DANMARKS
NATIONALBANK

OVERVÅGNINGSPOLITIK

2019

DANMARKS
NATIONALBANK

OVERVÅGNINGSPOLITIK

Publikationen er tilgængelig på Nationalbankens websted: www.nationalbanken.dk under publikationer. Publikationen oversættes til engelsk.

Rapporten består af en dansk og engelsk version. I tilfælde af tvivl om oversættelsens korrekthed gælder den danske version.

Redaktionen er afsluttet 4. marts 2019.

Information om publikationen kan fås ved henvendelse til:

Danmarks Nationalbank
Kommunikation
Havnegade 5
1093 København K

Telefon 33 63 70 00 (direkte) eller 33 63 63 63
Ekspeditionstider, mandag-fredag kl. 9.00-16.00
E-mail: kommunikation@nationalbanken.dk
www.nationalbanken.dk

ISBN: 978-87-92933-00-3

DANMARKS
NATIONALBANK

OVERVÅGNINGPOLITIK 2019

Nationalbankens politik for overvågning af den finansielle infrastruktur i Danmark

Det er vigtigt for samfundet, at betalinger og værdipapirhandler kan gennemføres sikkert og effektivt. Nationalbanken bidrager som andre centralbanker til dette ved at overvåge vigtige dele af den finansielle infrastruktur[1]. Nationalbanken overvåger de centrale danske betalings- og afviklingssystemer samt de vigtigste betalingsløsninger. Nationalbanken bidrager desuden til andre centralbankers overvågning af internationale systemer, der har relevans i Danmark. Nationalbankens politik for overvågningen fremgår af dette dokument.

Overvågningens formål og lovgrundlag

Ifølge nationalbanklovens § 1 har banken som opgave at "opretholde et sikkert pengevæsen her i landet samt at lette og regulere pengeomsætning og kreditgivning".[2] På den baggrund overvåger Nationalbanken, at de centrale danske betalings- og afviklingssystemer samt de vigtigste betalingsløsninger er sikre og effektive. Nationalbankens overvågningsbeføjelser er endvidere fastlagt i kapitalmarkedsloven, jf. boks 1.

Overvågningen sker med udgangspunkt i internationale standarder, som stiller krav til sikkerhed og effektivitet, herunder at driftsstabiliteten skal være høj, risici begrænsede, og at systemerne og løsningerne skal være tidssvarende og omkostningseffektive. Nationalbanken vurderer, om de overvågede systemers og løsningers indretning og funktion lever op til de internationale standarder. Nationalbanken foranlediger ændringer til systemerne og løsningerne, hvis dette ikke er tilfældet. Nationalbanken fører ikke tilsyn med de enkelte virksomheder i infrastrukturen.

Der kan være situationer, hvor Nationalbanken ud fra en samfundsmæssig betragtning stiller højere krav til sikkerhed og effektivitet, end de ansvarlige for et system eller en løsning finder det forretningsmæssigt optimalt. Nationalbankens opgave er at stille krav, så samfundsmæssige hensyn tilgodeses. Kravene kan ændre sig med tiden, fx på grund af den teknologiske udvikling, nye behov eller et ændret trusselsbillede. Især truslen om cyberangreb har en dynamisk karakter.

1 Den danske finansielle infrastruktur er det netværk af systemer, der muliggør, at forbrugere og virksomheder, herunder pengeinstitutter og andre finansielle aktører, kan udveksle betalinger og værdipapirer mellem hinanden. Nationalbankens system Kronos2 har en central rolle i den finansielle infrastruktur.

2 Lov om Danmarks Nationalbank (*link*).

Overvågningens udstrækning

Nationalbanken overvåger de systemisk vigtige dele af den finansielle infrastruktur, dvs. de dele, hvor fejl og nedbrud vurderes i værste fald at kunne true den finansielle stabilitet eller svække tilliden til det finansielle system i Danmark. Et betalings- og afviklingssystem kan eksempelvis true den finansielle stabilitet, hvis problemer i ét finansielt institut via systemet spreder sig til andre institutter eller til det finansielle system generelt. Der er meget lille sandsynlighed for, at det sker, men konsekvenserne for samfundet kan være store. Tilliden til det finansielle system kan trues, hvis fx en vigtig betalingsløsning ikke kan benyttes i længere tid på grund af driftsforstyrrelser, eller hvis der er et stort misbrug med en betalingsløsning.

Nationalbanken har opstillet kriterier, som benyttes til at vurdere betalings- og afviklingssystemers og betalingsløsningers systemiske vigtighed. Kriterierne bruges til at udvælge de systemer/løsninger, der overvåges, og til at prioritere overvågningsindsatsen. Kriterierne er:

- Hvor stort transaktionsomfanget er målt på antal og værdi
- Hvorvidt der er få eller ingen substitutionsmuligheder
- Hvad systemets/løsningens anvendelsesområde er
- Om fejl og nedbrud påvirker offentligheden

Lovgrundlaget for Nationalbankens overvågning

Boks 1

Overvågningen af den finansielle infrastruktur er traditionelt en centralbankopgave. Det primære formål er at bidrage til, at den finansielle infrastruktur er sikker og effektiv. Nationalbankens hjemmel til overvågning findes i nationalbankloven § 1, der fastslår, at banken har til opgave at "opretholde et sikkert pengevæsen her i landet samt at lette og regulere pengeomsætning og kreditgivning".[1] Ordet overvågning er ikke nævnt i loven, men overvågning betragtes som en naturlig opgave, hvis Nationalbanken skal opfylde sit lovfæstede formål om sikre og effektive betalinger.

Ved nationalbanklovens fremsættelse i 1936 udtalte handels-, industri- og søfartsministeren, at der med formålsangivelsen i § 1 tilsigtes at give "en principiel rettesnor for bankens ansvarlige ledelse (…) På hvilken måde og ved hvilke midler banken bedst kan sikre pengevæsenet og lette pengeomsætning og kreditgivning, vil afhænge af forholdene til de forskellige tider. At søge at fastslå og binde dette i selve loven ville på dette tidspunkt næppe være muligt eller heldigt."

Nationalbankens overvågningsbeføjelser er også fastlagt i kapitalmarkedsloven, KML[2]. Det fremgår af § 212, stk. 3, at Nationalbanken overvåger registrerede betalingssystemer, som banken finder har væsentlig betydning for betalingsafviklingen med det formål at fremme systemernes smidige funktion ved at bidrage til deres effektivitet og stabilitet. Nationalbanken meddeler Finanstilsynet, hvilke systemer det drejer sig om, og Finanstilsynet offentliggør i henhold til bemærkningerne til forslaget til KML en liste over de registrerede betalingssystemer, der er omfattet af overvågningen. Nationalbanken har en række myndighedsopgaver i relation til de betalingssystemer, der overvåges (§ 180), og Nationalbanken har beføjelser til at indsamle oplysninger om betalingssystemerne (§ 217, jf. § 216). Endvidere har Nationalbanken beføjelse til at pålægge de ansvarlige tvangsbøder, såfremt et påbud udstedt i forbindelse med overvågning ikke bliver efterkommet (§ 256).

Beføjelserne i KML vedrører alene betalingssystemer. Nationalbankens overvågning af VP-afviklingen er ikke reguleret i KML. Nationalbankens opgave med at overvåge andre systemer end betalingssystemer, heriblandt værdipapirafviklingssystemer som VP-afviklingen, sker med udgangspunkt i nationalbankloven og internationale standarder. I henhold til forordningen om forbedring af værdipapirafviklingen i Den Europæiske Union og om værdipapircentraler, CSDR[3], inddrages Nationalbanken, jf. artikel 12 om relevante myndigheder, i tilladelsen til og tilsynet med værdipapircentraler, når deres afvikling i danske kroner berettiger hertil. Det er tilfældet vedrørende Finanstilsynets tilladelse til og løbende tilsyn med VP.

1. Lov om Danmarks Nationalbank (*link*).
2. LBK nr. 12 af 08/01/2018 (*link*).
3. Europa-Parlamentets og Rådets forordning (EU) nr. 909/2014 af 23. juli 2014 (*link*).

- Om fejl og nedbrud kan påvirke andre systemer eller løsninger.

På nuværende tidspunkt omfatter Nationalbankens overvågning:

- Interbankbetalingssystemet Kronos2
- Detailbetalingssystemerne Sum-, Intradag- og Straksclearingen
- Værdipapirafviklingssystemet VP-afviklingen
- Betalingsløsningerne Dankort, konto til konto-overførsler og Betalingsservice.

Et system eller en løsning består af en teknisk infrastruktur, organisationen omkring denne og et sæt fælles regler og procedurer, herunder de involverede parters juridiske forpligtelser. Nationalbankens overvågning fokuserer på de elementer, hvor fejl, nedbrud og uhensigtsmæssigheder kan få en betydning for den generelle drift og brug af systemet/løsningen, dvs. centrale funktioner, sikkerhedselementer og it-systemer samt overordnede regler og vilkår.

Nationalbankens overvågning er rettet mod de ansvarlige for systemerne og løsningerne, der har det endelige ansvar for, at systemerne og løsningerne er sikre og effektive. Dette gælder også i tilfælde, hvor driften eller dele af driften er outsourcet til tredjepart.

Overvågningsmyndigheders ansvar Boks 2

CPMI-IOSCO har formuleret fem ansvarsområder for myndigheder med ansvar for regulering, tilsyn og overvågning af de systemisk vigtige dele af den finansielle infrastruktur. For overvågningsmyndigheder indebærer de fem ansvarsområder:

- Overvågningen skal definere og offentliggøre de kriterier, der benyttes til at udvælge de dele af den finansielle infrastruktur, der overvåges.
- Overvågningen skal have de fornødne beføjelser og ressourcer, således at overvågningsansvaret kan varetages effektivt.
- Der skal være gennemsigtighed omkring udøvelsen af myndighedsrollen, og overvågningspolitikken skal offentliggøres.
- Der skal overvåges efter internationalt anerkendte standarder, og der skal være konsistens i overvågningen, herunder skal systemer drevet af centralbanker og andre systemer behandles ens.
- Relevante myndigheder skal samarbejde om overvågning, tilsyn mv. Det gælder nationalt og internationalt.

Nationalbankens overvågning er tilrettelagt med udgangspunkt i disse fem ansvarsområder for overvågningsmyndigheder.

Kilde: CPMI-IOSCO, Principles for financial market infrastructures, 2012 (*link*).

Overvågningens tilrettelæggelse

Nationalbankens overvågning er tilrettelagt ud fra internationale retningslinjer for overvågningsmyndigheders ansvar, jf. boks 2.

Som led i overvågningen vurderer Nationalbanken, om systemer og løsninger lever op til relevante internationale standarder, og udviklingen i systemerne/løsningerne følges løbende gennem indsamling af information og dialog med de ansvarlige. Nationalbanken foranlediger ændringer til systemerne/løsningerne, når det er nødvendigt.

Nationalbankens overvågning af betalings- og afviklingssystemer sker med udgangspunkt i CPMI-IOSCO-principperne[3] for systemer, og overvågningen af betalingsløsninger sker med udgangspunkt i Den Europæiske Centralbanks, ECB's, standarder for betalingsløsninger, jf. boks 3.

Nationalbanken ejer interbankbetalingssystemet Kronos2. For at sikre konsistens og ligebehandling i

3 Committee on Payment and Market Infrastructures, CPMI, er en komité, som er knyttet til Bank for International Settlements, BIS. International Organization of Securities Commissions, IOSCO, er et internationalt samarbejde mellem myndigheder, der fører tilsyn med værdipapirmarkeder.

overvågningen af Kronos2 og de øvrige systemer er Nationalbankens overvågningsfunktion organisatorisk adskilt fra udviklingen og driften af Kronos2.

Vurderinger efter internationale standarder
Nationalbanken vurderer med jævne mellemrum, hvorvidt et system eller en løsning lever op til de internationale standarder. Vurderinger udarbejdes, når et system eller en løsning omfattes af overvågningen, eller hvis en tidligere vurdering ikke længere er dækkende. Der kan også være behov for en ny vurdering, hvis der har været en væsentlig udvikling i it, teknologi, sikkerhedsstandarder eller i trusselsbilledet, fx med nye typer af cyberangreb.

Nationalbanken initierer en vurdering ved at bede de ansvarlige for systemet/løsningen om at besvare en række spørgsmål i relation til standarderne. Nationalbanken vurderer på baggrund af besvarelserne og tilhørende dokumentation, om standarderne efterleves. Det kan resultere i anbefalinger om, at der skal rettes op på mangler og uhensigtsmæssigheder. Nationalbanken offentliggør en rapport med konklusioner og anbefalinger. Der følges op

Internationale standarder, der anvendes i Nationalbankens overvågning

Boks 3

Nationalbankens overvågning sker med udgangspunkt i internationale standarder. Nationalbanken overvåger de centrale danske betalings- og afviklingssystemer med udgangspunkt i CPMI-IOSCO's principper for systemer. Overvågningen af de vigtigste danske betalingsløsninger sker med udgangspunkt i ECB's standarder for betalingsløsninger. De internationale standarder stiller krav til sikkerhed og effektivitet.

CPMI-IOSCO-principperne
Overvågningen af de danske betalings- og afviklingssystemer sker med udgangspunkt i CPMI-IOSCO's principper for finansielle markedsinfrastrukturer, dvs. principper for betalingssystemer, værdipapirafviklingssystemer, værdipapircentraler, centrale modparter, CCP'er, og handelsregistre.[1] Der er 24 principper, hvoraf visse principper kun er relevante for nogle typer systemer. I principperne stilles krav til systemernes overordnede organisering, herunder om et velfunderet juridisk grundlag, en klar og transparent organisations- og ledelsesstruktur og robuste rammer for risikostyring. Endvidere stiller principperne nærmere krav til styringen af alle former for risici, som kan opstå i forbindelse med clearing og afvikling af finansielle transaktioner. Endelig stilles en række krav, der adresserer effektivitetsmæssige aspekter, herunder krav om fair og åben adgang, praktisk anvendelighed og omkostningseffektivitet for alle relevante parter samt krav vedrørende gennemsigtighed. Der stilles bl.a. krav om offentliggørelse af regler, procedurer og kvantitative data om anvendelse og drift.

CPMI-IOSCO har offentliggjort en vurderingsvejledning og nærmere krav vedrørende de overvågede systemers videregivelse af information til deltagere, myndigheder og den bredere offentlighed. De ansvarlige for betalings- og afviklingssystemer er ifølge principperne forpligtede til at offentliggøre en detaljeret beskrivelse af, hvordan systemet efterlever principperne, den såkaldte disclosure. Beskrivelsen skal opdateres mindst hvert andet år samt efter væsentlige systemændringer eller andre væsentlige ændringer.

Nationalbanken har i april 2013 offentliggjort en beskrivelse af principperne og baggrunden for deres tilblivelse.[2]

CPMI-IOSCO's principper for finansielle markedsinfrastrukturer suppleres af forskellige uddybende retningslinjer for specifikke emner, som der også tages højde for i Nationalbankens overvågning. Blandt andet indgår CPMI-IOSCO's cyber guidelines[3] og CPMI's strategi for endpoint-sikkerhed[4] i overvågningen af operationel risiko.

ECB's standarder for betalingsløsninger
Nationalbankens overvågning af de vigtigste danske betalingsløsninger sker med udgangspunkt i ECB's harmoniserede overvågningsstandarder for betalingsløsninger.[5] Standarderne er udmøntet i specifikke rammer for overvågning af henholdsvis konto til konto-overførsler, direkte debiteringer og betalingskort. Der er fem overordnede standarder, som indeholder krav til: 1) et velfunderet juridisk grundlag i alle relevante jurisdiktioner, 2) adgang til komplet information for alle aktører, inkl. om finansielle risici, 3) tilstrækkelig sikkerhed, operationel stabilitet og forretningsvidereførelse, 4) en effektiv og pålidelig ledelse og styring med klar rolle- og ansvarsfordeling, samt 5) at risici i relation til clearing- og afviklingsprocessen skal være styrede og begrænsede.

1. CPMI-IOSCO, *Principles for financial market infrastructures*, 2012 (*link*).
2. Katrine Skjærbæk Rasmussen og Tina Skotte Sørensen, Nye principper for finansielle markedsinfrastrukturer, *Danmarks Nationalbank Kvartalsoversigt*, 1. kvartal 2013, del 1 (*link*).
3. CPMI-IOSCO, *Guidance on cyber resilience for financial market infrastructures*, 2016 (*link*).
4. CPMI, *Reducing the risk of wholesale payments fraud related to endpoint security*, 2018 (*link*).
5. ECB, *Harmonised oversight approach and oversight standards for payment instruments*, 2009 (*link*).

på anbefalingerne i den løbende overvågning, jf. nedenfor.

Løbende overvågning
Den løbende overvågning af systemerne/løsningerne er bygget op omkring en formaliseret indhentning af information og jævnlige møder med de ansvarlige. Målet med den løbende overvågning er at vurdere den fortsatte efterlevelse af de internationale standarder.

Nationalbanken modtager en fast, kvartalsvis rapportering fra systemerne/løsningerne om det juridiske grundlag, organisation og strategi, risikostyring og beredskab, brug og drift samt om resultater af intern og ekstern revision. Nationalbanken modtager årligt systemernes/løsningernes opdaterede rammer for risikostyring, risikovurderinger, beredskabsplaner og for systemerne også stresstestplaner. I tilfælde af fejl og nedbrud orienteres Nationalbanken hurtigst muligt og senest ved dagens slutning. Efterfølgende modtager Nationalbanken en nærmere redegørelse for hændelsen. Redegørelsen skal omfatte årsager, konsekvenser og eventuelle tiltag, der skal forhindre gentagelse af hændelsen.

Der afholdes som hovedregel kvartalsvise møder mellem Nationalbanken og de ansvarlige for et system/en løsning. På møderne gennemgås den kvartalsvise rapportering, og opfølgningen på større fejl og nedbrud drøftes. Endvidere drøftes resultaterne af Nationalbankens årlige gennemgang af risikovurderinger, beredskabsplaner mv., og der følges op på eventuelle åbne anbefalinger.

Nationalbanken afrapporterer årligt fra overvågningsarbejdet i publikationen *Overvågning af den finansielle infrastruktur*.

Overvågningens virkemidler
Nationalbanken foranlediger ændringer i de overvågede systemer/løsninger, såfremt det findes nødvendigt. Ønskede tilpasninger fremmes via den løbende dialog med de ansvarlige for de overvågede systemer og løsninger. Nationalbankens vurderinger og anbefalinger offentliggøres, og bankens holdninger tilkendegives i artikler og publikationer, herunder i den årlige overvågningspublikation. Nationalbanken kan endvidere orientere Betalingsrådet[4] om identificerede svagheder i detailbetalingsinfrastrukturen og lade Betalingsrådet drøfte og eventuelt beslutte tiltag, der kan fremme effektiviteten og sikkerheden i detailbetalinger i Danmark. Problemstillinger vedrørende operationel risiko og cybersikkerhed kan tages op i Finansielt Sektorforum for Operationel Robusthed, FSOR[5], der kan beslutte at arbejde videre med tiltag til at reducere relevante risici.

Samarbejde med andre myndigheder

Nationalbankens overvågning sker i samarbejde med andre inden- og udenlandske myndigheder. Hensynet er at undgå dobbelt myndighedskontrol, at udnytte kompetencer hos de respektive myndigheder samt at sikre deling af relevant information. Der er etableret et formaliseret samarbejde med Finanstilsynet, der fører tilsyn med centrale aktører i den finansielle infrastruktur. Nationalbanken bidrager desuden til andre centralbankers overvågning af internationale systemer, der har relevans i Danmark.

Samarbejde med Finanstilsynet
Nationalbanken samarbejder med Finanstilsynet, når overvågningen berører forhold, hvor både Nationalbanken og Finanstilsynet har beføjelser. De overordnede rammer for samarbejdet er fastlagt i en samarbejdsaftale.[6] Aftalen angiver lovgrundlaget for Nationalbankens overvågning og Finanstilsynets

4 Betalingsrådets kommissorium, sammensætning og publikationer er beskrevet på Nationalbankens hjemmeside (*link*).

5 FSOR's kommissorium, sammensætning og publikationer er beskrevet på Nationalbankens hjemmeside (*link*).

6 Aftalen indgår som bilag 3 til den generelle samarbejdsaftale indgået mellem Danmarks Nationalbank og Finanstilsynet. Den er offentlig tilgængelig på Nationalbankens hjemmeside (*link*).

tilsyn, organiseringen af samarbejdet, samt hvilke dele af den finansielle infrastruktur der er omfattet af aftalen.

Overvågning af operationel risiko, herunder cyberrisiko
Nationalbankens samarbejde med Finanstilsynet vedrører især overvågning af operationel risiko i den finansielle infrastruktur, herunder cyberrisiko. Finanstilsynet fører bl.a. it-tilsyn med de datacentraler, der drifter systemer og løsninger, som Nationalbanken overvåger. Finanstilsynet fører tilsyn med, at relevante lovkrav er overholdt, bl.a. vedrørende it-sikkerhedsstyring, outsourcing og revision.[7]

Nationalbankens vurdering af, om et system eller en betalingsløsning lever op til internationale standarders krav vedrørende it-sikkerhed og håndtering af operationel risiko, bygger så vidt muligt på Finanstilsynets observationer og konklusioner. Nationalbanken deltager som observatør på Tilsynets it-inspektioner hos relevante datacentraler. Derved indhentes information om efterlevelsen af de dele af standarderne, der er dækket af Finanstilsynets arbejde. Derudover udveksles løbende information mellem Nationalbanken og Finanstilsynet, og eventuel opfølgning på fejl og nedbrud i den finansielle infrastruktur koordineres efter behov.

Samarbejdet om overvågning af/tilsyn med VP
Overvågningen af VP sker i samarbejde med Finanstilsynet. Finanstilsynet fører tilsyn med VP, herunder med, at VP's regler, organisationsplaner, forretningsgange og kontrol- og sikkerhedsforanstaltninger er betryggende og i overensstemmelse med lov om kapitalmarkeder. Nationalbanken deltager i Tilsynets it-inspektioner hos VP, der udveksles løbende information, og eventuel opfølgning over for VP koordineres efter behov. Nationalbanken og Finanstilsynet samarbejder desuden om udarbejdelsen af vurderinger af VP's efterlevelse af CPMI-IOSCO-principperne, og der offentliggøres en fælles rapport med konklusioner og anbefalinger.

VP skal have en licens udstedt under den fælleseuropæiske regulering af værdipapircentraler, CSDR, for at kunne fungere som værdipapircentral i EU. Finanstilsynet er kompetent myndighed for VP i forhold til at tildele licens og føre tilsyn med, at VP efterlever CSDR. Nationalbanken og ECB er relevante myndigheder, dvs. myndigheder med høringsret. Reglerne i CSDR er afstemt med CPMI-IOSCO-principperne.

Internationalt overvågningssamarbejde
Nationalbanken deltager i overvågningen af Target2 og T2S, som er ECB's systemer til henholdsvis interbankbetalinger i euro og afvikling af værdipapirhandler. Overvågningen af disse systemer varetages af de centralbanker, der er tilsluttet systemerne, under ledelse af ECB. Nationalbanken er i øvrigt ansvarlig for overvågningen af de danske komponenter af Target2.

Nationalbanken medvirker endvidere i overvågningen af CLS, som er et internationalt system til afvikling af valutahandler. Den amerikanske centralbank, Federal Reserve System, er hovedovervåger af CLS, og centralbankerne for de tilsluttede valutaer, herunder Nationalbanken, er medovervågere.

EuroCCP[8] er central modpart for aktiehandler indgået på Nasdaq OMX i København. Den hollandske centralbank og det hollandske finanstilsyn leder samarbejdet om overvågningen af EuroCCP. Nationalbanken deltager som observatør i arbejdet.

Endvidere er Nationalbanken relevant myndighed for Euroclear Bank i Bruxelles i forhold til CSDR på baggrund af omfanget af afviklingen af danske obligationer gennem Euroclear Bank. National Bank of Belgium er kompetent myndighed.

7 Datacentralerne skal bl.a. efterleve krav i ledelsesbekendtgørelsen (*link*), outsourcingbekendtgørelsen (*link*) og systemrevisionsbekendtgørelsen (*link*).

8 En central modpart, CCP, er kendetegnet ved, at den indtræder i en handel mellem køber og sælger og derved selv bliver modpart i handlerne. CCP'en sikrer, at handlerne gennemføres, så længe CCP'en er i stand til at overholde sine forpligtelser.