31 augusti. (Utfärdats 23.9.2019, gäller från 1.1.2020).

Anvisning (stycke 27)

(27) Finansinspektionen rekommenderar, till den del som det inte tidigare i detta avsnitt 9.4 särskilt har getts bindande föreskrifter om Europeiska bankmyndigheternas riktlinjer som avses ovan i stycke 20, att de som omfattas av detta kapitels tillämpningsområde följer nämnda riktlinjer. (Utfärdats 23.9.2019, gäller från 1.1.2020)

9.5 Ansökan om undantag från kravet på beredskapsmekanism för PSD2-specialgränssnittet (Utfärdats 23.9.2019, gäller från 1.1.2020)

(28) Europeiska bankmyndigheten har med stöd av artikel 16 i Europaparlamentets och rådets förordning (EU) Nr 1093/2010 utfärdat ”Riktlinjer för villkoren för att utnyttja undantaget från beredskapsmekanismen enligt artikel 33.6 i förordning EU 2018/389 (tekniska tillsynsstandarder för sträng kundautentisering och gemensamma och säkra öppna kommunikationsstandarder)” (EBA/GL/2018/07).

Föreskrift (stycke 29)

(29) Finansinspektionen rekommenderar att de institut som omfattas av dessa anvisningars tillämpningsområde följer Europeiska bankmyndighetens riktlinjer som avses i stycke 26 och som finns tillgängliga på finanssivalvonta.fi. (Utfärdats 23.9.2019, gäller från 1.1.2020).

10 Upphävda föreskrifter och anvisningar

När dessa föreskrifter och anvisningar träder i kraft upphävs följande standarder utgivna av Finansinspektionen:

- Finansinspektionens standard 4.4b Hantering av operativa risker
- Finansinspektionens standard RA4.2 Rapportering av händelser relaterade till operativa risker
- Finansinspektionens standard 6.1 Verksamhet som bedrivs av betalningsinstitut och personer som utan auktorisation tillhandahåller betaltjänster, avsnitt 9.7 Hantering av operativa risker
- Finansinspektionens standard RA6.1 Verksamhet som bedrivs av betalningsinstitut och personer som utan auktorisation tillhandahåller betaltjänster, avsnitt 4.3.4 Rapportering av händelser som gäller operativa risker.

11 Ändringshistorik

Föreskrifterna och anvisningarna har ändrats på följande sätt efter ikraftträdandet:

Utfärdade 21.4.2015, gäller från 1.7.2015.

- Hänvisningen till Europeiska centralbankens rekommendationer för säkerhet för internetbetalningar i avsnitt 2.5 och 7 har ersatts med en hänvisning till Europeiska bankmyndighetens riktlinjer av den 19 december 2014 om säkerheten vid internetbetalningar.

Utfärdats 6.11.2017, gäller från 1.3.2018

- till avsnitt 6.1 har det lagts till en hänvisning till Europeiska bankmyndighetens riktlinjer om IKT-riskbedömning av den 11 maj 2017, och som en följd av det har numreringen i kap. 6 ändrats.

Utfärdats 29.1.2018, gäller från 1.3.2018

- siffrorna i avsnitten 1.1 och 8.1 har ändrats att motsvara bestämmelserna i den nya lagen om värdeandelssystemet och om clearingverksamhet.
- siffrorna i avsnitten 2.1, 2.3, 2.4 och 8.1 har ändrats att motsvara bestämmelserna i den nya lagen om handel med finansiella instrument.
- avsnitt 8.1 har ändrats att motsvara bestämmelserna i lagen om investeringstjänster.
- i avsnitt 2.4 har hänvisningen till 7 kap. 23 § 1 mom. 3 punkten i lagen om investeringstjänster strukits, eftersom Finansinspektionens rätt att meddela föreskrifter enligt 7 kap. 23 § 1 mom. 3 punkten i lagen om investeringstjänster har upphävts i samband med att direktivet om marknader för finansiella instrument ((EU) 65/2014, MiFID II) nationellt sattes i kraft.
- kapitel 7 och avsnitt 9.1 har ändrats att motsvara bestämmelserna i den nya lagen om betalningsinstitut, och som en följd av det har kapitlets och avsnittets numrering ändrats.
- till kapitel 7 och avsnitt 9.1 har hänvisningar till Europeiska bankmyndighetens (EBA) riktlinjer om rapporteringen av allvarliga betaltjänstincidenter samt om hanteringen av operativa risker och säkerhetsrisker lagts till, och som en följd av det har kapitlets och avsnittets numrering ändrats
- ett nytt avsnitt 9.3 har lagts till

Utfärdats 23.9.2019, gäller från 1.1.2020

- avsnitt 1.1 har ändrats
- avsnitten 2.1, 2.3, 2.4 och 9.1 har ändrats så att de motsvarar direktivet om säkerhet i nätverks- och informationssystem (EU) 2016/1148) och de nationella lagarna för verkställandet av det
- avsnitt 2.2 har ändrats så att det motsvarar Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av

personuppgifter och om det fria flödet av sådana uppgifter

- avsnitt 2.5 har ändrats så att det lagts till en hänvisning till Europeiska bankmyndighetens riktlinjer ((EBA/GL/2018/05) om krav för rapportering av statistiska uppgifter om svikliga förfaranden enligt artikel 96.6 i det andra betaltjänstdirektivet)
- avsnitt 4.3 har ändrats genom att lägga till en hänvisning till kraven på processerna för produktgodkännande enligt 7 kap. 7 § i lagen om investeringstjänster
- avsnitt 6.2 har ändrats genom att lägga till en anvisning om certifiering av nättjänsternas dataskydd i stycke 35
- i avsnitt 8.3 och 8.4 har numrering korrigerats
- avsnitt 9.1 har ändrats vad gäller rapporteringen till Finansinspektionen i anslutning till rapporteringsskyldigheterna i dataskyddsförordningen och anvisningarna har specificerats vad gäller anmälningar om störningar
- avsnitt 9.2 har preciserats vad gäller anvisningarna om rapporteringen av förluster som orsakas av operativa risker
- till avsnitt 9.4 har anvisningar som gäller uppgifter om svikliga förfaranden i anslutning till betalningsinstrument lagts till
    - föreskrifter om insamling av statistik om bedrägeriuppgifter samt tidsfrister har lagts till
    - en hänvisning till Europeiska bankmyndighetens riktlinjer av den 18 juli 2018 om rapporteringen av statistiska uppgifter om svikliga förfaranden har lagts till
- avsnitt 9.5 har lagts till om ansökan om undantag från kravet på beredskapsmekanism för PSD2-specialgränssnittet
    - en hänvisning till Europeiska bankmyndighetens riktlinjer av den 4 december för villkoren för att utnyttja undantaget från beredskapsmekanismen

Utfärdats 16.2.2022, gäller från 1.3.2022

- Avsnitt 2.5 har ändrats med en hänvisning till Baselkommitténs uppdaterade riktlinjer Revisions to the Principles for the Sound Management of Operational Risk
- En hänvisning till Europeiska bankmyndighetens avförde riktlinjer om säkerheten vid internetbetalningar har avförts
- Avsnitt 2.5 har ändrats vad gäller Europeiska bankmyndighetens uppdaterade riktlinjer om rapportering av allvarliga incidenter
- En hänvisning till Europeiska bankmyndighetens avförde riktlinjer för säkerhetsåtgärder för operativa risker och säkerhetsrisker för betaltjänster enligt direktiv (EU) nr 2015/2366 (PSD2) har avförts
- En hänvisning till Europeiska bankmyndighetens riktlinjer för hantering av IKT- och säkerhetsrisker Guidelines on ICT and security risk management (EBA/GL/2019/04) har lagts till
- Avsnitt 7, anvisning (14) har uppdaterats med en hänvisning till Europeiska bankmyndighetens riktlinjer för hantering av IKT- och säkerhetsrisker

- Avsnitt 7, anvisning (15) har uppdaterats med en hänvisning till Europeiska bankmyndighetens riktlinjer för hantering av IKT- och säkerhetsrisker
- Avsnitt 9, föreskrift (7) har uppdaterats med en hänvisning till Europeiska bankmyndighetens uppdaterade riktlinjer om rapportering av allvarliga incidenter
- Avsnitt 9 har uppdaterats med en hänvisning till nya riktlinjer för rapportering om svikliga förfaranden

Utfärdats 1.12.2022, gäller från 1.1.2023

- I avsnitt 9.1 har anvisning (8) om anmälan om störningar och fel i verksamheten uppdaterats
- I avsnitt 9.1 har föreskrift (9) om inlämnandet av en anmälan om störningar i betaltjänsterna till Finansinspektionen uppdaterats
- I avsnitt 9.2 har anvisning (16) om inlämnandet av en årsanmälan till Finansinspektionen uppdaterats
- I avsnitt 9.3 har föreskrift (20) om inlämnandet av en årlig bedömning till Finansinspektionen uppdaterat