FSOR

FINANSIELT SEKTORFORUM
FOR OPERATIONEL ROBUSTHED

28. august 2020

Metodehåndbog for FSOR's risikoanalyse

1 Indledning

En af FSOR's opgaver er at sikre et fælles overblik over operationelle risici, der kan ramme på tværs af sektoren og potentielt true den finansielle stabilitet. FSOR udarbejder derfor en risikoanalyse for at identificere relevante risici og sikre et fælles overblik. Risikoanalysen danner grundlag for at beslutte og gennemføre fælles tiltag til at styrke den finansielle sektors robusthed over for store operationelle hændelser, herunder cyberangreb.

I det følgende beskrives den metode, som benyttes til at udarbejde og vedligeholde FSOR's risikoanalyse. Arbejdet udføres af arbejdsgruppen FSOR-RISK. Gruppens nuværende medlemmer og kontaktoplysninger fremgår af bilag 3.

2 Risikoanalysens formål og afgrænsning

FSOR's risikoanalyse har til formål at identificere og behandle operationelle risici, herunder cyberrisici, som potentielt kan true den finansielle stabilitet. Som en del af risikoanalysen kortlægges kritisk infrastruktur i den finansielle sektor. Denne kortlægning skal give FSOR et fælles overblik over kritiske forretningsaktiviteter, systemer, leverandører, sammenhænge og afhængigheder i den finansielle sektor.

Ved finansiel stabilitet forstås en tilstand, hvor det finansielle system som helhed er så robust, at eventuelle problemer i sektoren ikke spreder sig og hindrer det finansielle system i at fungere som effektiv formidler af kapital og finansielle tjenesteydelser. I relation til operationel robusthed kan finansiel stabilitet potentielt trues af alvorlige hændelser, der forårsager længerevarende nedbrud eller kompromittering af kritiske forretningsaktiviteter og/eller påvirker tilliden til det finansielle system. Risikoanalysens kriterier for at bedømme, om en risiko kan true den finansielle stabilitet, fremgår af boks 1.

Ved udvælgelse af mitigerende tiltag, der skal imødegå de identificerede risici, fokuserer FSOR på tiltag, hvor den finansielle sektor med fordel kan koordinere og samarbejde for at øge den operationelle robusthed for hele sektoren.

Enhver finansiel institution er ansvarlig for risikostyring i forhold til sin egen operationelle robusthed og it-sikkerhed. FSOR's risi-

koanalyse erstatter ikke de enkelte aktørers egen risikostyring og mitigerende handlinger, men skal ses som et supplement til aktørernes egen risikostyring og kan give input hertil. Ligeledes er FSOR's risikoanalyse et supplement til Risikoforum for Gensidige Afhængigheder, RGA's, risikoanalyse, der fokuserer på risici forbundet med afhængigheder mellem Kronos2, VP og detailbetalingssystemerne.

2.1 Kriterier for finansiel stabilitet

Nedenstående kriterier benyttes til at vurdere, om den finansielle stabilitet kan være truet af en operationel hændelse, herunder et cyberangreb.

Kriterier for at vurdere, om den finansielle stabilitet potentielt er truet — Boks 1

Den finansielle stabilitet kan potentielt være truet, når et eller flere af nedenstående kriterier er opfyldt:

Kritisk forretningsaktivitet er utilgængelig eller kompromitteret.

- Et nedbrud rammer flere kritiske aktører i et kritisk tidsrum eller på et kritisk tidspunkt
- Fortroligheden af kritiske aktiver brydes, fx som følge af et cyberangreb
- Der opstår tvivl om kritiske datas integritet, fx som følge af et cyberangreb.

Borgeres/virksomheders tillid til det finansielle system er truet.

- En kritisk stor andel er direkte berørt eller indirekte via medier.

Investorers tillid til danske aktiver/markeder er truet.

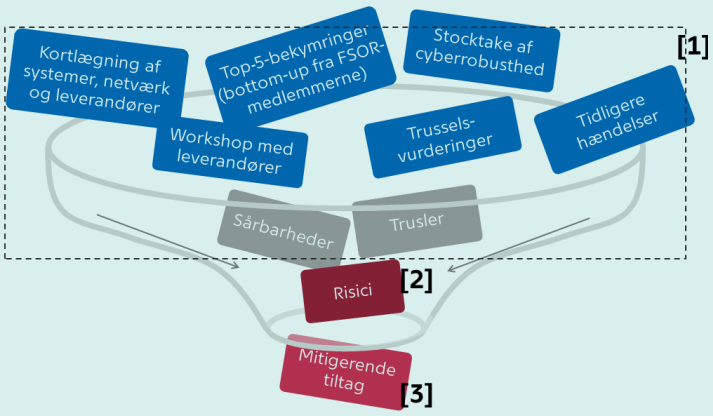
- Mange investorer berøres direkte eller indirekte via medier eller ratingbureauer.

3 Risikostyringsproces

FSOR's risikovurdering udarbejdes som illustreret i "tragten" i figur 1.

1. Først gennemføres en bred afdækning af de risici, som potentielt kan true den finansielle stabilitet, jf. [1] i figur 1. Dette sker for det første ved at vedligeholde et fundament for risikoanalysen, som består af en kortlægning af kritiske forretningsaktiviteter og kritisk infrastruktur, jf. afsnit 4.1, og for det andet ved løbende at indhente information om trusler og sårbarheder fra diverse kilder, jf. afsnit 4.2.
2. På baggrund af afdækningen af trusler og sårbarheder identificeres risici, jf. [2]. Risici vurderes ud fra sandsynlighed og konsekvens på en skala fra 1 til 5, jf. afsnit 5. Den indledende vurdering foretages af arbejdsgruppen FSOR-RISK.
3. Resultaterne rapporteres derefter til FSOR på de halvårlige FSOR-møder. På baggrund af input fra FSOR opstiller FSOR-RISK ligeledes forslag til mitigerende tiltag, jf. [3]. Implementering af mitigerende tiltag igangsættes af FSOR, og status på implementeringen drøftes på FSOR-møderne, jf. afsnit 6 og 7.

Arbejdsgang for FSOR's risikoanalyse **Figur 1**



Anm.: Risikoanalysen udarbejdes ved at indsamle input, der lægges i tragten øverst, hvorefter risici identificeres og behandles, så der ud af tragten kommer en række anbefalinger til FSOR om det videre arbejde med mitigerende tiltag.
Kilde: FSOR.

4 Identificering af risici

Risici identificeres på baggrund af en række kilder, som belyser sårbarheder og trusler mod finansiel stabilitet. Kilderne beskrives i det følgende.

4.1 Fundament og afgrænsning – ad [1]

Fundamentet for FSOR's risikoanalyse er en kortlægning af de kritiske forretningsaktiviteter i den finansielle sektor samt en kortlægning af kritisk infrastruktur, som giver et fælles overblik over kritiske forretningsaktiviteter, systemer, leverandører og sammenhænge i den finansielle sektor. Risikoanalysen afgrænses til at omhandle de risici, som potentielt kan ramme de kritiske forretningsaktiviteter og dermed kan true finansiel stabilitet.

Fundamentet for risikoanalysen består af:

- Bruttoliste over forretningsaktiviteter i den finansielle sektor.
- Udvælgelse af de mest kritiske forretningsaktiviteter, dvs. de aktiviteter, hvor nedbrud hurtigst kan få konsekvenser, der potentielt kan true den finansielle stabilitet. P.t. er der identificeret fem kritiske forretningsaktiviteter.
- Business Impact Analysis, BIA, for hver af de kritiske forretningsaktiviteter. I BIA'erne afdækkes konsekvenser af nedbrud, og de processer, systemer og leverandører, der understøtter forretningsaktiviteten, identificeres. BIA-formatet kan ses i bilag 1.
- Kortlægning af kritisk infrastruktur, der understøtter de kritiske forretningsaktiviteter og viser gensidige afhængigheder mellem centrale finansielle infrastrukturer.

Kortlægningen giver input til, hvor der kan være sårbarheder forbundet med fx koncentration på brug af få eller samme leverandører af kritiske systemer og netværk samt afhængigheder af offentlig infrastruktur, dvs. samfundets fælles digitale services og registre som NemID, e-Boks, Tingbogen, Det Centrale Personregister etc.

Fundamentet genbesøges minimum årligt, hvor det opdateres, eller hyppigere, såfremt forhold kræver et genbesøg.

4.2 Øvrige kilder til trusler og sårbarheder – ad [1]

Når risikoanalysen opdateres, indsamles endvidere input til trusler og sårbarheder i forhold til stabil drift af de fem kritiske forretningsaktiviteter. Der indsamles fx fra nedenstående kilder (ikke-udtømmende liste):

- Undersøgelse af FSOR-medlemmernes top-5-bekymringer
- Input fra Risikoforum for Gensidige Afhængigheder, RGA

- Input fra FSOR-RISK, herunder om kommende systemændringer og ny regulering
- CFCS' trusselsvurderinger
- Andre trusselsvurderinger, fx Nationalt Trusselsbillede, TIBER-DK's generiske trusselslandskab, NFCERT's kvartalsvise trusselsrapport og det europæiske samarbejde "Cyber Information and Intelligence Sharing Initiative (CIISI-EU)"
- Sårbarheder identificeret i FSOR's cyberstocktake
- Relevante hændelser.

Undersøgelsen af FSOR-medlemmernes top-5-bekymringer gennemføres årligt af FSOR's sekretariat. I undersøgelsen indhentes FSOR-medlemmernes 3-5 største bekymringer vedrørende stabil drift af kritiske forretningsaktiviteter i den finansielle sektor. Bekymringerne grupperes og indplaceres i et ISF-trusselskatalog, og der sammenlignes med resultaterne fra forrige år. Denne undersøgelse giver – sammen med øvrige kilder – input til, hvilke risici der skal fokuseres på i FSOR's risikoanalyse.

4.3 Risikobeskrivelser – ad [2]

Alle risici beskrives med risikoårsag, risikohændelse og risikoeffekt (bowtie-konceptet benyttes). Derudover kategoriseres hver risiko i en af fem nedenstående risikokategorier (risikokategorien fremgår af risikokortene):

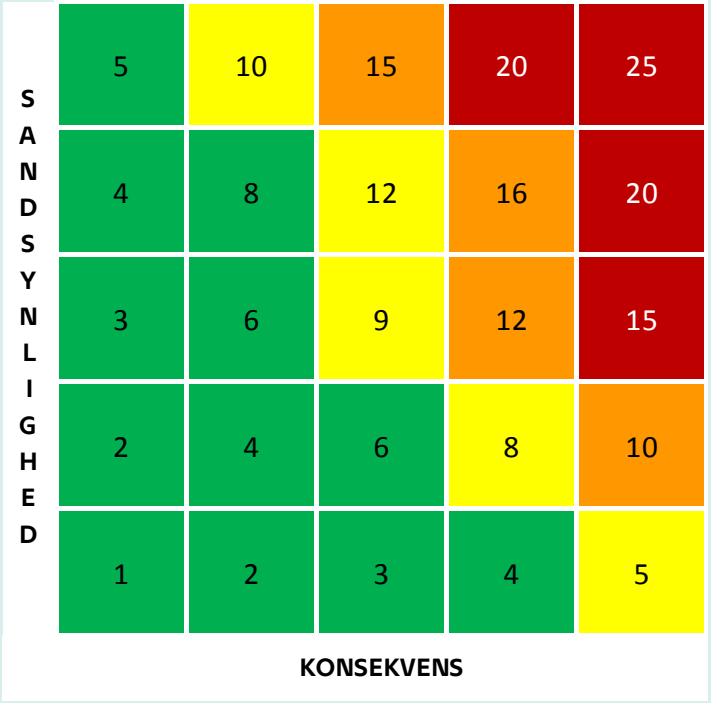
1. Driftsafbrydelser
2. Leverandørstyring
3. Cyberrobusthed
4. Compliance-risiko
5. Andet.

Risikobeskrivelserne danner grundlag for at give hver risiko en score på en skala fra 1 til 5 for henholdsvis sandsynlighed og konsekvens og indplacere risikoen i en risikomatrice, jf. næste afsnit.

5 Risikomatrice og risikoappetit – ad [2]

Indplacering af risici i risikomatricen sker ud fra en skala for henholdsvis sandsynlighed og konsekvens. Sandsynlighed (lodret akse) vurderes efter, hvor ofte en hændelse forventes at indtræffe, men den kan også vurderes ud fra bl.a. modenhed og kompleksitet på forskellige områder. Konsekvens (vandret akse) afspejler kriterierne for vurdering af, om den finansielle stabilitet potentielt er truet, jf. boks 1. Risikomatricen med alle skalaer fremgår af bilag 2.

FSOR's risikomatrice **Figur 2**



Anm.: Tallene angiver sandsynlighed (1-5) gange konsekvens (1-5).
Kilde: FSOR-RISK.

FSOR's risikomatrice inddeles i farverne rød, orange, gul og grøn, jf. figur 2. Farvefordelingen er let skævvredet mod nederste højre hjørne, således at FSOR er ekstra opmærksom på risici med høj konsekvens, også ved lav sandsynlighed.

6 Mitigerende tiltag – ad [3]

Alle risici rapporteres til FSOR. Risicienes farvekategori afspejler FSOR's risikoappetit og styrer FSOR's behandling af risiciene:

Risici i **rød**: FSOR drøfter alle risici i rød, og FSOR-RISK indstiller mitigerende tiltag til FSOR.

Risici i **orange**: FSOR drøfter alle risici i orange, herunder om der skal iværksættes potentielle mitigerende tiltag. FSOR-RISK giver input til, hvilke mitigerende tiltag det er mest relevant at iværksætte.

Risici i **gul**: FSOR drøfter, om der skal iværksættes mitigerende tiltag for udvalgte risici. FSOR-RISK giver input til, hvilke risici det er vigtigst at adressere.

Risici i **grøn**: Som udgangspunkt indstiller FSOR-RISK ikke mitigerende tiltag.

Der kan være behov for at indhente mere information om en risiko, før FSOR tager endelig stilling til, om en risiko skal gøres til genstand for mitigerende tiltag.

7 Løbende opdatering af risikoanalysen – årshjul

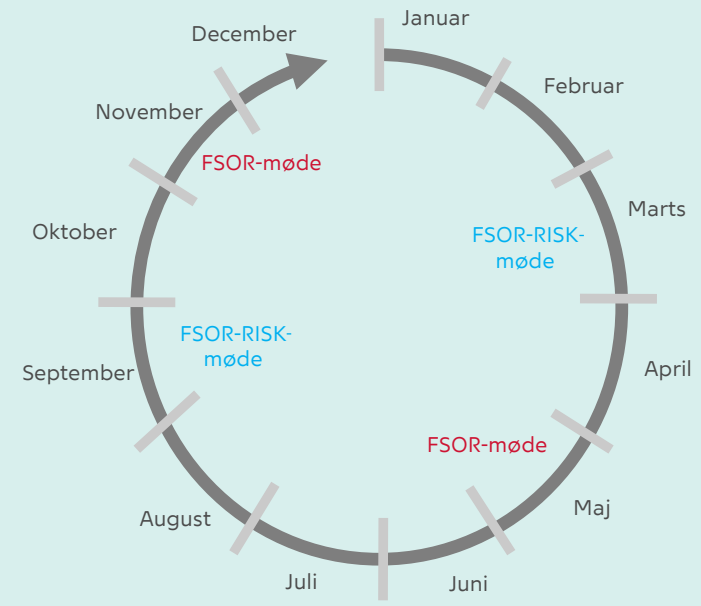
"Tragten" i figur 1 illustrerer, hvordan en enkelt opdatering af risikoanalysen gennemføres. I praksis er det en løbende proces, hvor risikoanalysen som udgangspunkt opdateres to gange årligt af arbejdsgruppen FSOR-RISK, der mødes hvert halve år – ca. 2 måneder før hvert FSOR-møde. Arbejdsgruppen rapporterer resultatet af opdateringen til FSOR til drøftelse på næstkommende FSOR-møde, jf. årshjulet illustreret i figur 3. Til FSOR-møderne rapporteres endvidere, hvad status er på igangsatte mitigerende tiltag, og det videre arbejde drøftes.

7.1 Arbejdsgruppemøder i FSOR-RISK

På arbejdsgruppemøderne varetages følgende opgaver:

- Input til trusler/sårbarheder/bekymringer drøftes, jf. **[1]** i figur 1.
- Indplaceringen af de eksisterende risici genbesøges, og eventuelle ændringer foretages, jf. **[2]**. Status på igangsatte mitigerende tiltag inddrages i drøftelserne, når det er relevant.
  - Nye risici drøftes og tilføjes eventuelt til risikoanalysen, jf. **[2]**, herunder berøres rutinemæssigt kommende større systemmæssige ændringer i infrastrukturen og ny regulering, der skal implementeres i den finansielle sektor, når det er relevant.
- Input til mitigerende tiltag, som skal fremlægges for FSOR, drøftes, jf. **[3]** i figur 1.
- Hvert 2.-3. år i **september** genbesøges bruttolisten over forretningsaktiviteter i den finansielle sektor, og risikoanalysens scope, dvs. de kritiske forretningsaktiviteter, genovervejes. Endvidere genbesøges tidshorisonten for, hvornår en forretningsaktivitet bliver kritisk, sammen med aktiveringskriterierne for FSOR's kriseberedskab.
- I **marts** genbesøges fundamentet for risikoanalysen (dvs. BIA'er for de kritiske forretningsaktiviteter og kortlægning).
- I **september** drøftes resultatet af undersøgelsen af FSOR-medlemmernes top-5-bekymringer vedrørende stabil drift af kritiske forretningsaktiviteter i den finansielle sektor.

Årshjul **Figur 3**



Kilde: FSOR-RISK.

- I **september** evalueres risikoanalysens metode, processer og modenhed, og der træffes beslutning om ændringer ved behov. Denne metodehåndbog opdateres, når det er relevant.

7.2 Telefonmøder

Mellem møderne kan der afholdes telefonmøder ved behov, hvor arbejdsgruppen fx drøfter sandsynlighed, konsekvens og behov for mitigerende tiltag for en opstået risiko.

7.3 Løbende input og håndtering

FSOR-RISK, FSOR-medlemmerne og FSOR's sekretariat kan løbende melde potentielle risici ind til risikoanalysen. Nye risici vil blive behandlet senest på næstkommende arbejdsgruppemøde, på et til lejligheden indkaldt telefonmøde eller på ekstra fysiske møder efter behov.

Ved behov for akut håndtering af en konkret situation varetages dette af FSOR's kriseberedskab.

8 Governance

8.1 Arbejdsgruppen FSOR-RISK

Risikoanalysen vedligeholdes af arbejdsgruppen FSOR-RISK, der sammensættes af repræsentanter fra et bredt udvalg af FSOR's medlemmer, herunder banker, finansielle infrastrukturer, datacentraler, myndigheder samt CFCS. FSOR's sekretariat leder arbejdsgruppen.

8.2 Dokumenthåndtering

Dokumenter vedrørende FSOR's risikoanalyse gemmes i området "FSOR risikoanalyse" på Nationalbankens ekstranet (fortroligt dokumenthåndteringssystem), hvortil arbejdsgruppen har adgang. FSOR's sekretariat vedligeholder området.

Risikoanalysen dokumenteres i et risikoværktøj, som opdateres af Nationalbanken. Risikoværktøjet gemmes på ekstranettet. Ligeledes gemmes de nyeste versioner af risikoanalysens fundament og metodehåndbog på ekstranettet.

FSOR klassificerer materiale ud fra en "Traffic Light Protocol", TLP. Der er fire klasser, som materialet kan kategoriseres i: TLP:HVID, TLP:GRØN, TLP:GUL og TLP:RØD. Dokumenter med informationer om trusler, sårbarheder, risici, mitigerende tiltag mv. klassificeres typisk som TLP:GUL (begrænset brug), hvilket påføres materiale, når indholdet har følsom karakter og kan have middelstore eller store negative følger for FSOR eller enkeltmedlemmer i tilfælde af læk. Dokumenter med TLP:GUL udveksles kun via ekstranettet og må alene deles på "need to know"-basis internt i FSOR-medlemmets organisation. Dokumenter med informationer om metoden klassificeres typisk med TLP:GRØN (intern brug), hvilket betyder, at de kan deles internt i medlemmets organisation til den arbejdsrelevante kreds. Udveksling af dokumenter med TLP:GRØN sker primært via ekstranettet. En oversigt over reglerne for fortrolighed, klassificering og håndtering af materiale fremgår af bilag 4, hvor det er specificeret, hvad TLP HVID, GRØN, GUL og RØD dækker over.

8.3 Ansvarsfordeling

Forskellige aktører kan være relevante for håndtering af de i risikoanalysen identificerede risici:

- Risici, hvor FSOR kan bidrage til øget operationel robusthed i den finansielle sektor ved fælles tiltag, håndteres af FSOR.
- Risici, som vedrører afhængigheder mellem VP, Kronos2 og detailbetalingssystemerne, overdrages til og håndteres af Risikoforum for Gensidige Afhængigheder, RGA.
- Risici, som vedrører flere kritiske sektorer i samfundet, bør håndteres på nationalt niveau.
- Nogle risici bør håndteres af enkelte aktører.

Der kan være behov for at håndtere en risiko på flere niveauer. Der er ikke en egentlig risikoejer for de risici, som håndteres af FSOR. Der udnævnes i stedet en tovholder blandt FSOR-medlemmerne for hvert af de initiativer, som FSOR vedtager at sætte i gang i forbindelse med risikoanalysen.

FSOR's sekretariat er overordnet ansvarlig for:
- at indkalde arbejdsgruppen til opdatering af risikoanalysen
- at materiale bliver udarbejdet og rapporteret til FSOR
- at koordinere igangsættelse af opgaver i forbindelse med mitigerende tiltag
- at koordinere rapportering af status på mitigerende tiltag.

FSOR-medlemmerne er ansvarlige for:
- at drøfte risici og godkende indplacerede risici i risikomatricen
- at beslutte, hvilke mitigerende tiltag der skal iværksættes
- at drøfte status på mitigerende tiltag, vedtage nye opgaver og foretage eventuelle justeringer
- at deltage i eller lede relevante undergrupper og taskforces, som nedsættes for at implementere mitigerende tiltag
- at indarbejde risici i egen risikostyring.

FSOR-RISK vedligeholder og opdaterer risikoanalysen. Herunder er opgaver i forbindelse med vedligeholdelse af risikoanalysens fundament fordelt blandt relevante medlemmer af arbejdsgruppen.

Bilag 1: Business Impact Analysis, BIA

FORRETNINGSAKTIVITET X

TLP

Ved brud på fortrolighed og integritet kan de konsekvenser, som ellers først opstår efter 1 uge, opstå med det samme

KONSEKVENSER AF NEDBRUD (TILGÆNGELIGHED):

1 time	4 timer	1 dag	1 uge
Mulige konsekvenser af et nedbrud, der varer i op til 1 time: • ... • ... • ... • ...	Mulige konsekvenser af et nedbrud, der varer i op til 4 timer: • ... • ... • ...	Mulige konsekvenser af et nedbrud, der varer i op til 1 dag: • ... • ... • ... • ... • ...	Mulige konsekvenser af et nedbrud, der varer i op til 1 uge: • ... • ... • ... • ... • ... • ...

UNDERLIGGENDE FORRETNINGSPROCESSER:

Underliggende proces 1:
• ...
• ...
• ...

Underliggende proces 2:
• ...
• ...

...

Underliggende proces *n*:
• ...
• ...
• ...

UNDERSTØTTENDE SYSTEMER [LEVERANDØRER]:

Infrastrukturer:
System A [Leverandør B]
System C [Leverandør D, Underleverandør E]
System F [Leverandør G, Leverandør H]

Netværk:
Netværk I [Leverandør J]
Netværk K [Leverandør L]

Offentlig infrastruktur:
Fælles digital service M [Leverandør N]
Fælles digital service O [Leverandør P]
Register Q [Leverandør R]

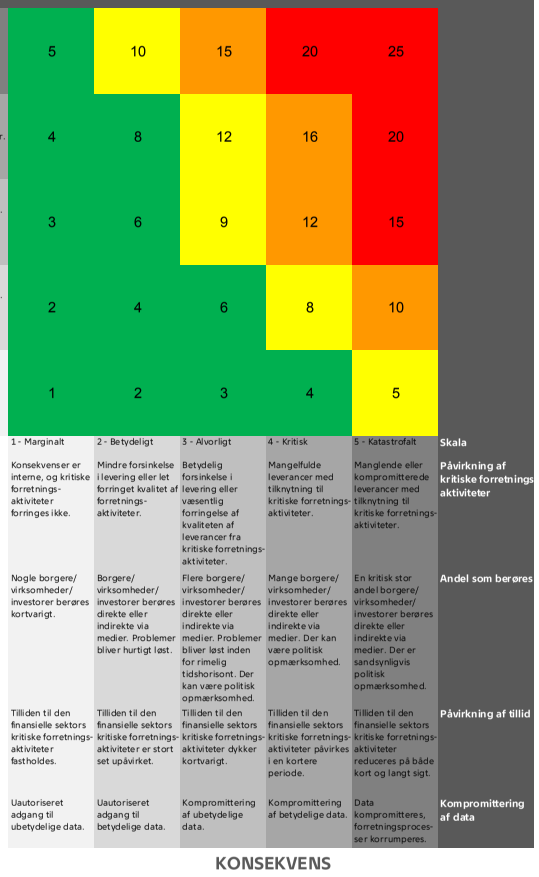
Anden service/infrastruktur:
Service S [Leverandør T]
Service U [Leverandør V]

Data:
Datasæt [Dataudbyder W]

Bilag 2: Risikomatrice

Trusselsbillede efter mitigerende handlinger	Vidensdeling og samarbejde	Deling af information om trusler mv.	Sporbarhed	Leverandør-kompleksitet	Modenhed og kontrolmiljø-bevidsthed hos relevante aktører og/eller leverandører	Manglende indsigt i risiko	Kompleksitet af it-arkitektur	Generelt
Meget høj	Aktører (og leverandører) arbejder separat på operationel robusthed og deler ikke viden.	Aktører (og leverandører) tilbageholder information om potentielle trusler, trusselsaktører, cyberangreb mv.	Næsten umulig at opdage, ingen beviser.	Ekstrem kompleksitet og/eller ingen governance og styring..	Ingen bevidsthed om risici og kontroller. Ikke kompetente og ikke tilstrækkelige ressourcer. Der udføres ikke eller meget sjældent tests, og de er dårligt dokumenterede.	Der er stor uklarhed om, hvor stor risikoen er. Det er ikke muligt at indhente viden om den egentlige risiko.	Ekstremt kompleks og ustabil drift.	Begivenheden sker 1 gang årligt.
Høj	Nogle aktører (og leverandører) deler viden på udvalgte/tilfældige områder.	Aktører (og leverandører) deler sjældent information om trusler, trusselsaktører, cyberangreb mv.	Kan påvises, muligt at indsamle beviser og dokumentation.	Meget komplekst leverandørbillede og svag governance og styring.	Ringe bevidsthed om risici og kontroller. Mangler på kompetence og ofte ikke tilstrækkelige ressourcer. Der testes og dokumenteres vilkårligt.	Der er stor uklarhed om, hvor stor risikoen er. Det er vanskeligt at indhente viden om den egentlige risiko.	Meget kompleks og varierende driftsstabilitet.	Begivenheden sker 1 gang på et tidspunkt inden for 1-3 år.
Middel	Nogle aktører (og leverandører) deler viden og samarbejder om løsninger på udvalgte områder.	Aktører (og leverandører) deler nogle gange information om trusler, trusselsaktører, cyberangreb mv. Det er ikke sat i system og kan være lidt tilfældigt.	Kan påvises, sletning af beviser og dokumentation kræver stor indsats og er kun muligt i kort tid.	Komplekst leverandørbillede og mindre stærk governance og styring.	Anvender standarder og dokumenterer dette. Begrænset bevidsthed om risici og kontroller. Delvist kompetente og ikke altid tilstrækkelige ressourcer. Der eksisterer men praktiseres ikke tilstrækkelige systematiske tests, og de er delvist dokumenterede.	Det er uklart, hvor stor risikoen er, men der er flere muligheder for at indhente viden om risikoens størrelse.	Normal kompleksitet og ret stabil drift.	Begivenheden sker sjældnere end hvert 3. år.
Lav	De fleste aktører (og leverandører) samarbejder om fælles problemstillinger, koordinerer tiltag og deler erfaringer og viden om best practice.	Aktører (og leverandører) deler al relevant information om potentielle trusler, trusselsaktører, cyberangreb mv.	Kan let påvises, beviser og dokumentation er ikke muligt at skjule.	Normalt leverandørbillede og rimelig governance og styring.	Følger anerkendte standarder og dokumenterer dette . Stærk bevidsthed om risici og kontroller. Kompetente og tilstrækkelige ressourcer. Der eksisterer og praktiseres systematiske tests, og de kan dokumenteres. Faste forbedringsrutiner følges	Der er nogen uklarhed om, hvor stor risikoen er, men gode muligheder for at øge viden om risikoen.	Mindre kompleksitet og ret stabil drift.	Begivenheden sker sjældnere end hvert 5. år.
Ingen trussels-vurdering	Aktører (og leverandører) samarbejder om relevante problemstillinger, koordinerer tiltag og deler systematisk erfaringer og viden om best practice. Aktørerne forholder sig aktivt til, hvilke områder det er relevant at	Information om trusler, trusselsaktører, cyberangreb mv. deles straks med andre aktører. Informationsdelingen er systematiseret og organiseret.	Fuld sporbarhed og dokumentation er til stede.	Enkelt leverandørbillede og stærk governance og styring	Følger anerkendte standarder og dokumenterer dette . Stærk bevidsthed om risici og kontroller. Kompetente og tilstrækkelige ressourcer. Der eksisterer og praktiseres systematiske tests, og de kan dokumenteres. Faste forbedringsrutiner følges.	Der er ret klart, hvor stor risikoen er, og der er gode muligheder for at indhente viden herom.	Lille kompleksitet og stabil drift.	Begivenheden sker sjældnere end hvert 10. år.

SANDSYNLIGHED



Bilag 3: Kontaktoplysninger

Organisation	Deltager	E-mail	Telefon

Bilag 4: Regler for fortrolighed

Regler for fortrolighed og håndtering af materiale fra FSOR Tabel 1

Farvekode	Beskrivelse	Informationsdeling	Forsendelse, opbevaring og destruktion
Hvid (TLP:HVID)	Materiale påføres koden TLP:HVID, når indholdet ikke har intern karakter for hverken FSOR eller dets medlemmer og dermed ingen negative virkninger har for FSOR eller enkeltmedlemmer i tilfælde af offentlig kendskab til indholdet.	TLP: HVID informationer og dokumenter kan cirkuleres internt i medlemmets organisation samt til eksterne interessenter eller samarbejdspartnere.	*Elektronisk forsendelse:* Ingen særlige krav til forsendelse. *Opbevaring:* Ingen særlig behandling eller krav til fysisk opbevaring. *Destruktion:* I almindelig papirkurv eller affaldssæk.
Grøn (TLP:GRØN)	Materiale påføres koden TLP:GRØN, når indholdet indebærer moderate negative følger for FSOR eller enkeltmedlemmer i tilfælde af læk. Fortrolighedsklassifikation "Intern brug".	TLP:GRØN informationer og dokumenter kan deles internt i medlemmets organisation til den arbejdsrelevante kreds.	*Elektronisk forsendelse*: Udveksling primært via Nationalbankens ekstranet. *Opbevaring:* Dokumenter skal påføres klassifikation og adgangsbegrænsning i overensstemmelse med farvekode ved elektronisk arkivering. Fysiske kopier opbevares i skab eller skuffe. *Destruktion:* I almindelig papirkurv eller affaldssæk.
Gul (TLP:GUL)	Materiale påføres koden TLP:GUL, når indholdet har følsom karakter og kan have middelstore eller store negative følger for FSOR eller enkeltmedlemmer i tilfælde af læk. Fortrolighedsklassifikation "Begrænset brug".	TLP:GUL informationer og dokumenter må alene deles på "need to know"-basis internt i medlemmets organisation.	*Elektronisk forsendelse*: Udveksling kun via Nationalbankens ekstranet. *Opbevaring:* Dokumenter skal påføres klassifikation og adgangsbegrænsning i overensstemmelse med farvekode ved elektronisk arkivering. Fysiske kopier opbevares i skab eller skuffe. *Destruktion:* I almindelig papirkurv eller affaldssæk.
Rød (TLP:RØD)	Materiale påføres koden TLP:RØD, når indholdet har særlig følsom karakter og kan have meget store negative følgevirkninger for FSOR eller enkeltmedlemmer i tilfælde af læk. Fortrolighedsklassifikation "Fortroligt" eller "Strengt fortroligt".	TLP: RØD informationer og dokumenter må ikke deles med andre uden for den personkreds, fx fra møde eller samtale, som de oprindelig deles i.	*Elektronisk forsendelse:* Udveksling kun via Nationalbankens ekstranet. *Opbevaring:* Dokumenter skal påføres klassifikation og adgangsbegrænsning i overensstemmelse med farvekode ved elektronisk arkivering. Fysiske kopier opbevares i skab eller skuffe. *Destruktion*: I makulator eller særlig lukket container beregnet til fortrolige dokumenter.