Cybermätaren

Nationell bedömningsmodell för cybersäkerhet

Bruksanvisning

Innehåll

1 Inledning ... 3
1.1 Målgrupp ... 4
1.2 Inledning ... 4
2 Användning av Cybermätaren ... 5
2.1 Starta bedömningen ... 5
2.2 Förbered bedömningen ... 6
2.3 Genomför bedömning med Cybermätaren ... 7
2.4 Identifiera utvecklingsåtgärder ... 7
2.5 Utveckla verksamheten och uppdatera bedömningen ... 8
3 Cybermätarens bedömningsmodell ... 11
3.1 Viktigaste begrepp ... 11
3.2 Avsnitt, mål och rutiner ... 12
3.3 Beräkningsmodell för mognadsnivå ... 13
4 Detaljerad anvisning för bedömningens projektledare ... 16
4.1 Mer om nyckelpersoner och roller ... 16
4.2 Bestämning av verksamhetsdelområde som ska bedömas ... 18
4.3 Sätt att genomföra bedömningen ... 20
4.4 Bedömningsresultat och rapporter ... 22
5 Detaljerad ifyllnadsanvisning för bedömningsverktyget Cybermätaren ... 26
5.1 Fliken Cybermätaren (Kybermittari) ... 26
5.2 Avsnittsspecifika flikar ... 29
5.3 Fliken Investeringar ... 31
5.4 Rapporter och jämförelseuppgifter ... 32
6 Ordlista ... 34
7 Källförteckning ... 39

1 Inledning

Hoten mot infrastruktur som är kritisk för samhället har utvecklats och blivit mer komplexa. Speciellt cyberhoten har ökat. Skyddet mot cyberhot har blivit en väsentlig del av att säkerställa informationssamhällets funktion och försörjningsberedskap. På grund av att funktionerna är sinsemellan beroende måste det säkerställas att varje organisation som är kritisk för samhällets funktion har beredskap för cyberhot. Detta kräver nationellt samarbete för att utveckla cybersäkerheten i organisationer, branscher och samhället.

I dag mäts cybersäkerhet med olika slags referensramar beroende på organisation och bransch. Resultaten som uppnås med olika referensramar är ofta inte jämförbara vilket gör det svårare att jämföra resultaten och ställa upp enhetliga utvecklingsmål. Förutom gemensamma mätare saknas metoder för att dela konfidentiell information om organisationens mognadsnivå och bästa praxis för att utveckla cybersäkerheten.

Cybermätaren är en nationell bedömningsmodell för cybersäkerhet utvecklad vid Cybersäkerhetscentret vid Transport- och kommunikationsverket Traficom. Bedömningsmodellen erbjuder ett enhetligt sätt för bedömning och utveckling av cybersäkerhet. Modellen har sammanställts av nationell och internationell praxis och med lösningen går det att övergripande bedöma status för cybersäkerheten i ett företag, en bransch och samhället samt identifiera potentiella utvecklingsområden. En nationell modell gör det möjligt att jämföra företag och branscher på ett enhetligt sätt och skapa ett gemensamt sätt att mäta och utveckla cybersäkerheten. Cybersäkerhetscentrets roll stöder modellens kontinuitet och långsiktighet samt skapar förutsättningar att dela konfidentiell information om bästa praxis, rekommendationer och referensresultat i samarbetet med kritiska organisationer.

Cybersäkerhetscentret tillhandahåller mätaren fritt för användning av företag, organisationer och offentliga aktörer. Dessutom kan den utnyttjas av kommersiella aktörer och myndigheter. Cybermätarens materialpaket och aktuella användningsvillkor finns på www.kybermittari.fi på finska, svenska och engelska. Mätarens huvudsakliga målgrupp är företag som är kritiska för försörjningsberedskapen, men den lämpar sig för bedömning av alla slags företag, organisationer och offentliga aktörer oberoende av bransch.

Nyttan med Cybermätaren för företag, organisationer och offentliga aktörer är bland annat:

- En öppen och fritt tillgänglig modell för bedömning av cybersäkerhet och för långsiktig styrning av utvecklingsverksamheten.
- Jämförelse av mognadsnivån i förhållande till andra finländska aktörer ("benchmarking") och delning av bästa praxis mellan aktörer.
- En gemensam modell för kommunikation, bedömning och utveckling av cybersäkerhet tillsammans med underleverantörer, tjänsteleverantörer och myndigheter.

På nationell nivå stöder Cybermätaren den nationella cybersäkerhetsstrategin där en strategisk åtgärd är utveckling av verifiering, testning, bedömning och användningsrekommendationer för produkter och hela lösningsmiljöer i anslutning till kritiska funktioner. En bred användning av mätaren stöder bildande av en nationell lägesbild, myndighetsverksamhet och beslutsfattande samt underlättar fokuseringen av nationella resurser.

1.1 Målgrupp

Denna bruksanvisning är avsedd att stöda användning och ibruktagning av Cybermätaren. Den ger anvisningar och råd för att ta mätaren i bruk, för genomförande av bedömningen och för att utnyttja resultaten. I organisationer är bruksanvisningen speciellt riktad till organisationsledningen, experter inom riskhantering och cybersäkerhet samt andra parter som deltar i bedömningen. Anvisningen har följande delar:

- **Kapitel 2** beskriver hur organisationen bäst kan utnyttja Cybermätaren och vad som krävs för att ta den i bruk i organisationen.
- **Kapitel 3** beskriver Cybermätarens struktur och funktionsprinciper.
- **Kapitlen 4 och 5** innehåller mer detaljerade anvisningar och rekommendationer för att använda Cybermätaren och genomföra bedömningar, stöda speciellt projektledare och deltagare i bedömningarna.
- **Kapitel 6** innehåller en lista över termer inom cybersäkerhet och i Cybermätaren.

Bruksanvisningen är avsedd att användas tillsammans med bedömningsverktyget.

1.2 Inledning

Cybermätaren har utvecklats i samarbete mellan Cybersäkerhetscentret och Försörjningsberedskapscentralen under 2019–2020 och den första versionen publicerades i oktober 2020. För underhåll av mätaren och fortsatt utveckling svarar Cybersäkerhetscentret.

I utvecklingsarbetet ville man som grund använda en befintlig internationellt känd referensram som är aktivt uppdaterad och fritt tillgänglig. Med dessa urvalskriterier valdes efter en bred kartläggning två referensramar ut som Cybermätaren i huvudsak baseras på. Dessa är *National Institute of Standards and Technology Cybersecurity Framework* (NIST CSF) [1] och *U.S. Department of Energy Cybersecurity Capability Maturity Model* (C2M2) [2] [3]. Vid utarbetande av anvisningarna utnyttjades dessutom bland annat Finlands nationella riskbedömning (2015) [4] och Säkerhetsstrategin för samhället [5].

Cybermätaren är baserad på C2M2-modell version 1.1 och utkastsversion 2.0. Cybermätaren inkluderar C2M2-modellens tio avsnitt som dessutom har översatts från engelska till finska och svenska. Dessa tio avsnitt utgör stommen i Cybermätaren. Utöver den ovan nämnda stommen har Cybersäkerhetscentret utvecklat separata delar om skydd av kritiska tjänster och om insamling av nivån på investeringar i cybersäkerhet. Cybermätaren inkluderar en av Cybersäkerhetscentret utvecklad riktgivande korsreferens med NIST CSF-modellen vilket gör det möjligt att också rapportera resultaten från Cybermätaren med indelning enligt NIST CSF-modellen.

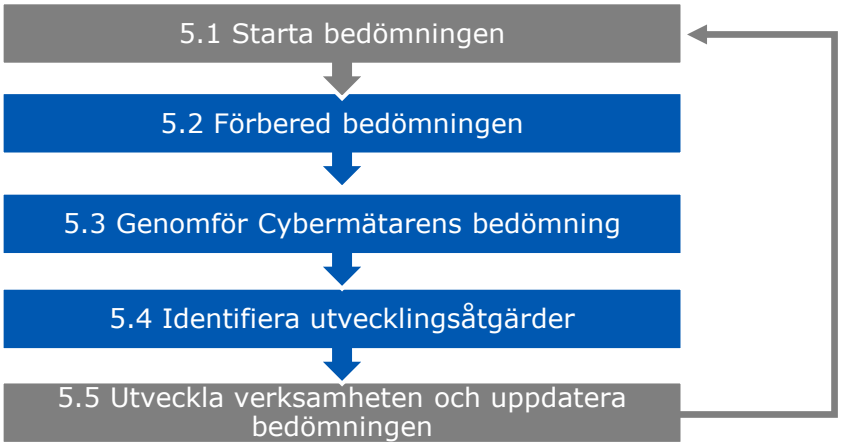
Organisationer kan om de så önskar, frivilligt och konfidentiellt, dela producerade bedömningsresultat med Cybersäkerhetscentret. Cybersäkerhetscentret kan utnyttja resultaten konfidentiellt för att utföra sina lagstadgade uppgifter. Dessutom kan centret med dessa resultat som grund utarbeta anonymiserade referens- och rekommendationsnivåer som det kan erbjuda organisationer som stöd för användningen av Cybermätaren och utvecklingen av cybersäkerheten. Referens- och rekommendationsnivåer utarbetas så att inga slutledningar kan dras på deras grund om enstaka organisationer och deras bedömningsresultat. Närmare uppgifter om delning av bedömningsresultat och referensnivåer finns på www.kybermittari.fi

2 Användning av Cybermätaren

Detta kapitel beskriver den bedömningsprocess som Cybersäkerhetscentret rekommenderar och som underlättar användningen av Cybermätaren i organisationer. Processen har utarbetats med erfarenheter från pilotkartläggningar som grund.

Det rekommenderas att Cybermätaren används som en del av verksamhetens kontinuerliga bedömnings- och utvecklingsprocess. Processen i fem steg består av start och förberedelser av bedömningen, genomförande av bedömningen samt identifiering och genomförande av utvecklingsåtgärder. När utvecklingsåtgärderna framskrider och verksamhetsmiljön ändras uppdateras bedömningen eller så genomförs en ny bedömning. Bedömningsprocessen och dess kontinuitet visas i figur 1.

Cybermätarens bedömning kan göras som en engångsföreteelse men den bästa nyttan med mätaren fås när den införs som en del av den ständiga utvecklingen av verksamheten. Dessutom rekommenderas det att bedömningen integreras till en del av annan riskhantering i organisationen och utvecklingsarbetet gällande cybersäkerhet till en del av organisationens övriga utvecklingsverksamhet.



Figur 1: Femstegsprocessen för bedömning av cybersäkerhet som underlättar användningen av Cybermätaren i organisationer.

Nedan beskrivs kortfattat varje processteg och de viktigaste deltagarna och uppgifterna i varje steg. I slutet av kapitlet finns en komprimerad minneslista över stegen och uppgifterna. Närmare anvisningar för användning av Cybermätaren finns i kapitel 4.

2.1 Starta bedömningen

Deltagare: Organisationens ledningsgrupp eller annat beslutsorgan.

Uppgift:

1. Besluta om att genomföra bedömningen och om vad som ska bedömas.
2. Utse en sponsor och en projektledare för bedömningen, dessa ansvarar för fortsatta åtgärder.

Bedömningen inleds med ett beslut om att bedömning ska göras för något visst objekt och i bestämd omfattning. Rekommendationen är att beslutet fattas i organisationens ledningsgrupp eller annat organ som fattar beslut om cybersäkerhet och riskhantering. På detta sätt uppnås tillräckligt stöd och förutsättningar för att genomföra bedömningen och för långsiktig utveckling av cybersäkerheten.

Det viktigaste beslutet gäller val av *verksamhetsdelområde som ska bedömas*. Med verksamhetsdelområde menas de tjänster eller verksamheter som är kritiska för organisationen eller samhället och som granskas i bedömningen av cybersäkerhet. Bedömningen kan omfatta organisationens hela verksamhet, men speciellt i större organisationer rekommenderas det att fokusera bedömningen bara på en kritisk tjänst eller funktion i taget. Behandling som en helhet förutsätter att de processer och de rutiner som används är tillräckligt enhetliga inom hela det delområde som bedöms. Om man vill bedöma flera separata verksamhetsområden är rekommendationen att starta en egen bedömning för var och en av dem.

Projektledaren för bedömningen kan väljas internt i organisationen eller från en extern tjänsteleverantör.

Valet påverkas av bland annat tidigare cyberkunskap, tidsanvändning och hur bedömningen är organiserad.

Det andra viktiga beslutet är att utse en *sponsor för bedömningen* samt för det praktiska genomförandet en *projektledare för bedömningen*. Projektledaren kan komma inifrån organisationen eller externt. Det rekommenderas att även dessa utses i ledningsgruppen eller annat beslutsfattande organ. Sponsorn för bedömningen bör vara en medlem i ledningsgruppen eller annan tjänsteman inom organisationen, men som projektledare för bedömningen kan även en expert från en extern tjänsteleverantör utnyttjas. Det är dessutom möjligt att helt eller delvis lägga ut bedömningen på en tjänsteleverantör.

När beslutet att genomföra en bedömning har fattats och bedömningen har fått en sponsor och en projektledare tar de ansvar för det praktiska genomförandet av bedömningen.

2.2 Förbered bedömningen

Deltagare: Sponsor och projektledare för bedömningen tillsammans.

Uppgift:

1. Göra en närmare avgränsning av det delområde i verksamheten som ska bedömas och identifiera delområdets kritiska beroenden.
2. Identifiera de experter som krävs för bedömningen.
3. Komma överens om bedömningsmetoden och tidplanen för bedömningen.

Sponsorn och projektledaren för bedömningen definierar närmare det delområde som ska bedömas och identifierar de beroenden som är kritiska för delområdet. Med kritiska beroenden avses de system, processer och informationstillgångar som behövs för att realisera de valda tjänsterna eller funktionerna. Om man i detta skede observerar utmaningar när det gäller till exempel omfattningen av bedömningen, kan beslutet om avgränsning av det delområde av verksamheten som ska bedömas övervägas på nytt i ledningsgruppen. Det finns närmare anvisningar för identifiering av delområdet av verksamheten och dess beroenden i kapitel 4.2.

Med det delområde av verksamheten som ska bedömas och dess beroenden som grund identifierar bedömningens sponsor och projektledare de experter inom organisationen som behövs för bedömningen. Experterna för nödvändig kunskap från sitt ansvarsområde till bedömningen, till exempel om organisationens verksamhet, riskhantering, informationsförvaltning eller andra processer. Lämpligt antal deltagare varierar från organisation till organisation, men i pilotkartläggningarna deltog typiskt två till fyra experter.

Avgränsningen av delområde *bör göras omsorgsfullt så att bedömningen kan genomföras inom planerad tid och resultaten kan tolkas på rätt sätt senare.*

Bedömning i workshop *har visat sig vara den mest populära*

Med bedömningens omfattning, antalet deltagare och organisationens preferenser som grund kommer bedömningens sponsor och projektledare överens om sättet att genomföra bedömningen. Rekommendationen är att använda antingen workshop- eller personalbaserad bedömning. Vid workshopbaserad bedömning kallas deltagarna samman i en eller flera bedömningsworkshopar där bedömningen görs från början till slut. Vid personalbaserad bedömning delas avsnitten ut till respektive deltagare för att fyllas i separat och projektledaren sammanställer svaren. Genomförandesättens fördelar beskrivs närmare i kapitel 4.3.

När alla ovanstående saker har bestämts, kommer bedömningens sponsor och projektledare också överens om tidplanen för bedömningen. Rekommendationen är att i förväg reservera tidpunkterna för möten i anslutning till bedömningen och de experter som deltar i bedömningen.

2.3 Genomför bedömning med Cybermätaren

Deltagare: Bedömningens projektledare, bedömningens sponsor och organisationens experter.

Uppgift: Genomföra bedömningen med valt bedömningssätt med hjälp av verktyget Cybermätaren.

Tidsåtgång: 1–2 arbetsdagar.

Projektledaren svarar för de praktiska arrangemangen kring bedömningen och för att introducera de experter inom organisationen som deltar i bedömningen i användningen av Cybermätaren. I arrangemangen ingår beroende på genomförandemetoden sammankallande till möten, utdelning av material och sammanställning av svar. För introduktionen finns Cybermätarens bruksanvisning samt annat stödmaterial.

Bedömningen utförs med hjälp av verktyget Cybermätaren. Deltagarna svarar på frågor om rutiner för cybersäkerhet och efterlevnaden i organisationens verksamhet. Verktyget styr genomförandet av bedömningen och bestämmer organisationens mognadsnivå baserat på svaren när bedömningen framskrider.

2.4 Identifiera utvecklingsåtgärder

Deltagare: Bedömningens projektledare, bedömningens sponsor, organisationens experter och ägare till utvecklingsplaner.

Uppgift:

1. Analysera bedömningens resultat.
2. Bestämma eventuell målnivå för verksamheten.
3. Identifiera och sätta prioriteter på de viktigaste utvecklingsåtgärderna.

Projektledaren svarar för sammanfattning och analys av svaren tillsammans med bedömningens sponsor, organisationens experter och ägarna till utvecklingsplanerna. De automatiska rapporter som verktyget Cybermätaren producerar stöder analys av resultaten och med hjälp av dem kan styrkorna och svagheterna i organisationens verksamhet identifieras med flera olika mätare. Om organisationen dessutom använder referensgruppernas referens- eller rekommenderade nivåer, kan rapporterna förses med information om till exempel den genomsnittliga mognadsnivån i branschen.

*Vid **bestämning av målnivån** bör man utnyttja referens-/rekommenderade nivåer, som kan begäras från Cybersäkerhetscentret.*

Den allmänna rekommendationen är att först sträva efter nivå 1 i all verksamhet.

För att identifiera lämpliga utvecklingsåtgärder rekommenderas det att alltid fastställa den målnivå för cybersäkerhet som organisationen eftersträvar. Det är inte nödvändigtvis kostnadseffektivt att sträva efter en högre mognadsnivå inom alla områden som bedöms. En tillräcklig nivå kan fastställas med till exempel uppnådda resultat, eventuella referens- och rekommenderade nivåer hos referensgrupper eller organisationens interna mål som grund. Dessa kan vara verksamhetsmässiga mål eller basera sig på till exempel risker som identifierats i riskbedömningar. För de organisationer som genomför bedömning för första gången bestäms målnivån i allmänhet först med resultaten och fynden från den första bedömningen som grund. En allmän rekommendation kan vara att alla organisationer strävar efter minst mognadsnivå 1 i sin verksamhet.

Med resultaten från bedömningen och målbilden som grund identifieras de utvecklingsåtgärder som organisationen bör genomföra för att utveckla sin verksamhet och uppnå målbilden. En utvecklingsplan utarbetas för åtgärderna, den bör utöver prioritering av åtgärder innehålla åtminstone en åtgärdsspecifik tidplan, ansvarig person och en mer detaljerad genomförandeplan. Cybersäkerhet kan inte utvecklas separat från organisationens övriga verksamhet och därför bör organisationens normala processer för verksamhetsutveckling och budgetering beaktas när utvecklingsplanen utarbetas. Dessa påverkar beslutsfattandet och tidplanen för genomförande av planen.

När utvecklingsåtgärderna är valda och tidplanerade övergår koordineringsansvaret till namngivna ägare av utvecklingsplaner.

2.5 Utveckla verksamheten och uppdatera bedömningen

Deltagare: Utvecklingsplanernas ägare, organisationens experter samt organisationens ledningsgrupp eller annat beslutsorgan.

Uppgift: Genomföra planerade utvecklingsåtgärder, uppdatera bedömningen och vid behov inleda en ny bedömningsprocess.

Användningen av Cybermätaren bör ses som en process där bedömning och genomförande av utvecklingsåtgärder sker växelvis. Mognadsnivån för cybersäkerhet kan höjas steg för steg med målet satt till den målnivå som bestämts enligt den egna riskvilligheten.

Den viktigaste uppgiften för ägarna till utvecklingsplanerna är att koordinera genomförandet av planerna och upprätthålla den övergripande bilden av hur åtgärderna framskrider. Målet är att säkerställa att beslutade åtgärder genomförs och identifiera rätt tidpunkt för att uppdatera bedömningen.

***Ombedömning** bör göras med 1–2 års intervall, beroende på organisationen och bedömningens objekt.*

Uppdaterad bedömning eller ombedömning blir aktuell när utvecklingsplanerna framskrider eller organisationens verksamhetsmiljö förändras. Nyttan med Cybermätaren blir som störst när verksamheten bedöms regelbundet på nytt och effekten av utvecklingsåtgärderna kan ses i rapporterna. Cybermätaren gör det möjligt att jämföra tidigare bedömningar, vilket underlättar uppföljningen och rapporteringen av utvecklingsåtgärdernas effekt.

Sammanfattning av bedömningsprocessen och minneslista

Nedan har samlats de centrala faserna av Cybermätarens bedömningsprocess och de viktigaste sakerna som ska beaktas i varje fas.

3 Cybermätarens bedömningsmodell

Detta kapitel beskriver Cybermätarens bedömningsmodell och dess viktigaste egenskaper. Dessa egenskaper är speciellt bedömningsmodellens struktur och beräkningsmodellen för mognadsnivå.

Cybermätaren representerar en mognadsmodell avsedd för bedömning och utveckling av förmågor inom cybersäkerhet. Med hjälp av modellen kan objektets förmågor inom cybersäkerhet bedömas och utvecklingsarbetet kan styras på fyra olika mognadsnivåer (nivå 0–3). Nivåerna visar hur systematisk och utvecklad verksamheten är, från svagare till bättre. Målet är att organisationen med hjälp av Cybermätaren bestämmer nuvarande nivå för sin verksamhet och framskrider från en nivå till nästa mot bättre och effektivare verksamhet.

Nivå 0 Verksamheten uppfyller inte grundläggande krav.

Nivå 1 Verksamheten uppfyller grundläggande krav, men kan fortfarande vara sporadisk och verksamhetens nivå kan variera från fall till fall.

Nivå 2 Verksamheten är mer avancerad och omfattande än på lägre nivå.

Hanteringen av cybersäkerheten karakteriseras dessutom av:

- Dokumenterade processer och rutiner.
- Tillräckliga resurser och kompetens.
- Definierad roll- och ansvarsfördelning.

Nivå 3 Verksamheten är avancerad och omfattande.

Hanteringen av cybersäkerheten karakteriseras dessutom av:

- Verksamheten styrs av organisationens policy (eller andra riktlinjer från ledningen).
- Verksamheten har prestandamål som följs.
- Dokumenterade processer och rutiner överensstämmer med organisationens normer och de utvecklas kontinuerligt.

3.1 Viktigaste begrepp

I samband med Cybermätaren används begrepp som det är viktigt att förstå för att kunna använda mätaren på rätt sätt och tolka resultaten. Här presenteras fyra sådana begrepp, utöver detta finns i kapitel 6 en mer omfattande ordlista över Cybermätarens begrepp och cybersäkerhetstermer.

Förmåga

Med hjälp av Cybermätaren strävar man efter att bedöma och utveckla organisationens förmågor inom cybersäkerhet. Med förmåga avses förmågan att agera på ett ändamålsenligt sätt inom ett visst delområde, och utnyttja sina kunskaper och resurser för att uppnå målen. För att förverkliga organisationers förmågor behövs i allmänhet en kombination av tre delhelheter, som är verksamhetsmodeller och processer, personal och kompetens samt information och system.

Mognadsmodell

Med mognadsmodell avses en modell där verksamheten granskas som nivåer eller steg och där man klättrar uppåt mot mer systematisk och avancerad verksamhet. För varje nivå har det ställts upp mål eller krav som den bedömda verksamheten måste uppfylla på ifrågavarande nivå. Dessa mål och nivåer representerar typiskt bästa praxis och kan till exempel följa verkställandet av någon lag eller standard. Dessutom är det karakteristiskt för mognadsmodellen att verksamheten delas in i olika avsnitt som granskas var för sig. Cybermätaren representerar en mognadsmodell där organisationens förmågor inom cybersäkerhet bedöms med hjälp av fyra olika mognadsnivåer och elva snitt som bedöms.

Delområde av verksamheten

Delområde av verksamheten är ett begrepp som används i samband med Cybermätaren och som avser de tjänster eller verksamheter som är kritiska för organisationen eller samhället och vars cybersäkerhet granskas i bedömningen. Utöver tjänster och funktioner omfattar definitionen de processer, system och informationslager som är kritiska för produktion av dessa tjänster. Identifiering och tydlig definition av delområdet av verksamheten spelar en viktig roll vid genomförande av bedömningen och utnyttjande av resultaten.

3.2 Avsnitt, mål och rutiner

Cybermätaren består av elva *avsnitt* fokuserade på bedömning av cybersäkerhet, *mål* som ställts upp för avsnitten samt *rutiner* som mäter uppnåendet av målen. Rutiner representerar typiska goda förfaringssätt inom cybersäkerhet som företag inom olika branscher följer i sin verksamhet. Varje rutin representerar ett visst krav/en viss mognadsnivå och ett visst mål. Rutinerna har grupperats enligt såväl mål som svårighetsgrad.

Avsnitt Cybermätarens elva avsnitt är (inom parentes namnet på verktygets flik):

1. Skydda kritiska tjänster (CRITICAL)
2. Riskhantering (RISK)
3. Hantering av leveranskedjor och externa beroenden (DEPENDENCIES)
4. Hantera skyddade objekt, ändringar och konfigurationer (ASSET)
5. Åtkomstkontroll och administration av åtkomsträttigheter (ACCESS)
6. Hantera hot och sårbarheter (THREAT)
7. Lägesbild (SITUATION)
8. Hantera händelser och incidenter (RESPONSE)
9. Personaladministration (WORKFORCE)
10. Cybersäkerhetsarkitektur (ARCHITECTURE)
11. Program för hantering av cybersäkerhet (PROGRAM).

Den aktuella ordningen är samtidigt också den rekommenderade ordningen för bedömning. Delarna kan också bedömas i en ordning som avviker från detta. Det rekommenderas dock att bedömningen omfattar alla avsnitt i bedömningsmodellen

så att slutresultatet blir en övergripande bild av organisationens arbete med cybersäkerhet och att eventuella dolda svagheter identifieras i bedömningen.

Mål Cybermätare innehåller 52 mål så att var och en av avsnitt innehåller tre till fem mål för cybersäkerheten.

Målen och de rutiner de innehåller representerar antingen:

- Cybersäkerhetsmål, eller
- Administrativa mål.

Mål och rutiner i anslutning till *cybersäkerhetsmål* är förfaringssätt som organisationen bör följa i sin verksamhet uttryckligen för att skydda sig mot cyberhot (jfr administrativa åtgärder, som gäller mer generella mål i anslutning till hur etablerad verksamheten är).

Mål och rutiner kopplade till *administrativa mål* mäter hur etablerad organisationens verksamhet är. De rutiner som ska bedömas är samma för varje avsnitt. Rutinerna gäller till exempel om verksamheten när det gäller aktuellt avsnitt baseras på dokumenterade processer, om resurstilldelningen är tillräcklig eller om mätbara prestationsmål används. Det bör observeras att inga administrativa mål har ställts upp på mognadsnivå 1. Med andra ord behöver inte verksamheten ännu vara etablerad eller följa formella processer för att uppnå mognadsnivå 1.

Rutiner Mognadsnivån för cybersäkerhet fastställs genom att bedöma rutiner som beskriver verksamheten. Varje avsnitt och mål i Cybermätaren består av en mängd rutiner. Rutinerna representerar typiska goda förfaringssätt inom cybersäkerhet som organisationer inom olika branscher följer i sin verksamhet. Rutinerna är ordnade enligt målen på så sätt att varje mognadsnivå representeras av en samling rutiner.

3.3 Beräkningsmodell för mognadsnivå

Cybermätarens beräkningsmodell för mognadsnivå beräknar organisationens mognadsnivå på skalan 0–3. Mognadsnivån bestäms enligt de implementerade rutinerna och hur krävande de är. Ju mer krävande rutiner som implementeras i verksamheten, desto högre är mognadsnivån för det delområde av verksamheten som bedöms.

Tekniskt sett följer beräkningen av mognadsnivå följande tre steg:

1) Implementeringen av alla rutiner.
2) Mognadsnivån för varje mål beräknas.
3) Mognadsnivån för varje avsnitt beräknas.

Fas 1: Implementeringen av rutiner bedöms genom fyra svarsalternativ.

1. **Ej implementerad** – organisationen implementerar inte beskrivna rutiner.
2. **Partiellt implementerad** – organisationen är bara i början av att implementera beskrivna rutiner eller så är verksamheten annars bristfällig i praktiken.
3. **Mestadels implementerad** – organisationen implementerar de beskrivna rutinerna åtminstone i huvudsak, även om utvecklingsarbetet ännu kan vara delvis oavslutat.
4. **Helt implementerad** – organisationen implementerar beskrivna rutiner och inga betydande utvecklingsåtgärder behövs.

För beräkningen komprimeras de fyra svarsalternativen till två alternativ. Rutinen är implementerad om:

- Implementerad = 4. Helt eller 3. Mestadels implementerad.
- Ej implementerad = 2. Partiellt eller 1. Ej implementerad.

Ansökan: för rutiner där organisationen har identifierat brister och utarbetat utvecklingsplaner för att lösa bristerna, bör svarsalternativet väljas till antingen 1 eller 2. När utvecklingsåtgärderna framskrider och blir färdiga bör bedömningen uppdateras. För rutiner där verksamheten beskrivs som ”från fall till fall” bör svarsalternativet väljas till antingen 1 eller 4. I dessa situationer ger inte möjligheten till fyra svarsalternativ ytterligare nytta. Fyra svarsalternativ används baserat på erfarenheterna från pilotkartläggningarna; till exempel visade sig alternativen ja/nej ofta otillräckliga.

Fas 2: Beräkningsmodellen fungerar på följande sätt på olika mognadsnivåer:

- På nivå 1 ska alla (100 %) av rutinerna på nivån implementeras.
- På nivå 2 ska mer än hälften (>50 %*) av rutinerna på aktuell nivå *och* alla (100 %) av rutinerna på nivå 1 implementeras.
- På nivå 3 ska mer än hälften (>50 %*) av rutinerna på aktuell nivå *och* alla (100 %) av rutinerna på nivå 2 implementeras och alla (100 %) av rutinerna på nivå 1 implementeras.

Fas 3: Mognadsnivån för avsnitten bestäms utifrån den lägsta mognadsnivån för avsnittet. Om ett avsnitt består till exempel av tre mål, vars mognadsnivåer har beräknats 1, 2 och 3, är mognadsnivån som beräknats för avsnittet den lägsta av dessa, dvs. mognadsnivå 1.

Å andra sidan betonar beräkningsmodellen övergripande riskhantering där betydelsen av verksamhetens svagaste delområde understryks. För att uppnå en viss mognadsnivå ska - beroende på nivå - antingen alla eller över hälften av rutinerna i aktuell mognadsnivå implementeras. Det är inte möjligt att gå vidare till nästa mognadsnivå innan *alla* rutiner på lägre mognadsnivåer har implementerats. Organisationen kan alltså inte uppnå högre mognadsnivåer innan dess verksamhet uppfyller kraven för en viss mognadsnivå för alla bedömda avsnitt.

***Obs!** Detta avviker från beräkningsmodellen som används i den ursprungliga C2M2-modellen där uppnående av varje nivå kräver att alla rutiner på aktuell nivå och lägre nivåer implementeras. Beräkningsmodellen i Cybermätaren har gjorts lättare för att bättre lyfta fram det utvecklingsarbete som gjorts på högre mognadsnivåer, trots att någon enstaka rutin på aktuell mognadsnivå ännu kan saknas.

Dessutom bör följande observeras om mognadsnivåerna i Cybermätarens bedömningsmodell.

Mognadsnivåerna är avsnittsspecifika. Mognadsnivån för varje avsnitt bestäms utifrån de mål och rutiner som ställs upp för avsnittet. Eftersom avsnitten inte är beroende av varandra kan företaget uppnå mycket olika mognadsnivåer inom olika avsnitt.

Mognadsnivåerna är kumulativa. För att uppnå en viss mognadsnivå ska organisationen implementera såväl alla rutiner på aktuell mognadsnivå som på alla lägre nivåer när det gäller aktuellt avsnitt eller mål. Trots avancerade eller dyra åtgärder uppnås inte en hög mognadsnivå om inte grundläggande förhållanden är klara.

Ställa upp målnivåer. Valet av en tillräcklig målnivå beror på organisation och bransch. Målen bör dock ställas avsnittsspecifikt och bör anpassas till organisationens nuvarande nivå, affärsmässiga mål, organisationens riskbedömning samt eventuella referens- eller rekommenderade nivåer inom branschen.

4 Detaljerad anvisning för bedömningens projektledare

Detta kapitel erbjuder detaljerade anvisningar för användning av Cybermätaren. Avsnittet är avsett speciellt som stöd för bedömningens projektledare och andra parter som deltar i bedömningen för att förbereda bedömningen, genomföra bedömningen och utnyttja resultaten. De följande underkapitlen omfattar nyckelpersonerna vid bedömningen, bestämning av delområde av verksamheten, sätt att genomföra bedömningen och utnyttjande av rapporterna.

4.1 Mer om nyckelpersoner och roller

Det rekommenderas att identifiera och utse nyckelpersoner för följande roller i bedömningen: bedömningens sponsor, projektledaren för bedömningen, deltagande experter inom organisationen och ägare till eventuella utvecklingsplaner.

Bedömningens sponsor skapar förutsättningarna för att genomföra bedömningen och svarar för ett lyckat genomförande tillsammans med projektledaren. Hans eller hennes uppgift är att säkerställa tillräckliga resurser och insatser för bedömningen och senare utvecklingsåtgärder. Dessutom har han eller hon en viktig roll i att engagera organisationens ledning i långsiktig utveckling av cybersäkerhet. Rollen ska alltid utses inifrån organisationen.

Projektledare svarar för genomförande av bedömningen med stöd av bedömningens sponsor. Han eller hon svarar för förberedelser inför bedömningen, praktiska arrangemang kring genomförandet och behandling av resultaten. Dessutom svarar han eller hon för att lära sig själv och övriga deltagare använda Cybermätaren och dess bedömningsverktyg. I projektledarens egenskaper betonas utöver cybersäkerhetskunskaper förmågan att organisera och tidplanera bedömningen.

Som projektledare för bedömningen kan man antingen utse en intern projektledare eller utnyttja kompetensen hos en extern tjänsteleverantör. Rollen kan också delas så att det inifrån organisationen utses en ansvarig person för bedömningen men de praktiska arrangemangen och genomförandet av bedömningen köps in externt.

- **Intern projektledare.** För rollen kan utses till exempel en informationssäkerhetschef eller annan expert på cybersäkerhet eller annan person som är insatt i ämnet.
- **Extern projektledare.** Kompetensen hos en tjänsteleverantör kan utnyttjas vid bedömningen till exempel som projektledare för bedömningen, extern expert eller vid planering av utvecklingsåtgärder.

En extern tjänsteleverantör kan rekommenderas för såväl små som stora företag. Utnyttjande av en extern expert rekommenderas framförallt för de organisationer där användningen av mognadsmodeller inte är känd sedan tidigare eller som har begränsade resurser för utveckling av cybersäkerhet. För små och medelstora företag fås nyttan speciellt i form av extern erfarenhet – för stora företag kan nyttan ligga mer på organisering och tidplanering av bedömningen.

Organisationens experter För bedömningen behövs sakkunskap om bland annat organisationens verksamhet, cybersäkerhet samt riskhantering och personaladministration. Projektledaren väljer tillsammans med sponsorn ut de deltagare som behövs för bedömningen, framförallt ur verksamhetens perspektiv. Antalet experter varierar beroende på organisationens storlek: i mindre företag kan

hela bedömningen skötas av några nyckelpersoner under det att det kan vara vettigt att kalla experter från flera olika avdelningar i större organisationer.

I tabell 1 listas viktiga experter för att svara på frågor inom olika ämnesområden. I förteckningen understryks rollerna för datasäkerhetsdirektören och -chefen, men i stället för dessa roller kan andra personer användas som har relevant ansvar i anslutning till cybersäkerhet inom det bedömda objektet.

Tabell 1. Centrala roller för ifyllnad av Cybermätarens ämnesområden.

Delområde i Cybermätaren	*Centrala roller*
CRITICAL *Skydda kritiska tjänster*	Riskhanteringschef, informationssäkerhetsdirektör och -chef, samt affärsverksamhetens representanter tillsammans
RISK *Riskhantering*	Riskhanteringschef, informationssäkerhetsdirektör och -chef
ASSET *Hantera skyddade objekt, ändringar och konfigurationer*	Informationssäkerhets- och informationsförvaltningsdirektören tillsammans (*OT tillgång: dessutom svarar affärsverksamhetens representanter för saken)
PROGRAM *Hantering av utvecklingsprogrammet för cybersäkerhet*	Informationssäkerhetsdirektör/chef eller annan person i organisationen med ansvar för cybersäkerhet.
DEPENDENCIES *Hantering av leveranskedjor och externa beroenden*	Inköpschefen, riskhanteringschefen, informationssäkerherhetsdirektören/chefen och informationsförvaltningsdirektören tillsammans
ACCESS *Åtkomstkontroll och administration av åtkomsträttigheter*	Informationssäkerherhetsdirektören/chefen och informationsförvaltningsdirektören tillsammans
RESPONSE *Hantera händelser och incidenter*	Informationssäkerhetsdirektören/chefen, informationsförvaltningsdirektören och risk-hanteringschefen tillsammans samt de represen-tanter för affärsverksamheten som sköter ärendet
ARCHITECTURE *Cybersäkerhetsarkitektur*	Informationssäkerhetsdirektören/chefen tillsammans med relevanta arkitekter
SITUATION *Lägesbild*	Informationssäkerherhetsdirektören/chefen och informationsförvaltningsdirektören tillsammans
THREAT *Hantera hot och sårbarheter*	Informationssäkerhetsdirektören och -chefen tillsammans, samt de representanter för affärsverksamheten som sköter ärendet
WORKFORCE *Personaladministration*	Informationssäkerhetsdirektören i samarbete med personaldirektören

Utvecklingsplanernas ägare Ägarna till utvecklingsplaner svarar för de utvecklingsplaner som har utarbetats med utgångspunkt i bedömningsresultaten. Deras uppgift är att koordinera utarbetandet av utvecklingsplanen, säkerställa att tillräckliga resurser söks för åtgärderna och följa genomförandet av planerna. Rollens ansvarsperson kan också vara samma person som bedömningens sponsor eller

projektledare. För utvecklingen av cybersäkerheten är det viktigt att rollen har synligt getts till en särskilt utsedd part och att han eller hon har skyldighet att rapportera framstegen till företagets ledning. Det rekommenderas att rollen utses inifrån organisationen.

4.2 Bestämning av verksamhetsdelområde som ska bedömas

Bedömningens sponsor och bedömningens projektledare bestämmer i detalj det delområde av verksamheten som ska bedömas. **Med delområde av verksamheten avses de *funktioner* och de *system, processer och informationstillgångar* som är kritiska för att producera funktionerna och som granskas i bedömningen.** Bestämningen av funktioner och deras beroenden är ett kritiskt arbetsmoment för en lyckad bedömning. En noggrann avgränsning och dokumentering gör det möjligt att genomföra bedömningen inom önskad tid, få bedömningsresultaten jämförbara och rikta senare utvecklingsåtgärder rätt.

Identifiering av kritiska funktioner

Det rekommenderas att rikta bedömningen på ***funktioner* som organisationen behöver för att producera tjänster som är kritiska för antingen det omgivande samhället eller den egna (affärs)verksamheten.** Cybermätaren riktar sig i första hand till organisationer som är kritiska för samhällets försörjningsberedskap, men modellen lämpar sig lika väl för användning av andra aktörer. I det fallet väljer man att granska till exempel funktioner som är kritiska för kontinuiteten i organisationens egen verksamhet och deras viktigaste beroenden.

Avgränsningen kan göras på många sätt, till exempel:

- Täcker **hela organisationen**, till exempel i små och medelstora företag.
- Enligt **organisationsstrukturen**, till exempel mark- eller affärsenheten.
- Enligt **funktioner,** till exempel en funktion som produceras över organisationsgränser.

Organisationen kan välja till exempel en viss funktion eller tjänst för granskning, som till exempel värmeproduktionen, vattenförsörjningen eller betalningstjänster, samt de system, processer och informationstillgångar som är kritiska för att producera dessa funktioner. Bedömningen kan också fokuseras på en viss del av organisationen, som ett affärsområde, en enhet eller ett verksamhetsland i taget. Geografisk indelning rekommenderas inte såvida den inte uppfyller någon av ovanstående beskrivningar.

Små eller medelstora aktörer kan rikta bedömningen till organisationens hela verksamhetsområde. Större aktörer kan i stället avgränsa bedömningen till att gälla till exempel en viss tjänstehelhet, affärsenhet eller en enstaka produktionsanläggning. Även om Cybermätaren lämpar sig för bedömning och utveckling av cybersäkerheten i en hel organisation, rekommenderas det att rikta granskningen speciellt i större organisationer till en kritisk funktion eller del av organisationen i taget. Behandling som en helhet förutsätter att de processer och de rutiner som används är tillräckligt enhetliga inom hela det delområde som bedöms.

Om man vill bedöma flera delområden av verksamheten samtidigt är rekommendationen att starta en egen bedömning för var och en. Då är det lättare att rikta utvecklingsåtgärder och resultat från en enskild bedömning rätt och

bedömningsprocessen förblir hanterbar. För rutiner som implementerats över hela organisationen kan samma svar utnyttjas i dessa separata bedömningar.

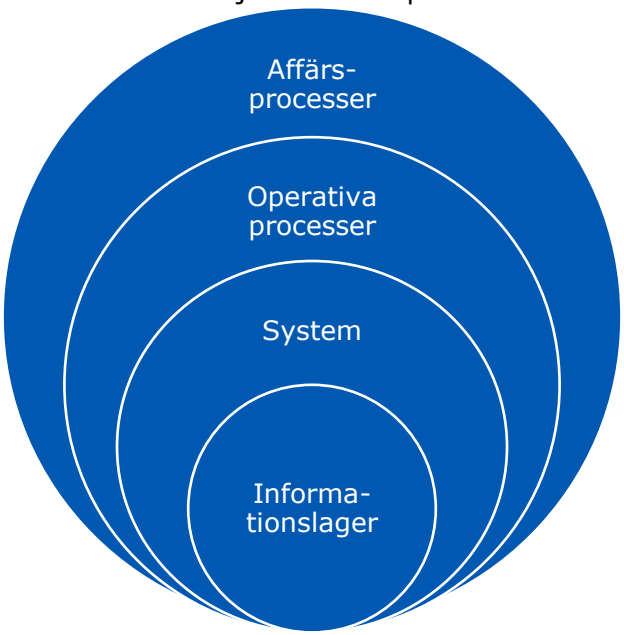
Identifiering av kritiska beroenden

Utöver att identifiera kritiska tjänster och funktioner ska de viktigaste beroendena identifieras för att bestämma bedömningens objekt. Sådana är som utgångspunkt alla i anslutning till kritiska tjänster:

- **Affärs- och operativa processer.**
- **System och delsystem**.
- **Informationslager**.

Beroenden som ska identifieras är olika slags system samt till dem knutna delsystem och informationslager. Beroenden utgörs också av anknutna operativa och affärsprocesser, inbegripet interna tjänster och kritiska tjänster som produceras av en extern leveranskedja. Av beroendena bör de viktigaste prioriteras och dessa val bör dokumenteras som en tydlig del av bedömningen.

Beroenden kan identifieras genom att börja med processerna och gå vidare till de system och den information som hänger samman med dem. Man kan också börja med den information som är kritisk för tjänster och funktioner och gå vidare därifrån mot system och processer. Figur 2 illustrerar dessa beroenden.



Figur 2: Exempel på strategier för att identifiera kritiska funktioner och deras beroenden.

Processen för identifiering av delområde av verksamheten och beroenden kan vara till exempel:

1. Organisationens kritiska funktioner eller tjänster identifieras.
2. Om det finns flera funktioner eller tjänster väljer man ut dem som man vill genomföra bedömningen för.
3. För varje kritisk funktion eller tjänst identifieras och listas anknytande kritiska beroenden, inklusive:
    a. Processer som styr kritiska funktioner och utnyttjar system som ska skyddas. Börja exempelvis med att lista affärskritiska processer och klassificera hur kritiska de är.
    b. System som producerar funktioner eller tjänster som är kritiska för samhället eller organisationen. Börja till exempel med inventarieförteckningar över system och klassificering av hur kritiska de är. Identifiera interna och externa beroenden i anslutning till systemen.

c. Information som används för produktion av kritiska funktioner eller tjänster eller i ett kritiskt systems arbete. Börja till exempel med inventarieförteckningen över information som ska skyddas.

Tjänst som är kritisk för samhället. En tjänst är kritisk för samhället om en störning i den påverkar ett stort antal kunder, ett stort geografiskt område eller om störningen har allvarliga följdverkningar. Vid bestämning av hur kritiskt något är kan Försörjningsberedskapscentralens branschdefinitioner vara till hjälp.

Tjänst som är kritisk för organisationens (affärs)verksamhet. Identifiering av tjänster som är kritiska för verksamheten kan man börja till exempel med organisationens mål eller affärsstrategins fokusområden.

4.3 Sätt att genomföra bedömningen

Projektledaren hjälper organisationen att välja det lämpligaste genomförandesättet. Bedömningen kan genomföras till exempel som en ledd workshop eller som mer självständig personlig bedömning. Avsnitt som ska bedömas kan delas ut för bedömning av olika personer. Beroende på genomförandesättet sköter projektledaren antingen de praktiska arrangemangen kring workshopen eller koordinerar genomförandet av bedömningen med experterna.

En **ledd arbetsform av workshopmodell** är en modell där projektledaren organiserar genomförandet av bedömningen genom att kalla experterna till en eller flera workshopar.

De faser vars koordinering projektledaren ansvarar för (eventuellt tillsammans med bedömningens sponsor och organisationens experter), är:

1. Utse experter och engagera dem i workshopen.
2. Inledande möte (1 h) eller inledande meddelande till de personer som deltar i bedömningen.
3. En eller flera workshopar (kan också genomföras som en serie workshopar i små grupper, t.ex. 2–3 h/workshop).
4. Sammanställning och analys av resultaten till den sista workshopen.
5. Genomgång av resultaten, identifiering av utvecklingsobjekt samt att utse personer med ansvar för utvecklingsåtgärder i den sista workshopen (2 h).

Programledaren svarar för genomförande av bedömningen, koordinering av uppgifter, tillräcklig dokumentation och att ordna workshoparna. En av projektledarens viktigaste uppgifter är att säkerställa att bedömningens syfte och omfattning förstås på samma sätt i varje diskussion och del av bedömningen. Projektledaren får under processens gång en omfattande helhetsbild av läget för cybersäkerheten i organisationen.

I en modell med grupparbete är syftet med det inledande mötet att kommunicera bedömningens syfte och genomförandeprocess till deltagarna. En mer detaljerad introduktion i de ämnesområden som ska bedömas kan göras i början av workshopen eller workshoparna. Det inledande mötet kan vid behov också ersättas med ett meddelande som skickas till alla i gruppen.

Utöver en längre workshop kan bedömningen genomföras som en serie kortare ämnesspecifika workshopar som genomförs i små grupper. I dessa kan utöver

projektledaren delta till exempel 2–4 personer innefattande experterna på ämnet och bedömningens sponsor. De diskussioner som förs i workshoparna skapar förståelse för cybersäkerheten och kan samtidigt fungera som kunskapsöverföring från en person till en större grupp.

I slutet av processen samlar projektledaren ihop resultaten och arrangerar en slutworkshop där rapporterna från verktyget gås igenom. I workshopen diskuterar man identifierade brister och kommer överens om ansvar och tidplaner för utvecklingsåtgärder och -planer. Frågor kring analys och rapportering av resultaten lämpar sig som agenda för workshopen liksom en diskussion om målnivå.

Fördelen med arbetssättet är att det som slutresultat uppstår en gemensam lägesbild och en förståelse om nuläget och om eventuell målnivå. Under bedömningen diskuteras alla ämnesområden i Cybermätaren under ledning och samtidigt delas synsätt och kunskap. Detta förebygger att cybersäkerhetskompetensen stannar hos en enda person i organisationen.

Utmaningen med grupparbetsmodellen är den tid den kräver och speciellt att hitta gemensam tid för alla. Å andra sidan är fördelen med workshopar i serieform att en mindre grupp personer närvarar i varje workshop och bara de som har en direkt koppling till ämnesområdet som behandlas. Arbetssättet kan kännas tungt för vissa roller, om en viss person förväntas delta i alla diskussioner.

Individuell bedömning är ett alternativt sätt att genomföra bedömning med Cybermätaren. I den organiserar projektledaren genomförandet av bedömningen med enskilda experter inom organisationen. Förutsättningen för en självbedömning med hög kvalitet är att den person som valts för att leda bedömningen har kunskap inom cybersäkerhet och möjlighet att sätta sig in i Cybermätaren innan projektet inleds.

Faser vars koordinering projektledaren svarar för är:

1. Utse experter och engagera dem i workshopen.
2. Inledande möte (1–2 h) för de personer som deltar i bedömningen.
3. De utsedda experterna fyller självständigt i de ämnesområden i Cybermätaren som de tilldelats, enligt överenskommen tidplan.
4. Sammanställning och analys av resultaten till workshopen.
5. Genomgång av resultaten i slutworkshopen (2–4 h) med alla personer som deltagit i ifyllandet av bedömningen.

Syftet med det inledande mötet är att ge de ansvariga personerna för olika ämnesområden en introduktion till Cybermätaren, dess användning och ämnesområdenas syfte. Efter detta fyller personerna i delområdena antingen självständigt eller i små grupper, beroende på ämnesområde. Projektledaren leder det självständiga ifyllandet och erbjuder stöd vid behov.

Resultaten lämnas till projektledaren som sammanställer dem för genomgång vid en avslutande workshop. Projektledaren försöker identifiera de viktigaste motsägelserna och bristerna i svaren som tas upp i workshopen.

I den avslutande workshopen diskuteras svaren och de kan finslipas till att vara mer jämförbara med varandra. I workshopen gås till slut igenom de rapporter som Cybermätaren producerat. I samband med analys av rapporterna kan diskussioner

föras om målnivån. I workshopen bör man komma överens om hur resultaten rapporteras vidare och hur man övergår till att utarbeta utvecklingsplaner.

Fördelarna med arbetssättet är dess effektivitet och enkelhet, framförallt när det gäller tidplanering, när endast ett kort inledande möte och en halvdags workshop för att gå igenom resultaten behöver ordnas för gruppen. Arbetssättet fungerar speciellt när det i organisationen finns tydligt identifierbara ansvarspersoner inom olika ämnesområden eller de mål dessa innehåller.

Utmaningen med självständigt arbete kan vara att ansvar för cybersäkerhet stannar hos en person och att bedömningen eventuellt ger en spretig lägesbild. Den avslutande workshopen blir arbetstyngd om de olika ämnesområdena har bedömts med mycket olika antaganden som grund. Förutsättningen för att arbetssättet ska lyckas är att det delområde av verksamheten som bedöms är tydligt avgränsat och att detta kommuniceras till alla som deltar i bedömningen.

4.4 Bedömningsresultat och rapporter

Cybermätarens automatiska rapporter stöder analysen av bedömningsresultaten och utnyttjandet av resultaten. Rapporterna kan utökas med olika slags referens- och jämförelseuppgifter och utnyttjas för att välja lämpliga målnivåer. Verktyget skapar tre rapporter av vilka var och en beskriver organisationens mognadsnivå ur lite olika perspektiv eller med olika noggrannhet. Dessa rapporter är:

1. **Ledningens mognadsrapport** är en rapport på allmän nivå som i enlighet med sitt namn är riktad till ledningen eller för användning i exempelvis extern kommunikation.

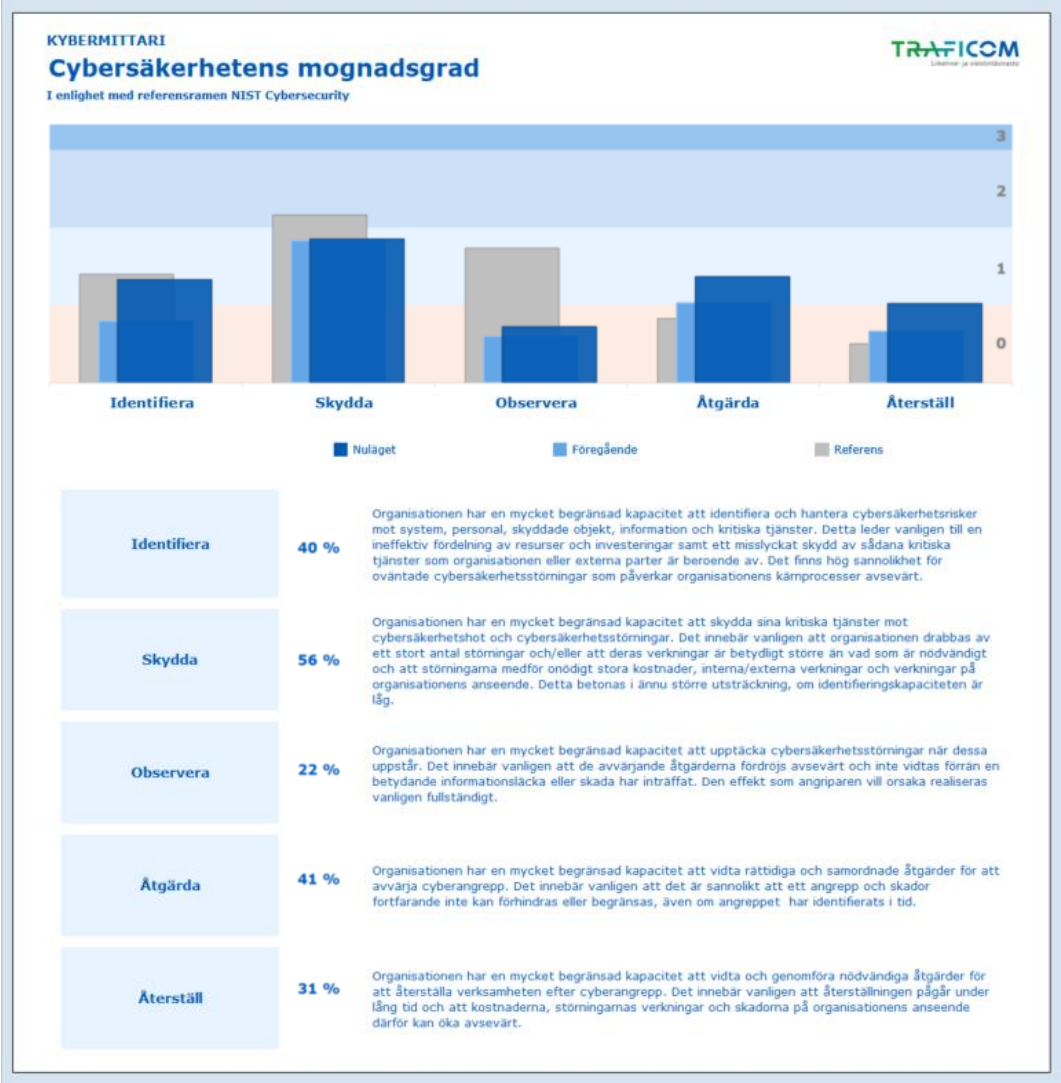
2. **Cybermätarens mognadsrapport** är en teknisk rapport som är riktad till yrkespersoner inom cybersäkerhet och riskhantering samt andra tekniska ansvarspersoner för att användas exempelvis för att bestämma organisationens nuläge och målbild samt identifiera utvecklingsåtgärder.

3. **Detaljerad mognadsrapport enligt referensramen NIST** är en annan teknisk rapport som presenterar Cybermätarens bedömningsresultat som ett slutresultat enligt NIST-modellen. Rapporten är avsedd exempelvis för organisationer som redan använder någon annan NIST-baserad bedömningsmodell eller annars vill analysera eller kommunicera resultaten enligt denna modell.

Till rapporterna kan läggas referens- och jämförelseuppgifter, till exempel resultaten från den föregående bedömningen i organisationen eller branschens genomsnittliga mognadsresultat. Samma egenskap kan alternativt utnyttjas till exempel för att visualisera organisationens målnivå.

Ledningens mognadsrapport

Ledningens mognadsrapport är speciellt avsedd för rapportering av bedömningsresultaten till organisationens ledning samt för att stöda organisationens interna och externa kommunikation.



Figur 3: Cybermätarens mognadsrapport riktad till ledningen, baserad på NIST-modellens fem avsnitt; identifiering, skyddsåtgärder, detektionsförmåga, respons och återställning.

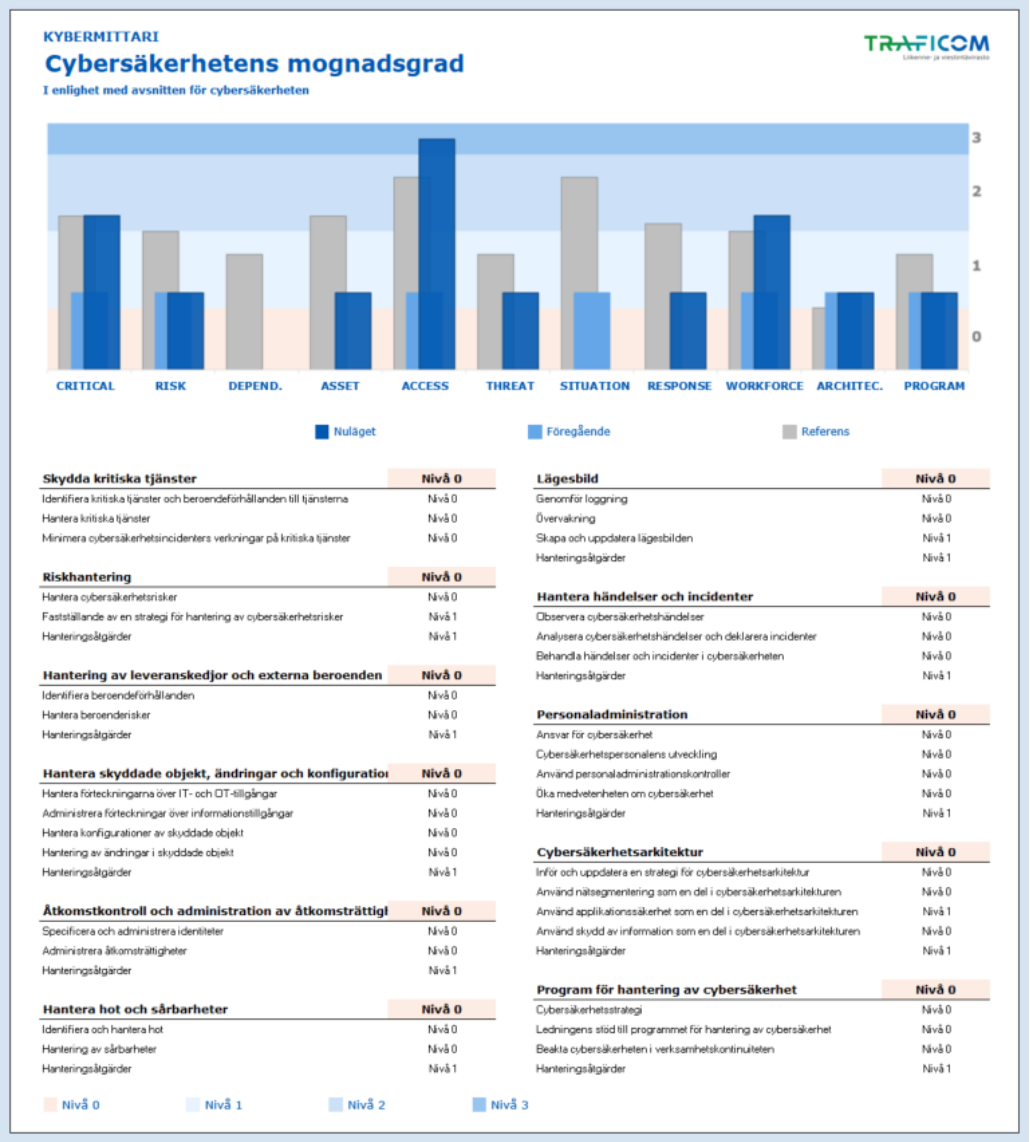
Bedömningsresultaten presenteras enligt NIST-modellens fem avsnitt (identifiering, skyddsåtgärder, detektionsförmåga, respons och återställning). Mognadsnivåerna visas med de av Cybermätaren definierade mognadsnivåerna från noll till tre.

Mognadsmodell och korskoppling. Mognadsnivåerna bestäms utifrån de rutiner som genomförts med Cybermätaren. Rutinerna har först i tillämpliga delar korskopplats med rutinerna i NIST-referensramen. Mognadsnivån för alla fem förmågor beräknas sedan enligt hur stor andel av rutinerna som har implementerats: nivå 0 betyder att under 30 % av rutinerna som syftar till förmågor har implementerats (nivå 1 under 60 %, nivå 2 under 90 % och nivå tre över 90 %).

Det bör observeras att NIST-modellen i sig inte inkluderar någon mognadsmodell. Korsreferenserna finns dokumenterade i Cybermätaren.

Cybermätarens mognadsrapport

Cybermätarens mognadsrapport är en detaljerad rapport i Cybermätaren och avsedd för analys och rapportering av bedömningsresultaten samt ledning av internt utvecklingsarbete. Rapporten riktar sig speciellt till organisationens specialist er inom cybersäkerhet och riskhantering samt övriga tekniska ansvarspersoner.



Figur 4: Cybermätarens mognadsrapport för cybersäkerhet är riktad till organisationens experter för analys av resultaten och ledning av utvecklingsarbetet.

För varje delområde som bedöms visar mognadsrapporten organisationens mognadsnivå inom cybersäkerhet som erhållits som resultat av bedömningen. Mognadsnivåerna visas på av Cybermätaren definierade mognadsnivåer från noll till tre.

Mognadsmodell. Beräkningsmodell för mognadsnivåer följer Cybermätarens beräkningsmodell som beskrivs i kapitel 3.3. Det bör observeras att Cybermätaren använder en generösare bedömning på mognadsnivåerna 2 och 3 jämfört med poängsättningen i C2M2-modellen. Det är möjligt att uppnå nivån om minst 50 % av rutinerna för nivån i fråga uppfyller kraven för varje mål. Även detta beskrivs närmare i kapitel 3.3.

Detaljerad mognadsrapport enligt NIST-referensramen Mognadsrapporten enligt NIST-referensramen är avsedd för mer detaljerad analys av bedömningsresultat och som stöd för planering av utvecklingsåtgärder. Den riktar sig speciellt till organisationens specialister inom cybersäkerhet och riskhantering samt övriga tekniska ansvarspersoner. Rapporten kan utnyttjas speciellt av de organisationer som redan tidigare använder någon bedömningsmodell som grundar sig på NIST-referensramen.

KYBERMITTARI

Detaljerad NIST Cybersecurity Framework Core-rapport

Baserad på en riktgivande korskoppling mellan C2M2 och NIST

NIST Cybersecurity Framework Core						Implementation of C2M2 Practices							
Function	ID	Category	Description	ID	Subcategory	Total implemented	# of controls	Maturity level 1		Maturity level 2		Maturity level 3	
Identify	ID.AM	Asset Management	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	ID.AM-1	Physical devices and systems within the organization are inventoried	50 %	4	100 %	1	0 %	1	50 %	2
				ID.AM-2	Software platforms and applications within the organization are inventoried	50 %	4	100 %	1	0 %	1	50 %	2
				ID.AM-3	Organizational communication and data flows are mapped	25 %	4	0 %	0	0 %	1	33 %	3
				ID.AM-4	External information systems are catalogued	20 %	5	100 %	1	0 %	3	0 %	1
				ID.AM-5	Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	29 %	7	100 %	2	0 %	4	0 %	1
				ID.AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	75 %	4	100 %	2	50 %	2	0 %	0
	ID.BE	Business Environment	The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	ID.BE-1	The organization's role in the supply chain is identified and communicated	0 %	5	0 %	1	0 %	3	0 %	1
				ID.BE-2	The organization's place in critical infrastructure and its industry sector is identified and communicated	17 %	6	0 %	1	25 %	4	0 %	1
				ID.BE-3	Priorities for organizational mission, objectives, and activities are established and communicated	0 %	1	0 %	0	0 %	1	0 %	0
				ID.BE-4	Dependencies and critical functions for delivery of critical services are established	24 %	17	100 %	3	0 %	7	14 %	7
				ID.BE-5	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	20 %	5	100 %	1	0 %	4	0 %	0
	ID.GV	Governance	The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-1	Organizational cybersecurity policy is established and communicated	0 %	3	0 %	0	0 %	1	0 %	2
				ID.GV-2	Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	67 %	6	100 %	2	100 %	2	0 %	2
				ID.GV-3	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	0 %	2	0 %	0	0 %	1	0 %	1
				ID.GV-4	Governance and risk management processes address cybersecurity risks	50 %	6	100 %	2	0 %	1	33 %	3
	ID.RA	Risk Assessment	The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-1	Asset vulnerabilities are identified and documented	67 %	12	100 %	4	40 %	5	67 %	3
				ID.RA-2	Cyber threat intelligence is received from information sharing forums and sources	71 %	7	100 %	5	0 %	1	0 %	1
				ID.RA-3	Threats, both internal and external, are identified and documented	71 %	7	100 %	2	50 %	4	100 %	1
				ID.RA-4	Potential business impacts and likelihoods are identified	25 %	4	0 %	0	25 %	4	0 %	0
				ID.RA-5	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	40 %	5	0 %	0	50 %	2	33 %	3
				ID.RA-6	Risk responses are identified and prioritized	50 %	6	0 %	0	50 %	4	50 %	2
	ID.RM	Risk Management Strategy	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	ID.RM-1	Risk management processes are established, managed, and agreed to by organizational stakeholders	63 %	19	100 %	3	78 %	9	29 %	7
				ID.RM-2	Organizational risk tolerance is determined and clearly expressed	50 %	2	0 %	0	0 %	1	100 %	1
				ID.RM-3	The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	0 %	1	0 %	0	0 %	1	0 %	0
	ID.SC	Supply Chain Risk Management	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	ID.SC-1	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	25 %	4	50 %	2	0 %	1	0 %	1
				ID.SC-2	Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	13 %	8	50 %	2	0 %	4	0 %	2
				ID.SC-3	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	44 %	9	100 %	1	60 %	5	0 %	3
				ID.SC-4	Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	0 %	3	0 %	0	0 %	1	0 %	2

Figur 5: Cybermätarens detaljerade rapport enligt NIST-referensramen.

Korskoppling. De procent och siffror som finns i rapporten baserar sig på implementerade rutiner i Cybermätaren. Rutinerna har först i tillämpliga delar korskopplats med rutinerna i NIST-referensramen. Procentandelarna beräknas genom att jämföra de implementerade rutinerna för varje punkt med alla för den aktuella punkten tillämpliga rutiner.

Det bör observeras att korskopplingen endast är riktgivande, eftersom NIST-referensramen varken omfattar någon mognadsmodell eller täcker alla avsnitt i Cybermätaren. Korskopplingen mellan rutinerna i Cybermätaren och rutinerna i NIST-referensramen finns i bedömningsverktyget Cybermätaren.

Obs! Om ”maturity level” visas i vitt betyder det att aktuell mognadsnivå inte är definierad i modellen.

Punkterna ”N/A” betyder att motsvarande punkt inte finns i Cybermätaren

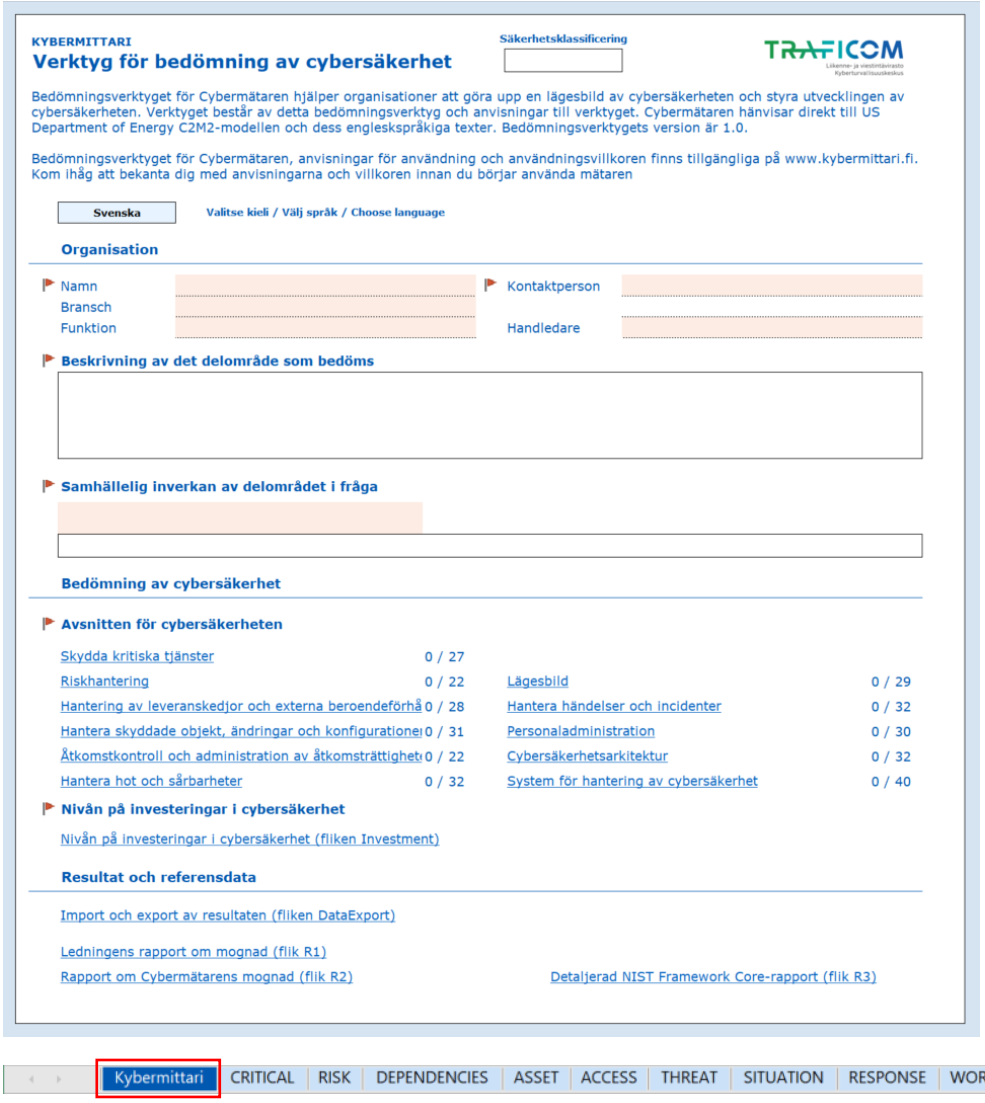
5 Detaljerad ifyllnadsanvisning för bedömningsverktyget Cybermätaren

Detta kapitel erbjuder detaljerade anvisningar för användning av Cybermätaren och inmatning av uppgifter. Verktyget stöder genomförandet av bedömningen och styr bedömningsprocessen. Anvisningarna är avsedda speciellt som stöd för projektledaren och andra parter som deltar i bedömningen för effektiv användning av verktyget.

5.1 Fliken Cybermätaren (Kybermittari)

På fliken **Cybermätaren (Kybermittari)** finns en sammanfattning av bedömningsprocessen som består av följande:

- Språkval (finska, svenska, engelska).
- Säkerhetsklassificering av information.
- Organisation och delområde av verksamheten.
- Resultat och referensdata.



Figur 6: Den första fliken i bedömningsverktyget Cybermätaren med en sammanfattning av den organisation som bedöms och bedömningens status.

Denna flik visar en sammanfattning av Cybermätarens bedömning omfattande en beskrivning av den organisation och det delområde av verksamheten som bedöms, elva bedömda avsnitt samt de rapporter som skapas som resultat av bedömningen. På fliken visas också läget för en ofullbordad bedömning och det finns direkta länkar till verktygets olika avsnitt.

Verktyget kan användas på finska, svenska eller engelska. Verktygets texter byts dynamiskt för att motsvara det språk som valts, med undantag av alternativen för rullgardinsmenyer (t.ex. översättningar av svarsalternativen för bedömningsavsnitt).

Klassificering av information kan dokumenteras under punkten Klassificering av information. Klassificeringen utförs i allmänhet av den organisation som bedöms under bedömningen eller som avslutning av bedömningen. Punkten klassificering av information kan också användas till exempel av myndigheter när de klassificerar handlingar som överlåtits till dem.

Organisation och delområde av verksamheten När det gäller organisationen och delområdet av verksamheten så dokumenteras den organisation som bedöms och det beskrivs kortfattat vad bedömningen fokuseras på. Dokumentationen består av följande fält:

- Organisationens namn, bransch och funktion.
- Kontaktperson och projektledare för bedömningen.
- Beskrivning av det delområde av verksamheten som bedöms.
- En bedömning av delområdets samhällsbetydelse.

Som namn på aktören antecknas det officiella namnet på företaget, organisationen eller annan aktör. Bransch och funktion väljs ur en rullgardinsmeny som visar de branscher och delområden som Försörjningsberedskapscentralen definierat som kritiska för försörjningsberedskapen (grundat på bransch*pooler)*. Alternativen beskrivs i tabell 2. Organisationer som inte identifierar sig som försörjningsberedskapskritiska aktörer bör välja alternativet ”ej fbk bransch” i båda fälten. Avsikten med menyerna är att stöda senare statistikföring och klassificering, menyerna har ingen inverkan på själva bedömningen.

Kontaktperson och/eller projektledare dokumenteras för eventuella preciseringar och senare användning.

Beskrivningen av delområdet av verksamheten dokumenteras för analys och jämförelse av resultaten. Detta är särskilt viktigt för att senare veta vilka funktioner, system, processer och informationstillgångar bedömningen gällde.

Tabell 2. Cybermätarens definitioner av försörjningsberedskapskritiska branscher och delområde av verksamheten som används för statistikföring.

Kritisk bransch	Kritiskt delområde av verksamheten
Livsmedelsförsörjning	*Primärproduktion* *Livsmedelsindustri* *Handel och distribution*
Finansbranschen	*Finansiell service* *Försäkringsbranschen*
Kritisk industriproduktion	*Kemi* *Skog* *MIL* *Plast och gummi* *Bygg* *Teknik*
Logistik	*Lufttransporter* *Landtransporter* *Sjötransporter*
Hälso- och sjukvård	*Hälso- och sjukvård* *Vattenförsörjning*
Informationssamhället	*Digital* *Media*
Ej försörjningsberedskaps-kritisk bransch	*Verksamhet som gäller annat än försörjningsberedskapskritisk verksamhet*

Bedömning av delområdets samhällsbetydelse gäller de organisationer som producerar *tjänster som är kritiska för samhället*. Effekterna beskrivs genom tre alternativa val och en preciserande beskrivning i fri form. Alternativ som kan väljas är:

1. **Små systemiska verkningar:** Verkningarna drabbar endast organisationen själv eller ett litet antal samarbetspartner och/eller kundorganisationer, eller verkningarna begränsas till mindre än 50 000 medborgare.

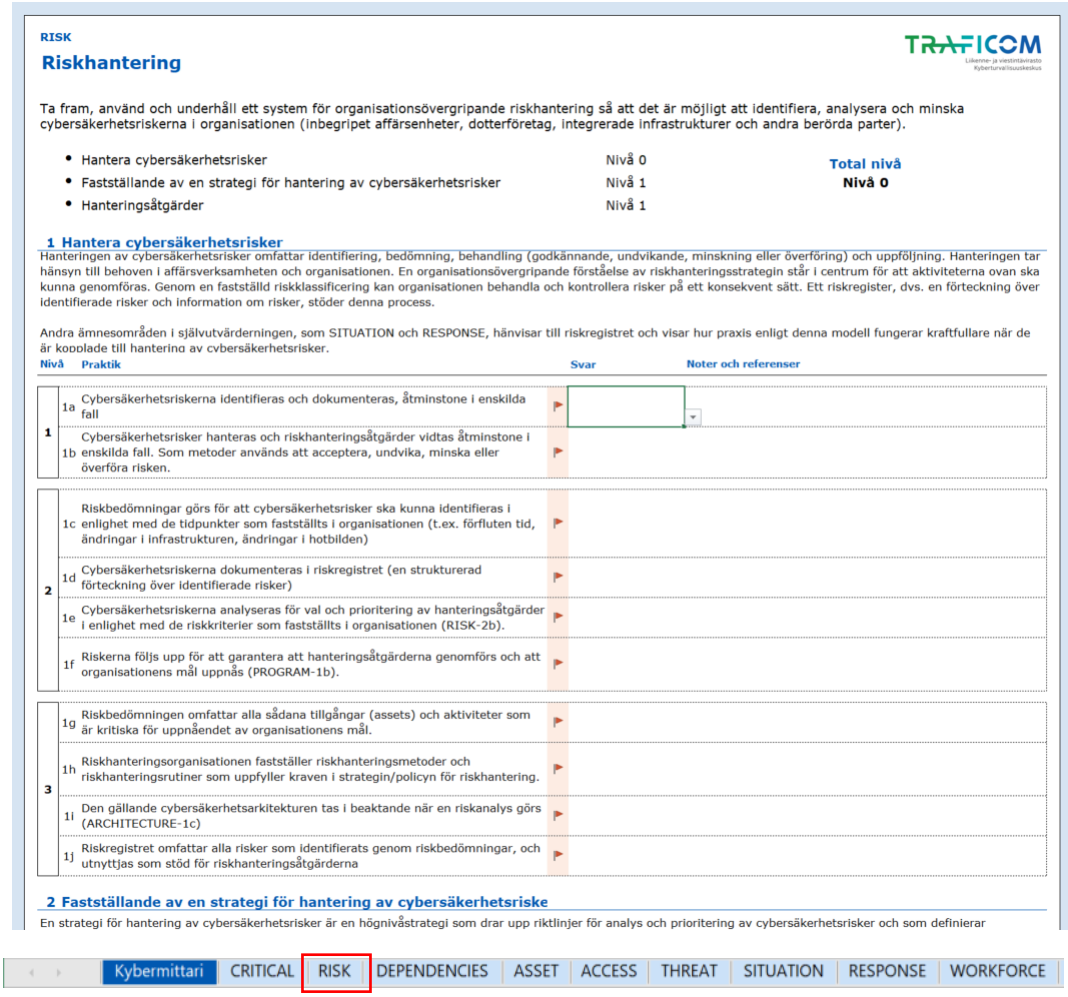
2. **Stora systemiska verkningar:** Verksamheten försvåras för ett stort antal samarbetspartner och/eller kundorganisationer, eller livet försvåras eller skador orsakas för mer än 50 000 medborgare.

3. **Förlamande systemiska verkningar:** Förlamar de grundläggande verksamheterna i samhället, eller mer än 100 000 medborgare drabbas av skada.

När organisationen och det delområde av verksamheten som ska bedömas har dokumenterats kan de avsnittsspecifika flikarna fyllas i.

5.2 Avsnittsspecifika flikar

Var och en av de **elva avsnitten av cybersäkerhet** finns på sin egen flik. Fliken Cybermätaren innehåller direkta länkar samt en lägesbild för varje avsnitt.



Figur 7: En avsnittsspecifik flik i bedömningsverktyget Cybermätaren (elva flikar i verktyget, en för varje avsnitt som ska bedömas).

Varje flik innehåller följande punkter:

- Avsnittets namn, en kort beskrivning samt en sammanfattning av uppställda mål och den mognadsnivå som beräknats för dem i nuläget.
- Målens namn, beskrivningar samt de rutiner som åsatts målen.
- Rutinernas koder och beskrivningar grupperade i stigande ordning enligt mognadsnivåerna. Dessutom för varje rutin:
    - Svarsalternativ 1–4 (flerval).
    - Plats för kommentarer och hänvisningar (fritt textfält).

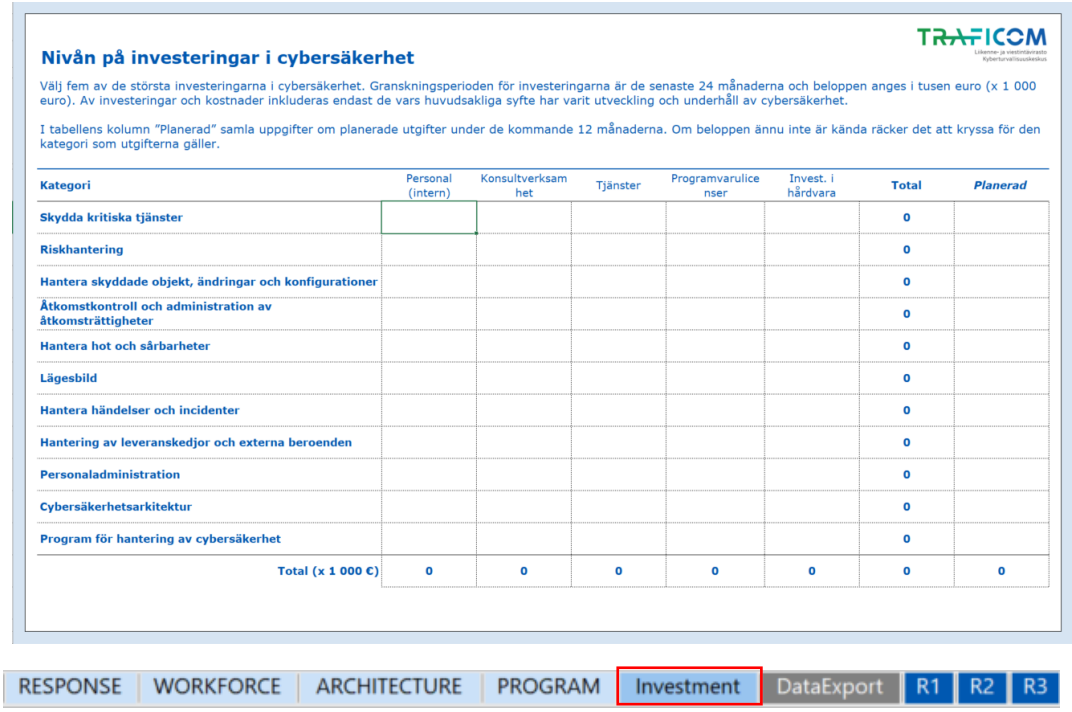
Användning: bedömningen sker genom att bedöma de rutiner som presenteras och för varje rutin fylla i det svarsalternativ som passar bäst. Kommentarer är frivilliga. Med de svar som lämnats beräknar verktyget automatiskt mognadsnivån för aktuellt mål, avsnitt och för hela organisationen allt efter att verktyget fylls i.

Avsnitten kan bedömas i vilken ordning som helst, men det rekommenderas att börja med avsnittet ”Skydda kritiska tjänster”. Detta avsnitt ger en god grund för förståelse av senare avsnitt.

När alla avsnitt i bedömningen har fyllts i kan man gå vidare och bedöma investeringsnivån och granska de bedömningsresultat som modellen producerat.

5.3 Fliken Investeringar

Nivån på investeringar i cybersäkerhet återfinns på en egen flik. Avsikten med denna flik är att bedöma storleken på de investeringar och kostnader som läggs ned på cybersäkerhet och kategorisera dem enligt de avsnitt som bedöms med Cybermätaren. Detta gör det möjligt att analysera effekten av investeringarna när den mognadsnivå som uppnåtts inom varje avsnitt i slutet av bedömningen jämförs med de investeringar som gjorts.



Nivån på investeringar i cybersäkerhet

Välj fem av de största investeringarna i cybersäkerhet. Granskningsperioden för investeringarna är de senaste 24 månaderna och beloppen anges i tusen euro (x 1 000 euro). Av investeringar och kostnader inkluderas endast de vars huvudsakliga syfte har varit utveckling och underhåll av cybersäkerhet.

I tabellens kolumn "Planerad" samla uppgifter om planerade utgifter under de kommande 12 månaderna. Om beloppen ännu inte är kända räcker det att kryssa för den kategori som utgifterna gäller.

Kategori	Personal (intern)	Konsultverksamhet	Tjänster	Programvarulicenser	Invest. i hårdvara	Total	*Planerad*
Skydda kritiska tjänster						0	
Riskhantering						0	
Hantera skyddade objekt, ändringar och konfigurationer						0	
Åtkomstkontroll och administration av åtkomsträttigheter						0	
Hantera hot och sårbarheter						0	
Lägesbild						0	
Hantera händelser och incidenter						0	
Hantering av leveranskedjor och externa beroenden						0	
Personaladministration						0	
Cybersäkerhetsarkitektur						0	
Program för hantering av cybersäkerhet						0	
Total (x 1 000 €)	0	0	0	0	0	0	0

RESPONSE | WORKFORCE | ARCHITECTURE | PROGRAM | Investment | DataExport | R1 | R2 | R3

Figur 8: Fliken Investeringar i cybersäkerhet i Cybermätaren som samlar uppgifter om investeringar i varje avsnitt och deras slag.

Användning: När tabellen fylls i ska följande observeras:

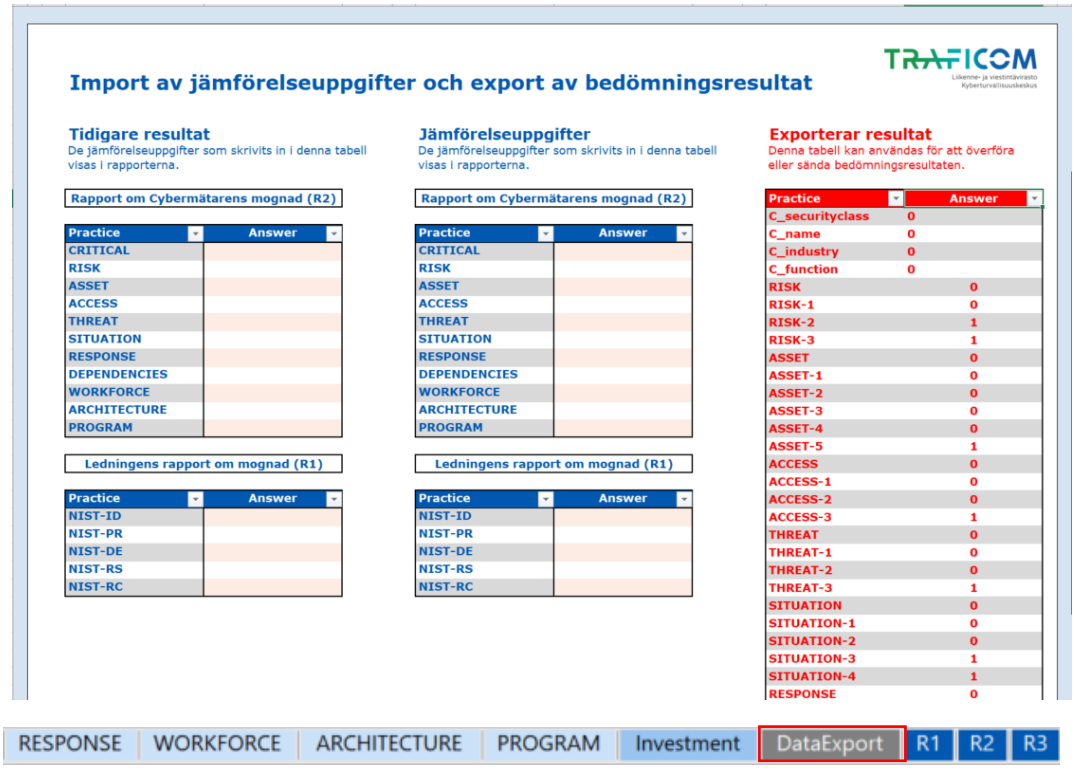
- Granskningsperioden för investeringarna är de senaste 24 månaderna.
- Beloppen anges i tusen euro (x 1 000 euro).
- Av investeringar och kostnader inkluderas endast de vars huvudsakliga syfte har varit utveckling och underhåll av cybersäkerhet. Förmågor och funktionaliteter i anslutning till cybersäkerhet, som följer med investeringar eller kostnader av någon annan anledning tas inte med.
- Det rekommenderas att avgränsa granskningen till exempelvis de 5–10 största utgiftsposterna.

I tabellens kolumn "Planerad" är tanken att samla uppgifter om planerade utgifter under de kommande 12 månaderna. Inkludera endast de utgifter som är godkända eller som har hunnit så långt i processen att ett godkännande verkar sannolikt. Om beloppen ännu inte är kända räcker det att kryssa för den kategori som utgifterna gäller. Ifyllandet underlättas om man först går igenom mognadsmodellens avsnitt så att man vet vad varje rad i kostnadstabellen innehåller.

5.4 Rapporter och jämförelseuppgifter

Cybermätarens bedömningsverktyg skapar tre automatiska rapporter med bedömningen som grund. Dessutom stöder verktyget utökning av rapporterna med externa jämförelseuppgifter och export av bedömningsresultaten i xml-format.

Jämförelseuppgifter. De rapporter som bedömningsverktyget skapar kan utökas genom att lägga till jämförelseuppgifter via fliken Resultat. Uppgifterna överförs automatiskt till de rapporter som verktyget skapar.



Figur 9: Fliken Resultat i Cybermätaren där man med hjälp av färdiga tabeller kan antingen exportera/spara resultat från Cybermätaren eller utöka de automatiska rapporterna.

Användning: i de angivna fälten kan önskade jämförelsevärden kopieras eller skrivas in. Värden som skrivits in i fälten syns i de automatgenererade rapporterna.

På fliken Resultat finns plats för två uppsättningar jämförelseresultat. Platserna har getts namnet ”Tidigare resultat” och ”Jämförelseresultat”, men organisationen kan utnyttja platserna på önskat sätt.

Export av bedömningsresultat. De bedömningsresultat som bedömningsverktyget skapar kan överföras från verktyget i en annan form, till exempel för lagring eller sändning. I de överförda överföringsresultaten ingår

- Grundläggande uppgifter om organisationen så att resultaten kan placeras och tolkas rätt senare.
- Numeriska resultat för varje avsnitt, mål och rutin, men inte kommentarer eller interna hänvisningar.
- Numeriska värden över investeringsnivåerna gällande cybersäkerhet.

De kommentarer, hänvisningar och personuppgifter som organisationen fyllt i ingår inte i överföringen av bedömningsresultat.

På fliken Resultat finns en färdig tabell över bedömningsresultaten. Tabellen uppdateras automatiskt enligt de svar som ges i bedömningen.

Användning: bedömningsresultaten kan överföras ur tabellen antingen genom att exportera resultaten ur verktyget i xml-format eller genom att klippa ut resultaten och klistra in dem i ett annat verktyg.

Obs! Om tabellens värden redigeras eller skrivs över är det inte säkert att bedömningsresultaten längre uppdateras som tänkt.

Automatiska rapporter. Bedömningsverktyget skapar tre automatiskt uppdaterade rapporter med de svar som lämnats och eventuella jämförelseuppgifter som grund.

- Cybermätarens mognadsrapport (flik R1).
- Ledningens mognadsrapport (flik R2).
- Detaljerad mognadsrapport enligt NIST-referensramen (flik R3).

Användning: rapporternas uppgifter läses från den dolda fliken *Data* (när det gäller bedömningsresultat) och fliken *Resultat* (när det gäller jämförelseuppgifter), från ovannämnda platser. Rapporterna uppdateras automatiskt från de svar som lämnas på de avsnittsspecifika flikarna och de jämförelseuppgifter som skrivs in.

6 Ordlista

De viktigaste termerna i Cybermätaren har samlats till en separat ordlista. Syftet med detta avsnitt är inte att tillhandahålla en omfattande ordlista för cybersäkerhet och därför kan det saknas termer som behöver förstås för att utarbeta bedömningen i Cybermätaren. Av denna orsak rekommenderas organisationerna att utnyttja de officiella dokumenten Ordlista om cybersäkerhet (TSK 52) och Ordlista om övergripande säkerhet (TSK 50) som Terminologicentralen publicerat. Ordlistorna är tillgängliga på finska, svenska och engelska från Terminologicentralens webbplats under Publikationer.

Cybermiljö, *”Cyber environment”*	En helhet bestående av ett eller flera digitala informationssystem där organisationens informationsbehandling sker. En organisations cybermiljö bildas av tekniska och teknologiska val, branschens särdrag samt kopplingar till externa intressentgrupper som myndigheter, avtalsparter och kunder.
Cybersäkerhet, *”Cyber security”*	En målbild där man kan lita på cybermiljön och där dess funktion tryggas. Cybersäkerhet skiljer sig från traditionell informationssäkerhet i det att det är en bredare helhet där målet är att också kontrollera hot mot den fysiska säkerheten.
Cyberhot, *”Cyber threat”*	En skadlig händelse eller utveckling som eventuellt kan ske och som riktar sig mot cybermiljön och som om den realiseras äventyrar en funktion som är beroende av den. Ett cyberhot kan utgöra en cybersäkerhetsrisk för organisationen. Ett exempel på ett cyberhot kan vara en fjärrstyrningsförbindelse som en extern angripare utnyttjar för att komma åt organisationens informationssystem. Det om fjärrstyrningsförbindelsen utgör en risk för organisationen beror på de informationssäkerhetskontroller som används och om det är möjligt att via förbindelsen äventyra en funktion eller uppgift som är kritisk för organisationens affärsverksamhet.
Cybersäkerhetsrisk, *”Cyber security risk”*	En helhet som förenar negativ inverkan från cybermiljön, cyberhot och cybersäkerheten på organisationens förmåga att agera. Exempel på cyberrisk är en händelsekedja där en motiverad hotaktör utnyttjar sårbarheten i organisationens verksamhet för att genomföra en skadlig åtgärd, som åstadkommer skada och äventyrar organisationens kritiska tillgångar som information eller produktionsprocessen.

Hantering av cybersäkerhetsrisker, *”Cyber security risk management”*	En förebyggande process med vars hjälp man förbereder sig för cybersäkerhetshot. Vid hantering av cybersäkerhetsrisker identifieras, bedöms och hanteras risker och de rapporteras och följs upp regelbundet.
System för hantering av cybersäkerhet, *”Cyber Security Management System”*	Samarbete mellan olika funktioner i en organisation för att hantera cybersäkerhetsrisker på ett systematiskt sätt. Hanteringsmodellen är organisationens beskrivning av hur den hanterar de olika delområdena av cybersäkerhet. Den består av policyer, anvisningar och processer samt roller, ansvar och mätare som bestämts för dem.
Ämnesområde inom cybersäkerhet (i Cybermätaren)	I Cybermätarens kontext avses med ämnesområden inom cybersäkerhet de tio helheter som förmågan inom cybersäkerhet bedöms mot.
Mål (i Cybermätaren)	Med mål avses i Cybermätarens kontext en till ämnesområde knuten helhet som förmågan inom ämnesområdet bedöms mot.
Rutin (i Cybermätaren)	Med rutiner avses i Cybermätarens kontext påståenden som är grupperade under målen i cybersäkerhetens ämnesområden. I Cybermätaren bedömer organisationen hur rutinerna implementeras i den egna verksamheten med hjälp av skalan med fyra steg, och med resultaten som grund bestäms ämnesområde och målspecifik mognad.
Resiliens	Organisationens motståndskraft mot kriser eller kristålighet eller förmåga att upprätthålla funktion under föränderliga förhållanden samt beredskap att möta störningar och kriser och återgå efter sådana.
Skyddade objekt *”Asset”*	Organisationens fysiska tillgång eller informationstillgång som har värde för verksamheten. Till exempel kunduppgifter, inställningsvärden för produktionssystem eller produktionsutrustning.
Inventarieförteckning, *”Inventory of assets”*	Förteckning över skyddade objekt i företaget. Inventarieförteckningen innehåller uppgifter om till exempel företagets skyddade informationstillgångar, apparater och deras konfigurationer, som företagets arbetsstationer med program- och datauppgifter, datanätets struktur, IPR, licenser, personuppgifter,

	övervakningssystem för fysiska lokaler och ritningar över lokaler.
Standardiserade grundinställningar, *"Configuration baseline"*	Standardiserade grundinställningar är inställningar som är definierade och dokumenterade så att processen på ett säkert sätt kan återställas till dem efter en störning.
Cybermätaren	Cybermätaren är ett verktyg som tagits fram av Traficoms Cybersäkerhetscenter och Försörjningsberedskapscentralen och med vars hjälp en organisation kan bedöma mognadsnivån för cybersäkerhet som bedömning.
Lägesbild *"Situational awareness"*	Organisationens kunskap om i vilket läge organisationens mognad inom cybersäkerhet befinner sig. En god lägesbild består av förmåga att samla, förstå och analysera information samt reagera på hot i realtid. En del i att skapa en lägesbild utgörs av organisationens förståelse av vilka delområden av cybersäkerhet som är under kontroll och i vilka det finns utmaningar och förbättringspotential.
Traffic Light Protocol-klassificeringen (TLP)	TLP-standarden är ett regelverk som utarbetats för delning och behandling av information och som används för att kommunicera den överlåtande partens önskemål gällande behandling och vidare delning av informationen. TLP-klassificeringen består av en färgkodning i fyra steg som visar hur informationen får användas i organisationen och delas vidare. Cybermätaren har en integrerad klassificering av information baserad på TLP-standarden.
IT-system	Informationstekniskt system
OT-system	Med operativ teknik (OT) menas allmänt informations- och kommunikationssystem som används för att övervaka och styra industriella eller fysiska apparater, processer eller händelser. Traditionellt har man med termen OT uttryckligen syftat på industriella styrsystem och med termen har man försökt skilja på termerna OT och IT (informationsteknik) som syftar på traditionella informations- och kommunikationssystem. I samband med Cybermätaren omfattar termen OT utöver traditionella industriella styranordningar även andra anordningar som kan jämföras med sådana och som antingen är kopplade till den fysiska världen eller annars

	uppfyller de typiska utmaningarna för OT-anordningar. Sådana anordningar kan vara till exempel vårdapparatur inom hälso- och sjukvården, terminal- eller automatutrustningar i finansbranschen, lyft-, transport- och andra automationsanordningar inom byggindustri eller logistik, eller styranordningar för uppvärmning, ventilation eller passersystem i fastighetsautomation. Ur cybersäkerhetsperspektiv är OT-system och -anordningar ofta förenade med karakteristiska utmaningar. OT-systemen är i ökande grad anslutna till nätet men hamnar ofta utanför IT-övervakningen, de kan inte uppdateras eller så är de inte alls kända.
NIST (National Institute of Standards and Technology)	NIST är en amerikansk myndighet under handelsministeriet med uppgift att utveckla och främja mätteknik, standarder och teknik. NIST producerar standarder och bästa praxis i anslutning till cybersäkerhet och integritetsskydd som stöder organisationers förmågor inom cybersäkerhet.
C2M2 (Cybersecurity Capability Maturity Model)	En mognadsmodell för förmåga inom cybersäkerhet som underhålls av USA:s energimyndighet. C2M2 stöder organisationer i att observera och hantera utmaningar inom cybersäkerhet samt fokusera och implementera rutiner. C2M2 är en av de referensramar som använts som grund i Cybermätaren.
Tjänst som är kritisk för samhället	En tjänst är kritisk för samhället om en störning i den påverkar en betydande mängd kunder, ett stort geografiskt område eller om störningen har allvarliga följdverkningar.
Cybersäkerhetsstrategi	Definierar organisationens cybersäkerhetsmål, prioriteter för målen, ansvar och uppföljning. Den kan vara dokumenterad som separat dokument, men är ofta dokumenterad i en cybersäkerhetspolicy som ledningen ställt upp (informationssäkerhetspolicy).
Cybersäkerhetsarkitekturstrategi	Mål, prioriteter, ansvar och uppföljningsprocess för cybersäkerhetsarkitekturstrategin. Den bör vara i överensstämmelse med den allmänna cybersäkerhetsstrategin och företagsarkitekturen.
Organisation som är kritisk för försörjningsberedskapen	En organisation som är kritisk för försörjningsberedskapen är en ”organisation som är särskilt betydelsefull med tanke på

	säkerställande av samhällets vitala funktioner. En organisation som är kritisk för försörjningsberedskapen kan vara ett företag eller en annan organisation.” [5] Det huvudsakliga syftet med Cybermätaren är att utveckla dessa kritiska aktörers beredskap och beroende på detta hänvisas det i Cybermätaren till sådana organisationer och för samhället kritiska tjänster och funktioner som de producerar. Det bör observeras att Cybermätaren lämpar sig lika väl för användning vid bedömning av organisationer som inte är kritiska för försörjningsberedskapen. I det fallet ska hänvisningar i Cybermätaren till kritiska tjänster och funktioner förstås som tjänster eller verksamheter som är kritiska för organisationens egen affärsverksamhet.

7 Källförteckning

[1] NIST Cybersecurity Framework Version 1.1, NIST, 04 2018 [Tillgänglig på: https://doi.org/10.6028/NIST.CSWP.04162018]

[2] Cybersecurity Capability Maturity Model (C2M2) version 1.1, U.S. Department of Energy, 02 2014 [Tillgänglig på: https://www.energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf]

[3] Cybersecurity Capability Maturity Model (C2M2) version 2.0 (draft), U.S. Department of Energy, 06 2019 [Tillgänglig på: https://www.energy.gov/sites/prod/files/2019/08/f65/ C2M2 v2.0 06202019 DOE for Comment.pdf]

[4] Kansallinen riskiarvio 2018, Sisäministeriö, 01 2019 [Tillgänglig på: http://urn.fi/URN:ISBN:978-952-324-245-6]

[5] Yhteiskunnan turvallisuusstrategia 2017, Turvallisuuskomitea, 11 2017 [Tillgänglig på: https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/YTS_2017_suomi.pdf]