FSPOS

Finansiella Sektorns Privat-Offentliga Samverkan

Identifiering och värdering av cyberrisker

2021-06-14
FSPOS Arbetsgrupp Analys

1 INLEDNING 3

1.1 SYFTE OCH METOD 3

2 BESKRIVNING AV BEGREPPET CYBERRISK 4

3 IDENTIFIERING OCH VÄRDERING AV CYBERRISKER 5

3.1 HOTBILDEN 5
3.2 RISKHANTERINGSPROCESSEN 6
3.3 ANVÄNDNING AV VERKTYG VID IDENTIFIERING OCH VÄRDERING AV CYBERRISKER 7
3.4 PRAKTISKA ERFARENHETER VID IDENTIFIERING OCH VÄRDERING AV CYBERRISKER 9
3.5 FÖRVÄNTNINGAR FRÅN TILLSYNSMYNDIGHETERNA 10

BILAGA – ENKÄTFRÅGOR TILL VERKSAMHETSUTÖVARE 13

1 Inledning

Betydelsen av cybersäkerhet inom finanssektorn, liksom inom andra samhällsviktiga sektorer, har både vuxit och synliggjorts under de senaste åren och cyberrisker utgör ett hot mot aktörernas verksamheter. I World Economic Forums årliga riskrapport[1] bedöms cyberhot vara det fjärde mest sannolika hotet att materialiseras inom de kommande två åren. Betydelsen av cyberhot understryks av Federal Reserves ordförande, Jerome H. Powell, som menar att cyberattacker är det största hotet mot hela det globala finansiella systemet.[2] Cybersäkerhet är en strategisk fråga för styrelser och ledningsgrupper som har det yttersta ansvaret, vilket ställer krav på proaktivitet och förmåga att fatta riskbaserade beslut. Den finansiella sektorn omfattas dessutom av ett flertal regelverk som ställer krav på aktörernas hantering av cyberrisker. Förmågan att identifiera och värdera cyberrisker på ett effektivt sätt är därmed centralt för att bemöta den växande hotbilden.

I takt med den tekniska utvecklingen och digitaliseringen har betydelsen av cyberrisker ökat ytterligare. Covid-19-pandemin har tvingat organisationer att ha stora delar av personalen arbetande på distans, vilket har inneburit ny riskexponering och risk för cyberintrång. Samtidigt blir it-system mer komplexa och sammanlänkade, både inom organisationer och mellan dessa och tredjepartsleverantörer, vilket ökar sårbarheten vid exempelvis dataintrång och överbelastningsattacker. En störning i organisationens verksamhetskritiska it-system kan få direkta och allvarliga konsekvenser såväl för den drabbade aktören som för andra organisationer och leverantörer, och i förlängningen utgöra en systemrisk för det finansiella systemet.

1.1 Syfte och metod

Detta PM beskriver hur verksamhetsutövare inom finansiell sektor arbetar med identifiering och värdering av cyberrisker. PM:et ger exempel på verktyg som kan användas, samt praktiska erfarenheter och utmaningar som finns i arbetet med cyberrisker.

Kunskapsunderlaget är inhämtat dels från öppna källor som exempelvis föreskrifter, standarder och andra publicerade rapporter, dels från enkätsvar från verksamhetsutövare som deltar i FSPOS arbete. Innehållet bygger på information som har erhållits genom FSPOS arbete och dess medlemmar.

---

[1] *World Economic Forum, The Global Risks Report 2021 16th Edition, http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf*

[2] *https://edition.cnn.com/2021/04/12/business/jerome-powell-cyberattacks-global-threat/index.html*

2 Beskrivning av begreppet cyberrisk

Begreppet cyberrisk är komplext och kan definieras på olika sätt beroende på vilken källa som används. En del använder en akademisk definition medan andra utgår från ett mer praktiskt synsätt. Innan begreppet cyberrisk beskrivs bör begreppen operativ risk, riskhantering och riskaptit förklaras.

Med operativ risk menas risken för förluster till följd av ej ändamålsenliga eller fallerade processer, människor, system eller yttre händelser, inbegripet legala risker.[3] För att hantera operativa risker behöver organisationen arbeta med riskhantering enligt en standard[4], bestämma sannolikheten för att en händelse inträffar och den potentiella konsekvens som händelsen medför. Med denna information kan organisationen bedöma en acceptabel nivå av operativ risk för att uppnå organisationens strategiska mål och därmed definiera sin riskaptit[5], vilket är ett krav enligt Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker, FFFS 2014:4.

Detta PM utgår från den beskrivning av begreppet cyberrisk som Financial Stability Board (FSB) har sammanställt i ett cyberlexikon från 2018,[6] då FSB anses ha en stark ställning inom finansiell sektor globalt. Med cyberrisk menas kombinationen av sannolikhet för och konsekvenser av cyberincidenter. En cyberincident är en händelse som (1) äventyrar bevarandet av konfidentialitet, och riktighet hos, samt tillgänglighet till, informationssystem eller information som systemen hanterar, lagrar eller sänder (via kommunikationsnätverk), eller (2) bryter mot säkerhetspolicyer, oavsett om det sker med ont uppsåt eller inte. Cyberrisker är med andra ord en form av operativa risker som uppkommer i informationssystem eller när data överförs via kommunikationsnätverk.

Genom att förstå risklandskapet uttryckt i cyberrisker och riskaptit, kan organisationen vidta väl avvägda och kommunicerade riskhanteringsbeslut för ökad cybersäkerhet och därigenom stärka sin digitala operativa motståndskraft. Till följd av komplexiteten vad gäller cyberrelaterade risker, i kombination med att det inte finns någon entydig definition av begreppet cyberrisk, finns ett flertal utmaningar kopplat till identifiering och värdering av cyberrisker, inklusive rapportering till organisationens ledning och styrelse. Några av dessa utmaningar kommenteras nedan.

---

[3] *Europaparlamentets och rådets förordning (EU) nr 575/2013, 26 juni 2013, artikel 4.1 (52)*
[4] *Förslagsvis enligt ISO 31 000:2018 Risk management*
[5] *NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 16, 2018*
[6] *https://www.fsb.org/2018/11/cyber-lexicon/*

3 Identifiering och värdering av cyberrisker

Detta avsnitt beskriver hur den finansiella sektorn kan arbeta med identifiering och värdering av cyberrisker och tar sin utgångspunkt i den aktuella hotbilden och de utmaningar som detta innebär. Arbetet med cyberrisker utgår från riskhanteringsprocessen samt Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker, FFFS 2014:4.

I avsnittet ges exempel på metoder och arbetssätt för identifiering och värdering av cyberrisker som återfinns i standarder och andra publikationer, samt en beskrivning av hur några aktörer i den finansiella sektorn arbetar med detta.

3.1 Hotbilden

I Finansinspektionens promemoria om cyberhot och finansiell stabilitet[7] konstateras att de senaste decenniernas digitala utveckling innebär stora möjligheter men samtidigt ställer krav på att hantera de risker som utvecklingen för med sig.

Några av huvuddragen från Finansinspektionens slutsatser följer nedan.

- Problem relaterade till cyber- och it-risker är av skiftande karaktär och kan uppdelas i icke-antagonistiska (rena tekniska problem och handhavandeproblem) respektive antagonistiska störningar (cyberattacker där någon medvetet skapar störningar för att komma över pengar eller information, manipulera uppgifter eller för att sabotera verksamheten).
- Effekterna av icke-antagonistiska och antagonistiska störningar är i stort sett samma. En god nivå på den rent operativa säkerheten är ett sätt att bygga motståndskraft och robusthet även mot cyberattacker. Finansinspektionen menar dock att vardagliga störningar kan ses som ett större problem i kvantitativ mening medan de mer omfattande attackerna fortfarande är ovanliga.
- Cyberattacker kräver ett särskilt fokus och i viss mån separat hantering då de adderar ytterligare en riskdimension utöver de traditionella operativa riskerna i form av komplexitet i hanteringen – analytiskt, juridiskt, tekniskt och organisatoriskt.
- Sannolikheten bedöms vara större för att samhällspåverkande och systemhotande incidenter inträffar, till exempel ett haveri i betalningssystem, till följd av en teknisk incident än av en cyberattack

[7] *Cyberhot och finansiell stabilitet – FI:s roll och uppgifter, Promemoria 4 mars 2021, FI Dnr 20-3685*

utförd som en antagonistisk handling. Skadorna av en antagonistisk attack kan dock väntas bli större.

I Europeiska kommissionens cybersäkerhetsstrategi från 2020[8] konstateras att finanssektorn är en av de mest utsatta sektorerna för cyberattacker och det finns fortfarande mycket att lära och utveckla i fråga om beredskap och medvetenhet. Hotbilden skapar nya behov av finansiell reglering, tillsyn och brett samarbete på europeisk nivå med olika aktörer, såväl privata som offentliga.

Riksbanken konstaterar i en ekonomisk kommentar från 2021[9] att cyberattacker riskerar att påverka den finansiella stabiliteten och utgör därmed en systemrisk. Bland annat konstateras att cyberrisker karaktäriseras av snabbhet och skalbarhet, där en cyberattack har potential att snabbt nå mycket stor spridning och innebär därför ett systemhot. Även indirekt kan attacker påverka den finansiella stabiliteten genom att de påverkar det allmänna förtroendet för det finansiella systemet.

3.2 Riskhanteringsprocessen

Finansinspektionen har tagit fram en rapport om operativ riskhantering[10] som beskriver en modell med komponenter i ett riskhanteringssystem. Denna modell är allmänt accepterad och används inom den finansiella sektorn. Modellen startar med riskstrategin som utgör ramverket för hur hanteringen ska se ut, vilken sedan formaliseras genom företagets riskpolicy.

Riskpolicy följs av riskhanteringsprocessen som omfattar (1) identifiering och (2) värdering av risker, (3) åtgärder för att styra riskprofilen, samt (4) rapportering av riskerna. Processen stöds av ett antal olika analysverktyg som självutvärderingar, processanalys, riskindikatorer eller avancerade interna modeller (AMA, Advanced Measurement Approach).

Detta PM fokuserar främst på steg (1) och (2) i riskhanteringsprocessen, se figur 1. På övergripande nivå bör hantering av cyberrisker inte skilja sig från hantering av övriga operativa risker, varför denna modell är fullt tillämpbar även för identifiering och värdering av cyberrisker. I Finansinspektionens föreskrifter om

---

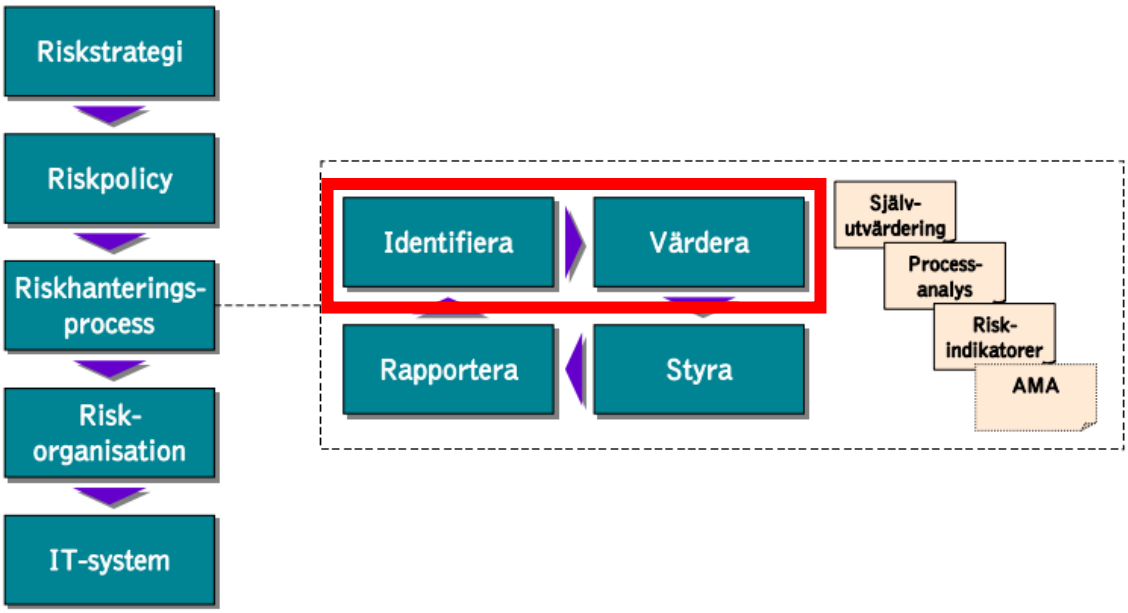
[8] *Gemensamt meddelande till Europaparlamentet och Rådet, EU:s strategi för cybersäkerhet för ett digitalt decennium, JOIN(2020) 18 final*

[9] *https://www.riksbank.se/sv/press-och-publicerat/nyheter-och-pressmeddelanden/nyheter/2021/cyberattacker-har-potential-att-hota-den-finansiella-stabiliteten/*

[10] *Operativa risker - företagens hantering och FI:s rekommendationer, Rapport 13 december 2006, DNR 06-11714-601*

hantering av operativa risker, FFFS 2014:4, omnämns steg (2) som mätning av risker, vilket kan likställas med värdering av risker.

De regler som finns utgivna av EBA och EIOPA inom området för hantering av cyber- och IKT-risker fungerar som allmänna råd i lagens mening och detaljerar Finansinspektionens riktlinjer. De allra flesta aktörer använder någon form av ramverk eller standard för hantering av cyberrisker.



Figur 1. Komponenter i ett riskhanteringssystem (Finansinspektionen 2006:18)

3.3 *Användning av verktyg vid identifiering och värdering av cyberrisker*

Självutvärdering, processanalys och riskindikatorer används ofta för identifiering och inventering av operativa risker. Självutvärdering är ett vanligt verktyg som innebär att organisationens riskfunktion analyserar sina identifierade risker och värderar dem med hjälp av på förhand framtagna checklistor. Processanalysen går systematiskt igenom processdokumentation, normalt i form av processkartor, och identifierar risker med stöd av en detaljerad riskklassificering. Riskindikatorer utgår från nyckeltal och mäter funktionen i processen över tid i syfte att komplettera de subjektiva riskanalysmetoderna.

Vid identifiering och inventering av cyberrisker är olika former av självutvärdering en vanligt förekommande metod. Här finns ett flertal internationella standarder som är tillämpbara inom finanssektorn, varav några omnämns nedan. En del av dessa standarder utgör ett komplett ramverk/ledningssystem för hantering av företagets cybersäkerhet, medan andra är bäst lämpade som rena checklistor.

Nästa steg i riskhanteringsprocessen är värdering och kvantifiering av cyberrisker. I detta steg värderas och kvantifieras riskerna utifrån de viktigaste riskhändelserna, med vilken sannolikhet de kan inträffa, hur allvarlig förlusten blir om risken faller ut, hur stor exponering som risken representerar, samt storlek på kapitalkrav för att hantera risken.

Enkätsvaren visar att några av de mest använda verktygen av aktörer i finanssektorn är *ISO 27001* i kombination med *NIST Cyber Security Framework*[11] samt *ISF Standard of Good Practice for Information Security*[12]. Några aktörer tillämpar även *ISF Information Risk Assessment Methodology 2*[13] samt *CIS Top 20 Critical Security Controls*[14] i olika uträckning i arbetet med cyberrisker.

Även verktyg utgivna av *Open Web Application Security Project (OWASP)*[15] samt organisationens *Security Operations Center (SOC)*[16] lyfts fram som viktiga stöd i arbetet med identifiering och inventering av cyberrisker. Ytterligare exempel som lyfts fram är vikten av nationella och internationella samverkansforum i syfte att utbyta erfarenheter.

Enkätsvaren visar också att aktörer baserar identifiering och värdering av cyberrisker på *ISO 27005* samt *MSB:s metodstöd för systematiskt informationssäkerhetsarbete*[17]. Egenutvecklade metoder baserade på *ISO 27001* förekommer också. För några aktörer ligger *ISO 31000* till grund för arbetet med operativa risker, där sannolikhets- och konsekvensskalor för värderingen av risker anpassas till organisationens verksamhet.

---

[11] *https://www.nist.gov/cyberframework*
[12] *https://www.securityforum.org/solutions-and-insights/standard-of-good-practice-for-information-security-2020/*
[13] *https://www.securityforum.org/solutions-and-insights/information-risk-assessment-methodology-iram2/*
[14] *https://www.cisecurity.org/controls/cis-controls-list/*
[15] *https://owasp.org/*
[16] *https://en.wikipedia.org/wiki/Security_operations_center*
[17] *https://www.informationssakerhet.se/metodstodet/*

Det verkar inte finnas något entydigt svar på vad som anses vara *best practice* inom sektorn. Ett flertal aktörer bedömer frågan som komplex och svårbesvarad. De standarder som ändå omnämns som *best practice* för identifiering och värdering av cyberrisker är *NIST Risk Management Framework*[18] och *NIST Cyber Security Framework*. Genom den kommande Dora-förordningen[19] förtydligas vikten av att använda standarder ännu tydligare. Även *ISO 27001* uppfattas som *best practice* inom den svenska/nordiska marknaden. För hantering av cyberrisker omnämns *ISO 27001* och *NIST Cyber Security Framework* som *best practice*. Vad gäller standarder för benchmarking/mätning av säkerhetsnivåer är uppfattningen att variationen av använda standarder är betydligt större.

3.4 Praktiska erfarenheter vid identifiering och värdering av cyberrisker

Enkätsvaren visar att aktörernas praktiska erfarenheter vid användning av de verktyg som beskrivs ovan, indikerar ett stort behov av anpassning till den egna verksamheten. Standarder, ramverk och verktyg som tillämpas skapar förutsättningar och ger stöd i införandet men behöver anpassas efter organisationens förutsättningar och behov för att fungera i praktiken.

Några ytterligare erfarenheter som lyfts fram är behovet av att kunna sammanfatta verksamhetens identifierade cyberrisker och åtgärder för att hantera riskerna på ett konstruktivt sätt till ledningen. Även vikten av att ansvariga inom riskfunktionen säkerställer användning av och utbildning i verktygen och lokalt anpassade mallar ute i organisationen framhålls som en viktig parameter för ett lyckat införande. Det anses vara viktigt att ramverket för hantering av cyberrisker används i det dagliga arbetet med cybersäkerhet, inte enbart en gång per år vid exempelvis en övning. Ramverket ska ligga till grund för organisationens förändringsarbete och vara integrerat med organisationens ramverk för operativ risk-, kontinuitets- och säkerhetshantering.

En viktig faktor som lyfts fram är att tillgängliga verktyg för mätning och värdering av cyberrisker påverkas av det faktum att standarder ständigt ändras och utvecklas, vilket försvårar möjligheten till jämförbara resultat och att kunna påvisa förbättringar över tid. En ytterligare viktig faktor är behovet av att tillgängliggöra resultat från andra organisationer inom finanssektorn i benchmarkingsyfte.

---

[18] *https://csrc.nist.gov/projects/risk-management/about-rmf*
[19] *https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:52020PC0595&from=EN*

ISO 27000-serien anses vara värdefull utifrån ett internstyrningsperspektiv, där NIST-standarden fungerar som ett bra komplement i syfte att utvärdera organisationens cybersäkerhetsarbete. Det kan också konstateras att flertalet verktyg förutsätter att organisationen har uppnått en tillräckligt hög riskmognadsnivå och har erfarenhet av operationell riskhantering sedan tidigare för att uppnå en effektiv hantering av cyberrisker.

En utmaning med identifiering av cyberrisker är den tids- och resursåtgång som krävs för att genomföra hotbilds- och riskanalyser. Några aktörer anser att detta arbete bör prioriteras högre då det kräver att representanter från alla delar av verksamheten deltar. I detta sammanhang nämns också utmaningen i att utbilda medarbetare i syfte att kunna fånga upp och rapportera cyberrisker och incidenter i en stor organisation. En ytterligare utmaning som lyfts fram är svårigheten att hitta rätt nivå på cyberrisker för att möjliggöra tydlig rapportering till ledning och styrelse. En ökad tydlighet i rapportering till ledning och styrelse behövs enligt aktörerna.

Värdering av cyberrisker är också något som generellt sett lyfts fram som utmanande av ett flertal aktörer. Ett exempel är utmaningen i att översätta cyberrisker till ett monetärt värde, liksom svårigheten att bedöma relevanta och trovärdiga kostnader för åtgärder av cyberrisker. En ytterligare utmaning är svårigheten att kunna bedöma kontrollernas styrka vid organisationens egenutvärdering. En potentiell angripare kan utnyttja eventuella brister i kontrollerna eller andra sårbarheter som verksamheten har svårt att bedöma i förväg.

Nya cyberrisker som uppkommer i samband med teknikskiften, förändringar i it-infrastruktur och arbetssätt upplevs som utmanande, liksom förmågan att kunna identifiera de senaste trenderna och hoten inom cyberområdet, samt nya risker koppat till dessa. Exempel på detta är användning av molntjänster och *DevOps*[20] som har förändrat många organisationers sätt att arbeta på.

3.5 Förväntningar från tillsynsmyndigheterna

I detta avsnitt presenteras ett urval av förväntningar från Finansinspektionen på aktörernas arbete med identifiering och värdering av cyberrisker. Dessa

[20] *DevOps härstammar från orden "development" och "operations" och är ett sätt att utveckla mjukvara eller system där ett team utvecklar, driftar, testar, integrerar och övervakar ett system i ett automatiserat flöde, vilket i praktiken innebär att teamet tar ansvar för mjukvarans eller systemets hela livscykelhantering*

förväntningar kopplas till några överväganden samt aktörernas egna erfarenheter inom området.

I Finansinspektionens tillsynsrapport från december 2018[21] utpekas några centrala förväntningar som myndigheten har på bank- och finanssektorn:

- Vikten av tydligt införda ledningssystem för informationssäkerhet (LIS), baserat på exempelvis *ISO 27001*, *NIST Cyber Security Framework* eller *ISF Standard of Good Practice for Information Security*.
    - Enkätsvaren bekräftar att aktörerna helt eller delvis har infört ett LIS enligt någon av de standarder som föreslås av Finansinspektionen, eller har utvecklat ett eget ledningssystem baserat på dessa standarder.

- Vikten av tydliga roller och ansvarsområden när det gäller information- och cybersäkerhet. Styrelsen och ledningen behöver visa engagemang, ha en god förståelse för påverkan av informations- och cyberrisker, samt styra och följa upp arbetet.
    - Enkätsvaren visar att de tillfrågade aktörerna har tydligt definierade roller och ansvarsområden beträffande information- och cybersäkerhet, samt hur de arbetar med cyberrelaterade risker. Dessa finns beskrivna i styrande dokument (till exempel policyer och processer) som aktörerna kontinuerligt arbetar med att förbättra för att följa utvecklingen både internt och externt. Dessutom finns en utpekad central riskfunktion hos aktörerna som ansvarar för insamling, sammanställning och rapportering av cyberrisker till styrelse, ledning och andra viktiga funktioner.

- Vikten av en tydlig och uppdaterad riskanalys och adekvata kontrollfunktioner (funktionerna för riskkontroll och internrevision) för att värdera informations- och cyberrisker. Riskhantering behöver göras på olika nivåer och de etablerade riskkategorierna affärsrisk och strategisk risk behöver kompletteras med informationssäkerhets- och cyberrisker.
    - Här framgår av enkätsvaren att arbetet med cyberrisker är väl integrerat med aktörernas övergripande arbete med operativa risker och gällande risktaxonomi. Samtidigt lyfts ett antal förbättringsområden fram som exempelvis förtydligande av riskansvar, effektivare bedömning av riskaptit, ett tydligare

[21] *https://www.fi.se/contentassets/84144fb815c44be88f2bc1773e55a559/fi-tillsyn-9-banker-info-cybersakerhet.pdf*

verksamhetsperspektiv på cyberrisker, samt minska den tekniska komplexiteten i riskerna.

- Vikten av att informations- och cyberrisker alltid beaktas i samband med uppdragsavtal när verksamhet läggs ut på en utomstående part. Även hantering av risker kopplade till redan ingångna avtal om utlagd verksamhet behöver ske kontinuerligt. I båda fallen behöver leverantörerna involveras aktivt i riskarbetet.
    - Här visar enkätsvaren att det finns vissa utmaningar i att involvera leverantörerna i riskarbetet. Generellt uppger aktörerna att arbete pågår för att förbättra samarbetet med leverantörer i ännu högre grad. Några leverantörer upplevs inte ha kommit tillräckligt långt i sitt eget riskarbete, medan andra är mer proaktiva. Aktörerna anger också att ytterligare förbättringar kan göras i kravställandet gentemot leverantörer.

- Vikten av att cyberrisker analyseras årligen och vid förändringar som kan påverka informationssäkerheten, samt att analysen omfattar såväl människor och processer som teknik. Verksamhetens mest kritiska informationstillgångar behöver identifieras genom en strukturerad och uppdaterad kunskapsdatabas över användare, enheter, it-system och deras inbördes beroenden.
    - Enkätsvaren visar att de tillfrågade aktörerna genomför informationsklassificering av system och tjänster som kompletteras av bland annat gapanalys mellan informationsklass och nuvarande krav. Aktörerna genomför regelbundet hotbilds- och riskanalyser, där även säkerhetsgranskningar och leverantörsgranskningar ingår. Några ytterligare exempel på aktiviteter som genomförs är övervakning av nätverkstrafik i it-infrastrukturen i syfte att fånga upp avvikande beteende och andra sårbarheter, samt löpande rapportering och uppföljning av cyberrelaterade kontroller och incidenter för särskilt utsatta system och centrala plattformar.

Bilaga – Enkätfrågor till verksamhetsutövare

1. Vilka är de största utmaningarna med identifiering och värdering av cyberrelaterade risker i er verksamhet?

2. Vilka verktyg/ramverk/standarder/ledningssystem etc använder ni för att identifiera och värdera cyberrelaterade risker i er verksamhet? Vad uppfattar ni som ”best practise” inom området?

3. Vilka är era erfarenheter när det gäller dessa verktyg, vad krävs för att de ska fungera inom ramen för verksamhetens riskstyrning och rapportering till ledning?

4. Hur fångar ni upp risker i olika delar av verksamheten som har koppling till cyberrelaterade hot? Hur arbetar ni med hotbildsanalys som lägger grunden för er riskaptit?

5. Finns tydliga roller och ansvarsområden definierade när det gäller informations- och cybersäkerhet, samt hur dessa arbetar med cyberrelaterade risker?

6. Hur integrerat är arbetet med cyberrelaterade risker med ert övriga arbete med operativa och strategiska risker? Vilka eventuella förbättringsbehov ser ni?

7. Hur upplever ni samarbetet med tredjepartsaktörer när det gäller att identifiera och värdera cyberrelaterade risker? Deltar era leverantörer aktivt i riskarbetet?