EUROPEAN UNION AGENCY
FOR CYBERSECURITY

NATIONELL RAM FÖR KAPACITETSBEDÖMNING

DECEMBER 2020

OM ENISA

Europeiska unionens cybersäkerhetsbyrå, Enisa, är ett EU-organ som har till uppgift att säkerställa en hög nivå av cybersäkerhet i Europa. Europeiska unionens cybersäkerhetsbyrå, som grundades 2004 och stärktes genom EU:s cybersäkerhetsakt, bidrar till EU:s cyberpolitik och förbättrar tillförlitligheten hos produkter, tjänster och processer inom IKT genom program för cybersäkerhetscertifiering. Dessutom samarbetar byrån med medlemsstater och andra EU-organ, och hjälper Europa att förbereda sig inför morgondagens cyberutmaningar. Genom kunskapsspridning, kapacitetsuppbyggnad och åtgärder för att öka medvetenheten arbetar byrån tillsammans med sina huvudintressenter för att stärka tillförlitligheten i den uppkopplade ekonomin, motståndskraften i unionens infrastruktur och, mer generellt, för att upprätthålla den digitala säkerheten i Europa och för dess medborgare. För mer information, besök www.enisa.europa.eu.

KONTAKT

Kontakta författarna på team@enisa.europa.eu.
För frågor från medier om detta dokument, kontakta press@enisa.europa.eu.

FÖRFATTARE

Anna Sarri, Pinelopi Kyranoudi – Europeiska unionens cybersäkerhetsbyrå (Enisa)
Aude Thirriot, Federico Charelli, Yang Dominique – Wavestone

TACK

Enisa vill tacka alla experter som deltagit och lämnat värdefulla bidrag till denna rapport, särskilt följande:

Centrala statsbyrån för utvecklingen av ett digitalt samhälle (Kroatien), Marin Ante Pivcevic

Centrumet för cybersäkerhet (Belgien)

CFCS – Center for Cybersikkerhed (Danmark), Thomas Wulff

Europols it-brottscentrum – EC3, Alzofra Martinez Alvaro

Europols it-brottscentrum – EC3, Adrian-Ionut Bobeica

Förbundsministeriet för inrikes frågor (Tyskland), Sascha-Alexander Lettgen

Informationssäkerhetsadministrationen (Slovenien), Marjan Kavčič

Italiens regering (Italien)

Maltas IT-byrå (Malta), Katia Bonello och Martin Camilleri

Justitie- och säkerhetsministeriet (Norge), Robin Bakke

Digitala policyministeriet (Grekland), George Drivas, Nestoras Chouliaras, Evgenia Tsaprali och Sotiris Vasilos

Ministeriet för ekonomi och kommunikation (Estland), Anna-Liisa Pärnalaas

Nationella cyber- och informationssäkerhetsbyrån (Tjeckien), Veronika Netolická

Nationella säkerhetsmyndighet (Slovakien)

Nationella säkerhetsavdelningen (Spanien), Maria Mar Lopez Gil

Justitie- och säkerhetsministeriet, NCTV (Nederländerna)

Portugals nationella cybersäkerhetscenter (Portugal), Alexandre Leite och Pedro Matos

Cyber Security Policy Division, Department of Environment, Climate and Communications (Ireland), James Caffrey

University of Oxford Global Cyber Security Capacity Centre, Carolin Weisser Harris

Enisa vill också tacka alla experter som bidragit med synpunkter men föredrar att vara anonyma, för deras värdefulla bidrag till denna studie.

RÄTTSLIGT MEDDELANDE

Observera att denna publikation speglar Enisas synpunkter och tolkningar, om inget annat anges. Publikationen ska inte ses som ett rättsligt initiativ från Enisa eller dess organ, såvida den inte antas i enlighet med förordning (EU) nr 2019/881.
Publikationen speglar inte nödvändigtvis de senaste tekniska landvinningarna och Enisa kan komma att uppdatera den ibland.

Hänvisningar till tredjepartskällor görs när så är relevant. Enisa ansvarar inte för innehållet i externa källor, inte heller externa webbplatser som det hänvisas till i denna publikation.

Publikationen är endast avsedd att användas i informationssyfte. Den ska tillhandahållas utan kostnad. Varken Enisa eller någon person som agerar på Enisas vägnar ansvarar för hur informationen i detta dokument kan komma att användas.

MEDDELANDE OM UPPHOVSRÄTT

ISBN: 978-92-9204-495-4

DOI: 10.2824/943770

KATALOG: TP-02-21-253-SV-N

1. INNEHÅLLSFÖRTECKNING

TERMER

AKRONYMER	BESKRIVNING
AI	Artificiell intelligens
C2M2	Mognadsmodell för cybersäkerhetskapacitet
CCRA	System för erkännande av gemensamma kriterier (Common Criteria Recognition Arrangement)
CCSMM	Samhällsmodell för cybersäkerhetsmognad
CMM	Mognadsmodell för nationell cybersäkerhetskapacitet
CMMC	Mognadsmodellcertifiering för cybersäkerhet
CPI	Cyber Power Index
CSIRT	It-incidentcentrum
Dataskyddsförordningen	Den allmänna dataskyddsförordningen
Ecso	Europeiska cybersäkerhetsorganisationen
Efta	Europeiska frihandelssammanslutningen
EQF	Europeiska referensramen för kvalifikationer
EU	Europeiska unionen
FoU	Forskning och utveckling
GCI	Det globala cybersäkerhetsindexet
IA-CM	Modell för intern redovisningskapacitet för den offentliga sektorn
IKT	Informations- och kommunikationsteknik
ISMM	Mognadsmodell för informationssäkerhet för NIST cybersäkerhetsramverk
ITU	Internationella teleunionen
NCSS	Nationell cybersäkerhetsstrategi
NIS	Nät- och informationssäkerhet
NIST	Nationella standardiserings- och teknikinstitutet
OPP	Offentlig-privata partnerskap
PIMS	Hanteringssystem för sekretessuppgifter (Privacy Information Management System)
Q-C2M2	Qatars mognadsmodell för cybersäkerhetskapacitet
SOG-IS MRA	Avtal om ömsesidigt erkännande från högnivågruppen för informationssystemsäkerhet

SAMMANFATTNING

I takt med att den nuvarande hotbilden på cyberområdet fortsätter att förvärras och cyberattackerna fortsätter att öka i både intensitet och antal, måste EU:s medlemsstater reagera effektivt genom att vidareutveckla och anpassa sina nationella strategier för cybersäkerhet. Sedan Enisa offentliggjorde de första studierna om nationella cybersäkerhetsstrategier 2012, har EU:s medlemsstater och Eftaländerna gjort stora framsteg när det gäller att utveckla och genomföra sina strategier.

I denna rapport presenteras Enisas arbete med att bygga upp en nationell ram för kapacitetsbedömning.

Ramen syftar till att ge medlemsstaterna ett instrument för självutvärdering av sin mognadsnivå genom bedömning av sina mål i fråga om nationell cybersäkerhetsstrategi, vilket kommer att underlätta främjandet och uppbyggnaden av cybersäkerhetskapaciteten såväl på strategisk som på operativ nivå.

Ramen ger en enkel, representativ bild av medlemsstatens mognadsgrad när det gäller cybersäkerhet. Den nationella ramen för kapacitetsbedömning är ett verktyg som hjälper medlemsstaterna att

- tillhandahålla användbar information för att utveckla en långsiktig strategi (t.ex. god praxis, riktlinjer),
- identifiera saknade element inom den nationella cybersäkerhetsstrategin,
- bygga upp ytterligare cybersäkerhetskapacitet,
- stärka ansvarsskyldigheten för politiska åtgärder,
- stärka trovärdigheten gentemot allmänheten och internationella partner,
- stödja uppsökande verksamhet och förstärka den offentliga bilden av en transparent organisation,
- föregripa framtida frågor och problem,
- identifiera dragna lärdomar och bästa praxis,
- tillhandahålla en utgångspunkt för cybersäkerhetskapacitet i hela EU för att underlätta dialogen,
- utvärdera den nationella kapaciteten när det gäller cybersäkerhet.

Denna ram utformades med stöd av Enisas ämnesområdesexperter och företrädare för 19 medlems- och Eftastater.[1] Målgruppen för denna rapport är beslutsfattare, experter och myndighetspersonal som ansvarar för eller deltar i utformningen, genomförandet och

[1] Företrädare för följande medlemsstater och Eftastater intervjuades: Belgien, Kroatien, Tjeckien, Danmark, Estland, Tyskland, Grekland, Ungern, Irland, Italien, Lichtenstein, Malta, Nederländerna, Norge, Portugal, Slovakien, Slovenien, Spanien och Sverige.

utvärderingen av nationella cybersäkerhetsstrategier och, i bredare bemärkelse, i arbetet med cybersäkerhetskapacitet.

Den nationella ramen för kapacitetsbedömning omfattar 17 strategiska mål och är uppbyggd kring fyra huvudkluster:

- Kluster 1: Styrning och standarder för cybersäkerhet
  1. Utarbeta en nationell it-beredskapsplan
  2. Upprätta grundläggande säkerhetsåtgärder
  3. Förstärka säkerheten på området digital identitet och bygga upp förtroende för offentliga digitala tjänster

- Kluster 2: Kapacitetsuppbyggnad och medvetenhet
  4. Organisera cybersäkerhetsövningar
  5. Upprätta en kapacitet för incidenthantering
  6. Öka användarnas medvetenhet
  7. Stärka kompetensutveckling och utbildningsprogram
  8. Främja forskning och utveckling
  9. Tillhandahålla incitament för att den privata sektorn ska investera i säkerhetsåtgärder
  10. Förbättra cybersäkerheten i leveranskedjan

- Kluster 3: Lagstiftning och föreskrifter
  11. Skydda kritisk informationsinfrastruktur, samhällsviktiga tjänster och digitala tjänster
  12. Bekämpa it-brottslighet
  13. Inrätta mekanismer för incidentrapportering
  14. Stärka sekretess och dataskydd

- Kluster 4: Samarbete
  15. Inrätta ett offentlig-privat partnerskap
  16. Institutionalisera samarbete mellan offentliga organ
  17. Delta i internationellt samarbete

1. INLEDNING

Enligt nätverks- och informationssäkerhetsdirektivet (NIS-direktivet) från juli 2016 ska EU:s medlemsstater inrätta en nationell strategi för nät- och informationssystemsäkerhet, dvs. en nationell cybersäkerhetsstrategi, i enlighet med artiklarna 1 och 7. I detta sammanhang definieras en nationell cybersäkerhetsstrategi som en ram som fastställer strategiska principer, riktlinjer, strategiska mål, prioriteringar, lämplig politik och lagstiftningsåtgärder. Det planerade målet för en nationell cybersäkerhetsstrategi är att uppnå och upprätthålla en hög nivå av nät- och systemsäkerhet för att möjliggöra för medlemsstaterna att minska potentiella hot. Den nationella cybersäkerhetsstrategin kan också fungera som katalysator för industriell utveckling och ekonomiska och sociala framsteg.

Enligt EU:s cybersäkerhetsakt ska Enisa främja spridningen av bästa praxis vid utformningen och genomförandet av en nationell cybersäkerhetsstrategi genom att stödja medlemsstaterna i införandet av nätverks- och informationssäkerhetsdirektivet och genom att samla in värdefull återkoppling om deras erfarenheter. I detta syfte har Enisa tagit fram flera verktyg för att hjälpa medlemsstaterna att utveckla, genomföra och utvärdera sina nationella cybersäkerhetsstrategier.

Som en del av sitt uppdrag syftar Enisa till att utveckla en nationell ram för självutvärdering av kapacitet för att mäta mognadsnivån hos de olika nationella cybersäkerhetsstrategierna. Syftet med denna rapport är att presentera den genomförda studien vid fastställandet av självutvärderingsramen.

1.1 TILLÄMPNING, OMFATTNING OCH MÅL

Huvudsyftet med denna studie är att skapa en nationell ram för självutvärdering av kapacitet, nedan kallad *nationell ram för kapacitetsbedömning*, för att mäta mognadsgraden i fråga om medlemsstaternas cybersäkerhetskapacitet. Mer specifikt bör ramen göra det möjligt för medlemsstaterna att

- genomföra utvärderingen av den nationella cybersäkerhetskapaciteten,
- öka medvetenheten om landets mognadsnivå,
- identifiera förbättringsområden,
- bygga upp cybersäkerhetskapacitet.

Denna ram bör hjälpa medlemsstaterna, och särskilt de nationella beslutsfattarna, att genomföra en självutvärdering i syfte att förbättra den nationella cybersäkerhetskapaciteten.

1.2 METOD

Den metod som används för att utveckla den nationella ramen för intern kapacitetsutvärdering bygger på fyra delar:

1. **Skrivbordsundersökning**: Det första steget bestod i att genomföra en omfattande litteraturöversyn för att samla in bästa praxis och utveckla en ram för bedömning av nationella cybersäkerhetsstrategiers mognadsnivå. Skrivbordsundersökningarna är inriktade på systematisk analys av relevanta dokument om kapacitetsuppbyggnad och strategidefinition inom cybersäkerhet, på befintliga medlemsstaters nationella cybersäkerhetsstrategier och på en jämförelse av befintliga mognadsmodeller för cybersäkerhet. En riktmärkesaktivitet för befintliga mognadsmodeller fastställdes genom införandet av ett analysramverk som utvecklats för denna studie. Analysramen

bygger på Beckers[2] metod för utveckling av mognadsmodeller. Enligt denna fastställs en generisk och konsoliderad förfarandemall för utformning av mognadsmodeller med tydliga krav för utvecklingen av dessa. Analysramen anpassades ytterligare för att tillgodose behoven i denna studie.

2. **Insamling av synpunkter från experter och berörda parter**: Denna fas tar avstamp i de data som samlats in genom skrivbordsundersökningarna och de tillhörande preliminära analysresultaten, och omfattar identifiering och inbjudan av ett antal identifierade experter med erfarenhet av utveckling och genomförande av nationella cybersäkerhetsstrategier eller mognadsmodeller, för att intervjua dessa. Enisa kontaktade sin nationella expertgrupp på området nationell cybersäkerhetsstrategi och sina nationella kontaktpersoner för att hitta relevanta experter i varje medlemsstat. Dessutom intervjuades några experter som var involverade i arbetet med att utveckla mognadsmodeller. Totalt genomfördes 22 intervjuer, varav 19 genomfördes med företrädare för cybersäkerhetsorgan i olika medlemsstater (och Eftaländer).
3. **Analys av översynens resultat:** De uppgifter som samlats in genom skrivbordsundersökningar och intervjuer analyserades sedan för att identifiera bästa praxis vid utformningen av en ram för självutvärdering för att mäta den nationella cybersäkerhetsstrategins mognadsnivå, i syfte att förstå medlemsstaternas behov och avgöra vilka uppgifter som rimligen kan samlas in i de olika europeiska länderna[3]. Denna analys gör det möjligt att finjustera den preliminära modell som utvecklats i de föregående stegen och förfina de indikatorer som ingår i modellen, mognadsnivåerna och dess dimensioner.
4. **Slutförande av modellen:** Det fjärde steget innebar att den uppdaterade versionen av den nationella ramen för intern kapacitetsutvärdering granskades av Enisas ämnesexperter. Ramen bekräftades sedan av experter genom ett seminarium som hölls i oktober 2020, före dess offentliggörande.

1.3 MÅLGRUPP

Målgruppen för denna rapport är beslutsfattare, experter och myndighetspersonal som ansvarar för eller deltar i utformningen, genomförandet och utvärderingen av nationella cybersäkerhetsstrategier och som på en bredare nivå hanterar cybersäkerhetskapacitet. Dessutom kan de resultat som formaliseras i detta dokument vara av värde för experter på cybersäkerhetsområdet och forskare på nationell eller europeisk nivå.

[2] J. Becker, R. Knackstedt, och J. Pöppelbuß, "Developing Maturity Models for IT Management: A Procedure Model and its Application", Business & Information Systems Engineering, vol. 1, nr 3, s. 213–222, juni 2009.
[3] Hänvisningar till de "europeiska länderna" som görs i denna studie och i denna rapport syftar på de 27 EU-medlemsstaterna.

2. BAKGRUND

2.1 TIDIGARE ARBETE MED DE NATIONELLA CYBERSÄKERHETSSTRATEGIERNAS LIVSCYKEL

Som anges i EU:s cybersäkerhetsakt är ett av Enisas huvudmål att stödja medlemsstaterna i utvecklingen av nationella strategier för nät- och informationssystemens säkerhet, främja spridningen av dessa strategier och övervaka genomförandet av dem. Som en del av sitt uppdrag har Enisa tagit fram flera dokument på detta ämne för att främja utbyte av god praxis och stödja genomförandet av nationella cybersäkerhetsstrategier i hela EU:

- ”Practical guide on the development and execution phase of NCSS” (praktisk vägledning om utvecklings- och genomförandefasen för nationella cybersäkerhetsstrategier”[4], offentliggjord 2012
- ”Setting the course for national efforts to strengthen security in cyberspace” (färdplan för nationella insatser i syfte att förstärka cybersäkerheten)[5], offentliggjord 2012
- Enisas första ram för utvärdering av en medlemsstats nationella cybersäkerhetsstrategi[6] offentliggjordes 2014.
- Den interaktiva onlinekartan över nationella cybersäkerhetsstrategier[7], offentliggjord 2014.
- ”NCSS Good Practice Guide” (vägledning för bästa praxis i fråga om nationella cybersäkerhetsstrategier)[8], offentliggjord 2016.
- ”National Cybersecurity Strategies Evaluation Tool” (utvärderingsverktyg för nationella cybersäkerhetsstrategier)[9], offentliggjord 2018.
- ”Good practices in innovation on Cybersecurity under the NCSS” (god praxis för innovation inom cybersäkerhet inom ramen för nationella cybersäkerhetsstrategier)[10], offentliggjord 2019.

I BILAGA A finns en kort sammanfattning av Enisas viktigaste publikationer inom ämnet.

Ovannämnda vägledningar och dokument ingick som en del i skrivbordsundersökningen. I synnerhet är utvärderingsverktyget för nationella cybersäkerhetsstrategier[11] en grundläggande

[4] NCSS: Practical Guide on Development and Execution (Enisa, 2012)
https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
[5] NCSS: Setting the course for national efforts to strengthen security in cyberspace (Enisa, 2012)
https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
[6] An evaluation framework for NCSS (Enisa, 2014)
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
[7] National Cybersecurity Strategies – Interactive Map (Enisa, 2014, uppdaterad 2019)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[8] Detta dokument är en uppdaterad version av 2012 års vägledning: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (Enisa, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide
[9] National Cybersecurity Strategies Evaluation Tool (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[10] https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1
[11] National Cybersecurity Strategies Evaluation Tool (2018)
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

del av den nationella ramen för kapacitetsbedömning. Den senare bygger nämligen på de mål som beskrivs i det webbaserade utvärderingsverktyget för nationella cybersäkerhetsstrategier.

2.2 GEMENSAMMA MÅL SOM IDENTIFIERATS I NATIONELLA CYBERSÄKERHETSSTRATEGIER I EU

Skillnaderna mellan de olika medlemsstaterna gör det svårt att identifiera gemensamma aktiviteter eller handlingsplaner i olika nationella sammanhang, rättsliga ramar och politiska dagordningar. Medlemsstaternas nationella cybersäkerhetsstrategier har dock ofta strategiska mål som rör samma frågor. Baserat på Enisas tidigare arbete och analysen av medlemsstaternas nationella cybersäkerhetsstrategier har 22 strategiska mål därmed kunnat identifieras. Av dessa fastställdes 15 strategiska mål redan i Enisas tidigare publikationer, två har tillkommit i samband med denna studie och fem mål har identifierats för övervägande.

2.2.1 Gemensamma strategiska mål som medlemsstaterna använder

Tabellen nedan bygger på Enisas tidigare arbete, närmare bestämt utvärderingsverktyget för nationella cybersäkerhetsstrategier[12], och visar de 15 strategiska mål som vanligtvis ingår i medlemsstaternas nationella cybersäkerhetsstrategier. I målen beskrivs kärnan i den övergripande nationella tillnärmningen i frågan. För ytterligare information om de mål som beskrivs nedan hänvisas till Enisas vägledning för bästa praxis i fråga om nationella cybersäkerhetsstrategier, ”NCSS Good Practice Guide”[13].

Tabell 1: Gemensamma strategiska mål som ingår i medlemsstaternas nationella cybersäkerhetsstrategier

ID	Strategiska mål för nationella cybersäkerhetsstrategier	Mål
1	**Utarbeta nationella beredskapsplaner för cybersäkerhet**	▶ Presentera och förklara de kriterier som bör användas för att definiera en situation som en kris. ▶ Definiera viktiga processer och åtgärder för att hantera krisen. ▶ Tydligt definiera olika intressenters roller och ansvar under en cybersäkerhetskris. ▶ Presentera och förklara kriterierna för att en kris ska anses vara över och/eller vem som har befogenhet att avgöra detta.
2	**Upprätta grundläggande säkerhetsåtgärder**	▶ Harmonisera de olika metoder som tillämpas av organisationer inom såväl den offentliga som den privata sektorn. ▶ Skapa ett gemensamt språk för kommunikationen mellan de behöriga offentliga myndigheterna och organisationerna samt öppna säkra kommunikationskanaler. ▶ Göra det möjligt för olika intressenter att kontrollera och jämföra sin cybersäkerhetskapacitet. ▶ Utbyta information om god praxis för cybersäkerhet inom alla industrisektorer. ▶ Hjälpa intressenterna att prioritera sina investeringar i säkerhet.
3	**Organisera cybersäkerhetsövningar**	▶ Identifiera vad det är som behöver testas (planer och processer, människor, infrastruktur, svarskapacitet, samarbetsförmåga, kommunikation etc.).

https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool

[12] National Cybersecurity Strategies Evaluation Tool (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool

[13] Detta dokument är en uppdaterad version av 2012 års vägledning: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (Enisa, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide

ID	Strategiska mål för nationella cybersäkerhetsstrategier	Mål
		▶ Inrätta en nationell planeringsgrupp för cyberövningar med ett tydligt uppdrag. ▶ Integrera cyberövningar i den nationella cybersäkerhetsstrategins eller den nationella beredskapsplanens livscykel.
4	Upprätta en kapacitet för incidenthantering	▶ Uppdrag – gäller de befogenheter, roller och ansvarsområden som respektive regering måste tilldela arbetsgruppen. ▶ Tjänsteportfölj – omfattar de tjänster som en arbetsgrupp tillhandahåller sina uppdragsgivare eller använder för sin egen interna funktion. ▶ Operativ kapacitet – gäller de tekniska och operativa krav som en arbetsgrupp måste uppfylla. ▶ Samarbetsförmåga – omfattar krav på informationsutbyte med andra arbetsgrupper som inte omfattas av de tre föregående kategorierna, t.ex. beslutsfattare, försvaret, tillsynsmyndigheter, operatörer (på området kritisk informationsinfrastruktur) och brottsbekämpande myndigheter.
5	Öka användarnas medvetenhet	▶ Identifiera kunskapsluckor vad gäller cybersäkerhet eller informationssäkerhetsfrågor. ▶ Fylla kunskapsluckorna genom att öka medvetenheten eller utveckla/stärka grundläggande kunskaper.
6	Stärka kompetensutveckling och utbildningsprogram	▶ Förbättra den befintliga informationssäkerhetspersonalens operativa kapacitet. ▶ Skapa intresse hos studenter och förbereda dem inför en framtid inom cybersäkerhetsområdet. ▶ Främja och uppmuntra kontakten mellan de akademiska grenarna av informationssäkerhet och informationssäkerhetssektorn. ▶ Anpassa cybersäkerhetsutbildningar efter företagens behov.
7	Främja forskning och utveckling	▶ Identifiera de verkliga orsakerna till sårbarheter i stället för att reparera de skador som uppstår till följd av dem. ▶ Sammanföra forskare från olika discipliner för att hitta lösningar på flerdimensionella och komplexa problem som till exempel fysiska cyberhot. ▶ Förena industrins behov och forskningsresultaten för att på så sätt underlätta övergången från teori till praktik. ▶ Hitta sätt att upprätthålla och öka cybersäkerhetsnivån för produkter och tjänster som bygger på befintliga it-infrastrukturer.
8	Tillhandahålla incitament för att den privata sektorn ska investera i säkerhetsåtgärder	▶ Identifiera eventuella incitament för privata företag att investera i säkerhetsåtgärder. ▶ Ge företagen incitament som uppmuntrar till investeringar i säkerhet.
9	Skydda kritisk informationsinfrastruktur och leverantörer av samhällsviktiga tjänster samt av digitala tjänster (kritisk informationsinfrastruktur)	▶ Identifiera kritisk informationsinfrastruktur. ▶ Identifiera och minska relevanta risker för kritisk informationsinfrastruktur.
10	Bekämpa it-brottslighet	▶ Lagstiftning på området it-brottslighet. ▶ Öka de brottsbekämpande organens effektivitet.
11	Inrätta mekanismer för incidentrapportering	▶ Få kunskap om den övergripande hotmiljön. ▶ Bedöma konsekvenserna av incidenter (t.ex. säkerhetsöverträdelser, nätverksfel, serviceavbrott). ▶ Få kunskap om befintliga och nya sårbarheter och typer av attacker. ▶ Uppdatera säkerhetsåtgärderna i enlighet med detta. ▶ Genomföra bestämmelserna i NIS-direktivet gällande incidentrapportering.
12	Stärka sekretess och dataskydd	▶ Bidra till att stärka grundläggande rättigheter när det gäller integritet och uppgiftsskydd.
13	Inrätta ett offentlig-privat partnerskap (OPP)	▶ Avskräcka (avskräcka angripare). ▶ Skydda (använda forskning om nya säkerhetshot).

ID	Strategiska mål för nationella cybersäkerhetsstrategier	Mål
		▶ Upptäcka (dra växlar av informationsdelning för att hantera nya hot). ▶ Reagera (tillhandahålla kapacitet att hantera en incidents initiala påverkan). ▶ Återhämtning (tillhandahålla kapacitet för att reparera den slutliga effekten av en incident).
14	**Institutionalisera samarbete mellan offentliga organ**	▶ Stärka samarbetet mellan offentliga organ med ansvar och kompetens på cybersäkerhetsområdet. ▶ Undvika överlappning av befogenheter och resurser mellan offentliga organ. ▶ Förbättra och institutionalisera samarbetet mellan offentliga myndigheter inom olika cybersäkerhetområden.
15	**Bedriva internationellt samarbete (inte bara med EU-medlemsstater)**	▶ Utnyttja fördelarna med att skapa en gemensam kunskapsbas mellan EU:s medlemsstater. ▶ Skapa synergieffekter mellan nationella cybersäkerhetsmyndigheter. ▶ Möjliggör och utöka kampen mot gränsöverskridande brottslighet.

2.2.2 Ytterligare strategiska mål

Med utgångspunkt i den skrivbordsundersökning och de intervjuer som genomförts av Enisa fastställdes ytterligare strategiska mål. Medlemsstaterna tar i allt högre utsträckning upp dessa aspekter i sina nationella cybersäkerhetsstrategier eller fastställer handlingsplaner inom området. Exempel på åtgärder som genomförts av medlemsstaterna ges också. Om ett exempel kommer från en allmänt tillgänglig källa görs en hänvisning till denna. I de fall där exempel grundar sig på konfidentiella intervjuer med tjänstemän från EU:s medlemsstater ges inga referenser.

Följande ytterligare strategiska mål har identifierats:

- Förbättra cybersäkerheten i leveranskedjan.
- Förstärka säkerheten på området digital identitet och bygga upp förtroende för offentliga digitala tjänster.

Förbättra cybersäkerheten i leveranskedjan

Små och medelstora företag är ryggraden i Europas ekonomi. De utgör 99 procent av alla företag i EU[14] och 2015 uppskattades de små och medelstora företagen ha skapat omkring 85 procent av alla nya arbetstillfällen och stått för två tredjedelar av den totala sysselsättningen inom den privata sektorn i EU. Eftersom små och medelstora företag tillhandahåller tjänster till stora företag och i allt högre grad samarbetar med offentliga förvaltningar[15], är det viktigt att observera att de små och medelstora företagen utgör den svaga länken vad gäller it-attacker i dagens sammanlänkade värld. Små och medelstora företag är de aktörer som utsätts mest för it-attacker, men de saknar ofta de ekonomiska resurser som krävs för att investera tillräckligt i

[14] https://ec.europa.eu/growth/smes/
[15] https://www.oecd.org/fr/publications/smes-in-public-procurement-9789264307476-en.htm
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

cybersäkerhet[16]. Förbättringarna av cybersäkerheten i leveranskedjan bör därför vara inriktade på små och medelstora företag.

Utöver detta systembaserade tillvägagångssätt kan medlemsstaterna också lägga tonvikten på insatser för cybersäkerhet för särskilda IKT-tjänster och IKT-produkter som anses vara särskilt betydelsefulla: IKT-teknik som används i kritisk informationsinfrastruktur, säkerhetsmekanismer inom telekommunikationssektorn (kontroller på ISP-nivå etc.), betrodda tjänster enligt definitionen i eIDA-förordningen och leverantörer av molntjänster. Till exempel åtog sig Polen i sin nationella strategi för cybersäkerhet 2019–2024[17] att utveckla ett nationellt system för bedömning och certifiering av cybersäkerhet som en mekanism för kvalitetssäkring i leveranskedjan. Detta certifieringssystem kommer att anpassas till EU:s certifieringsram för digitala IKT-produkter, tjänster och processer som inrättats genom EU:s cybersäkerhetsakt (2019/881).

Det är därför av största vikt att förbättra cybersäkerheten i leveranskedjan. Detta kan uppnås genom att en kraftfull politik införs för att bland annat främja små och medelstora företag, tillhandahålla riktlinjer för cybersäkerhetskrav i offentliga upphandlingsförfaranden, främja samarbete inom den privata sektorn, bygga upp offentlig-privata partnerskap, främja mekanismer för samordnad information om sårbarheter[18], skapa produktcertifieringssystem, inklusive cybersäkerhetskomponenter i digitala initiativ för små och medelstora företag, och finansiera kompetensutveckling.

Förstärka säkerheten på området digital identitet och bygga upp förtroende för offentliga digitala tjänster

I februari 2020 lade kommissionen fram sin vision för den digitala omvandlingen av EU i meddelandet ”Att forma Europas digitala framtid”[19], med målet att tillhandahålla inkluderande teknik som arbetar för människor och som respekterar EU:s grundläggande värderingar. I meddelandet anges särskilt att det är av avgörande betydelse att främja den digitala omvandlingen av offentliga förvaltningar runtom i Europa. I det avseendet är det av yttersta vikt att bygga upp förtroende för myndigheter när det gäller digital identitet och förtroende för den offentliga sektorn. Det blir ännu viktigare om man betänker att transaktioner och datautbyte inom den offentliga sektorn ofta innehåller känslig information.

Många länder har gett uttryck för sin avsikt att ta upp denna fråga i sina nationella cybersäkerhetsstrategier, däribland Danmark, Estland, Frankrike, Luxemburg, Malta, Spanien, Nederländerna och Förenade kungariket. Bland dessa länder har vissa också uttryckt att detta strategiska mål skulle kunna tas upp som en del av en bredare plan:

- Estland kopplade till exempel sin handlingsplan för säkerhet i fråga om elektronisk identitet och elektronisk autentisering till den bredare digitala agendan för Estland år 2020.
- I den franska nationella cybersäkerhetsstrategin anges att statssekreteraren med ansvar för digital teknik övervakar utarbetandet av en färdplan ”för att skydda det franska folkets digitala liv, integritet och personuppgifter”.
- I den nederländska nationella cybersäkerhetsstrategin anges att cybersäkerhet i offentliga förvaltningar samt offentliga tjänster som tillhandahålls till medborgare och

[16] https://www.eesc.europa.eu/sv/news-media/news/european-companies-especially-smes-face-growing-risk-cyber-attacks-study
[17] http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf
[18] https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline
[19] Att forma Europas digitala framtid, COM(2020) 67 final: https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_3.pdf

företag diskuteras mer ingående inom ramen för landets allmänna agenda för digital förvaltning.

- Den brittiska regeringen fortsätter att göra allt fler av sina tjänster tillgängliga på nätet och har utsett en statlig digital tjänst för att säkerställa att alla nya digitala tjänster som skapas eller upphandlas av regeringen har inbyggd säkerhet ”som standard”, med stöd av det brittiska organet National Cybersecurity Centre (NCSC).

2.2.3 Andra strategiska mål som övervägts

Under skrivbordsundersökningen och intervjufasen undersöktes även andra strategiska mål. Det beslutades dock att dessa mål inte skulle ingå i ramen för självutvärdering. BILAGA C – Andra undersökta mål

innehåller definitioner för vart och ett av dessa mål som kan användas som underlag för framtida diskussioner om möjliga förbättringar av nationella cybersäkerhetsstrategier.

Följande strategiska mål togs upp för övervägande inför eventuell inkludering i framtiden:

- Utveckla sektorsspecifika strategier för cybersäkerhet.
- Bekämpa desinformationskampanjer.
- Säkra spetsteknik (5G, AI, kvantdatorteknik etc.).
- Säkerställa datasuveränitet.
- Tillhandahålla incitament för utvecklingen av cyberförsäkringssektorn.

2.3 VIKTIGA RESULTAT AV BENCHMARKINGAKTIVITETEN

Skrivbordsundersökningen av befintliga mognadsmodeller för cybersäkerhet genomfördes i syfte att samla in information och bevis till stöd för utformningen av nationella ramar för självutvärdering av kapacitet i samband med nationella cybersäkerhetsstrategier. Mot denna bakgrund genomfördes en omfattande litteraturgenomgång av befintliga modeller för att komplettera resultaten från de inledande sonderingsstudierna om mognadsmodeller för cybersäkerhet och befintliga nationella cybersäkerhetsstrategier, som förklaras närmare i avsnitt 2.1 och 2.2. Denna systematiska översyn stödjer urvalet och motiveringen av bedömningsramens mognadsnivåer och fastställandet av de olika dimensionerna och indikatorerna.

Inom ramen för den systematiska översynen av mognadsmodellerna övervägdes och analyserades tio modeller baserat på deras viktigaste egenskaper. Den övergripande översikten över nyckelfunktionerna för varje modell som granskas inom ramen för studien finns att läsa i Tabell 2: Översikt över analyserade mognadsmodeller och en mer detaljerad analys finns i BILAGA A.

Tabell 2: Översikt över analyserade mognadsmodeller

Modellens namn	Antal mognads nivåer	Antal egenskaper	Bedömningsmetod	Representation av resultat
Mognadsmodell för nationell cybersäkerhetskapacitet (CMM)	5	5 huvuddimen sioner	Samarbete med en lokal organisation för att finjustera modellen innan den tillämpas i en nationell kontext	5-sektionsradar
Mognadsmodell för cybersäkerhetskapacitet (C2M2)	4	10 huvuddomä ner	Metod för självutvärdering och verktygslåda	Poängkort med cirkeldiagram

Ram för förbättring av kritisk cybersäkerhetsinfrastruktur	Inte tillämpligt (4 skikt)	5 kärnfunktioner	Självutvärdering	Inte tillämpligt
Qatars mognadsmodell för cybersäkerhetskapacitet (Q-C2M2)	5	5 huvuddomäner	Inte tillämpligt	Inte tillämpligt
Certifiering av mognadsmodell för cybersäkerhet (CMMC)	5	17 huvuddomäner	Bedömning av utomstående revisorer	Inte tillämpligt
Samhällsmodell för cybersäkerhetsmognad (CCSMM)	5	6 huvuddimensioner	Bedömning inom samhällen med stöd från statliga och federala brottsbekämpande organ	Inte tillämpligt
Mognadsmodell för informationssäkerhet för NIST cybersäkerhetsramverk (ISMM)	5	23 utvärderade områden	Inte tillämpligt	Inte tillämpligt
Modell för intern revisionskapacitet (IA-CM) för den offentliga sektorn	5	6 element	Självutvärdering	Inte tillämpligt
Globalt cybersäkerhetsindex (GCI)	Inte tillämpligt	5 pelare	Självutvärdering	Rangordningstabell
Cyber Power Index (CPI)	Inte tillämpligt	4 kategorier	Benchmarking av Economist Intelligence Unit	Rangordningstabell

Denna systematiska översyn gjorde det möjligt att dra slutsatser om bästa praxis som antagits i befintliga modeller för att stödja utvecklingen av den konceptuella modellen för den nuvarande mognadsmodellen. Benchmarkingaktiviteten främjade särskilt fastställandet av mognadsnivåer, skapandet av dimensionskluster och urvalet av indikatorer samt en lämplig visualiseringsmetod för modellens resultat. De mest relevanta undersökningsresultaten för var och en av dessa faktorer beskrivs närmare i Tabell 3.

Tabell 3: Viktiga resultat av benchmarkingaktiviteten

Egenskap	Viktigaste lärdomar
Mognadsnivåer	▶ En femgradig skala för bedömningsramar för cybersäkerhetskapacitet är allmänt accepterad och kan ge detaljerade bedömningsresultat (se 6 Tabelljämförelse av mognadsnivåer för en uttömmande bild av definitionen av mognadsnivåerna för varje modell). ▶ Alla modeller ger en definition på en allmän nivå av varje mognadsnivå, vilken sedan anpassas till de olika dimensionerna eller klustren av dimensioner. ▶ Två huvudaspekter bedöms vanligtvis när man mäter cybersäkerhetskapacitetens mognad: strategiernas mognad och mognaden hos de processer som införts för att genomföra strategierna.
Attribut	▶ Den jämförande analysen av attribut i de befintliga mognadsmodellerna visar heterogena resultat med i genomsnitt 4–5 attribut per modell. ▶ En modell som bygger på fyra eller fem attribut ger länderna rätt nivå av datagranularitet genom att relevanta dimensioner grupperas tillsammans och genom att resultaten blir läsbara (se Tabell 7: Jämförelse av attribut och dimensioner en beskrivning av attribut för varje modell). ▶ Den nyckelprincip som tillämpas för alla modeller vid definitionen av klustren bygger på enhetligheten hos de element som grupperas inom varje kluster.
Utvärderingsmetod	▶ De bedömningsmetoder som används i de olika analyserade modellerna varierar från en modell till en annan. ▶ Den vanligaste bedömningsmetoden bygger på självutvärdering.
Resultatpresentation	▶ Det är viktigt att resultaten presenteras med olika granularitetsnivåer. ▶ Visualiseringsmetoden bör vara självförklarande och lättläst.

Den konceptuella modellen bygger på benchmarking av de olika mognadsmodellerna samt på Enisas tidigare arbete. Man beslutade också att bygga vidare på *Enisas interaktiva onlineverktyg* för att utveckla mognadsindikatorer som används för varje attribut.

2.4 UTMANINGAR I SAMBAND MED UTVÄRDERING AV NATIONELLA CYBERSÄKERHETSSTRATEGIER

Medlemsstaterna står inför många utmaningar när det gäller att bygga upp cybersäkerhetskapacitet och mer specifikt när det gäller att säkerställa att kapaciteten är i linje med den senaste utvecklingen. Nedan följer en sammanfattning av de utmaningar som identifierats av och diskuterats med medlemsstaterna som en del av denna studie:

- **Svårigheter med samordning och samarbete:** Att samordna cybersäkerhetsinsatserna på nationell nivå för att säkerställa effektiva svarsåtgärder vid cybersäkerhetsproblem kan visa sig bli en utmaning på grund av det stora antalet berörda parter.
- **Brist på resurser för att genomföra bedömningen:** Beroende på det lokala sammanhanget och den nationella styrningsstrukturen för cybersäkerhet kan utvärderingen av den nationella cybersäkerhetsstrategin och dess mål ta mer än femton persondagar.
- **Brist på stöd för att utveckla cybersäkerhetskapacitet:** Vissa medlemsstater anser att de för att försvara en budget och få stöd för att utveckla cybersäkerhetskapaciteten först måste genomföra en utvärderingsfas för att identifiera luckor och begränsningar.
- **Svårigheter att bedöma strategins framgångar eller ändra den:** Allteftersom hoten utvecklas och tekniken förbättras måste handlingsplanerna ständigt anpassas. Det är dock fortfarande en mödosam uppgift att utvärdera nationella cybersäkerhetsstrategier

och driva igenom förändringar av dem. Det gör det i sin tur svårt att identifiera begränsningar och brister i nationella cybersäkerhetsstrategier.

- **Svårigheter att mäta effektiviteten hos nationella cybersäkerhetsstrategier:** Mätningar kan samlas in för att mäta olika områden, såsom framsteg, genomförande, mognad och effektivitet. Det är relativt enkelt att mäta framsteg och genomförande jämfört med att mäta effektivitet, men det senare är fortfarande mer meningsfullt för att utvärdera resultaten och effekterna av en nationell cybersäkerhetsstrategi. I de intervjuer som genomfördes av Enisa uppgav ett stort antal medlemsstater att det är viktigt att kvantitativt mäta effektiviteten hos en nationell cybersäkerhetsstrategi, men det är samtidigt en mycket krävande och i vissa fall omöjlig uppgift.
- **Svårigheter att anta en gemensam ram:** EU:s medlemsstater är verksamma i olika sammanhang vad gäller politik, organisationer, kultur, samhällsstruktur och mognad i fråga om nationell cybersäkerhetsstrategi. Vissa medlemsstater som intervjuades inom ramen för denna studie uttryckte att det kan vara svårt att försvara och använda en enda universalram för självutvärdering (”one-size-fits-all”).

2.5 FÖRDELARNA MED NATIONELL KAPACITETSBEDÖMNING

Sedan 2017 har alla EU-medlemsstater en nationell cybersäkerhetsstrategi[20]. Det är visserligen en positiv utveckling, men det är också viktigt att medlemsstaterna kan göra en ordentlig bedömning av sina nationella cybersäkerhetsstrategier och därigenom tillföra ett mervärde till sin strategiska planering och till genomförandet.

Ett av målen med den nationella ramen för kapacitetsbedömning är att utvärdera cybersäkerhetskapaciteten utifrån de prioriteringar som anges i de olika dokument som lägger grunden för den nationella cybersäkerhetsstrategin. Ramen bedömer mognadsnivån för medlemsstaternas cybersäkerhetskapacitet på de områden som definieras i målen för den nationella cybersäkerhetsstrategin. Resultaten av ramverket stödjer därmed medlemsstaternas beslutsfattare när de fastställer den nationella strategin för cybersäkerhet genom att den förser dem med information om det aktuella läget i landet[21]. Den nationella ramen för kapacitetsbedömning är till syvende och sist avsedd att hjälpa medlemsstaterna att identifiera förbättringsområden och bygga upp kapacitet.

Ramen syftar till att ge medlemsstaterna ett verktyg för självutvärdering av sin mognadsnivå genom bedömning av målen med den nationella cybersäkerhetsstrategin. Detta kommer att hjälpa dem att utöka och bygga vidare på deras cybersäkerhetskapacitet på både strategisk och operativ nivå.

På grundval av de intervjuer som Enisa genomfört med flera myndigheter med ansvar för cybersäkerhet i olika medlemsstater identifierades och betonades följande fördelar med den nationella ramen för kapacitetsbedömning. Ramen

- tillhandahåller användbar information för att utveckla en långsiktig strategi (t.ex. god praxis, riktlinjer),
- bidrar till att identifiera saknade element inom den nationella cybersäkerhetsstrategin,
- bidrar till att bygga upp ytterligare cybersäkerhetskapacitet,
- stärker ansvarsskyldigheten för politiska åtgärder,
- stärker trovärdigheten gentemot allmänheten och internationella partner,

[20] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[21] Weiss, C.H. (1999). The interface between evaluation and public policy. Evaluation, 5(4), 468-486.

- stödjer uppsökande verksamhet och förstärker den offentliga bilden av en transparent organisation,
- hjälper till att föregripa framtida frågor och problem,
- hjälper till att identifiera dragna lärdomar och bästa praxis,
- tillhandahåller en utgångspunkt för cybersäkerhetskapacitet i hela EU för att underlätta dialogen,
- utvärdera den nationella kapaciteten när det gäller cybersäkerhet.

3. METODIK FÖR DEN NATIONELLA RAMEN FÖR KAPACITETSBEDÖMNING

3.1 ALLMÄNT SYFTE

Huvudsyftet med den nationella referensramen för cybersäkerhet är att mäta mognadsnivån hos **medlemsstaternas** cybersäkerhetskapacitet för att stödja dem i genomförandet av en utvärdering av den nationella cybersäkerhetskapaciteten, öka kunskaperna om landets mognadsnivå, identifiera områden för förbättring och bygga upp cybersäkerhetskapacitet.

3.2 MOGNADSNIVÅER

Ramen bygger på **fem mognadsnivåer** som definierar de stadier som medlemsstaterna går igenom när de bygger upp cybersäkerhetskapacitet inom det område som täcks av varje mål som ingår i den nationella cybersäkerhetsstrategin. Mognadsskalan börjar med **nivå 1**, där medlemsstaterna inte har någon klart definierad strategi för kapacitetsuppbyggnad inom cybersäkerhet på de områden som omfattas av målen med den nationella cybersäkerhetsstrategin, och slutar med **nivå 5**, där strategin för kapacitetsuppbyggnad inom cybersäkerhet är dynamisk och anpassad till utvecklingen. Tabell 4 visar mognadsskalan med en beskrivning av varje mognadsnivå.

Tabell 4: Enisas nationella ram för kapacitetsbedömning, mognadsskala i fem nivåer

NIVÅ 1 – INLEDANDE/AD HOC	NIVÅ 2 – TIDIG DEFINITION	NIVÅ 3 – ETABLERING	NIVÅ 4 – OPTIMERING	NIVÅ 5 – ANPASSNINGSFÖRMÅGA
Medlemsstaten har inte någon klart definierad strategi för kapacitetsuppbyggnad inom cybersäkerhet på de områden som täcks av målen i den nationella cybersäkerhetsstrategin. Det kan dock hända att landet fastställt vissa allmänna mål och har genomfört vissa studier (tekniska, politiska, policyrelaterade) för att förbättra den nationella kapaciteten.	Det nationella tillvägagångssättet för kapacitetsuppbyggnad på de områden som omfattas av målen med den nationella cybersäkerhetsstrategin har fastställts. Handlingsplanerna eller åtgärderna för att uppnå resultaten har fastställts men befinner sig fortfarande i ett tidigt skede. Utöver detta kan aktiva intressenter ha identifierats och/eller involverats.	Handlingsplanen för kapacitetsuppbyggnad inom det område som omfattas av målen med den nationella cybersäkerhetsstrategin är tydligt definierad och stöds av berörda parter. Metoderna och åtgärderna verkställs och genomförs på ett enhetligt sätt på nationell nivå. Åtgärderna definieras och dokumenteras med tydlig resursfördelning och styrning samt fastställda tidsgränser.	Handlingsplanen utvärderas regelbundet för att säkerställa att den har rätt prioritering, är optimerad och hållbar. Effekten av kapacitetsuppbyggnaden inom cybersäkerhet mäts regelbundet. Framgångsfaktorer, utmaningar och luckor i genomförandet av olika aktiviteter identifieras.	Strategin för kapacitetsuppbyggnad inom cybersäkerhet är dynamisk och anpassningsbar. Ständig uppmärksamhet på omvärldsutvecklingen (tekniska framsteg, globala konflikter, nya hot etc.) gör det möjligt att fatta snabba beslut och få igenom förbättringar på kort tid.

3.3 KLUSTER OCH ÖVERGRIPANDE STRUKTUR HOS RAMEN FÖR SJÄLVUTVÄRDERING

Ramen för självutvärdering kännetecknas av **fyra kluster**: I) styrning och standarder för cybersäkerhet, II) kapacitetsuppbyggnad och medvetenhet, III) lagstiftning och regelverk samt IV) samarbete. Vart och ett av dessa kluster täcker ett centralt tematiskt område för uppbyggnaden av cybersäkerhetskapacitet i ett land och innehåller ett flertal olika mål som medlemsstaterna kan komma att inkludera i sin nationella cybersäkerhetsstrategi. Det gäller framför allt följande:

- **(I) Förvaltning och standarder för cybersäkerhet**: Det här klustret mäter medlemsstaternas förmåga att få till stånd en god förvaltning, lämpliga standarder och god praxis på cybersäkerhetsområdet. Denna dimension beaktar olika aspekter av cyberförsvar och motståndskraft samtidigt som den stödjer utvecklingen av den nationella cybersäkerhetsindustrin och bygger upp myndighetsförtroende.
- **(II) Kapacitetsuppbyggnad och medvetenhet**: Det här klustret bedömer medlemsstaternas förmåga att öka medvetenheten om cybersäkerhetsrisker och it-hot och hur de ska hanteras. Dessutom mäter denna dimension landets förmåga att kontinuerligt bygga upp cybersäkerhetskapacitet och öka den övergripande kunskaps- och kompetensnivån inom detta område. Den behandlar utvecklingen av marknaden för cybersäkerhet och framstegen inom forskning och utveckling på cybersäkerhetsområdet**.** Detta kluster omgrupperar alla mål och lägger grunden för att främja kapacitetsuppbyggnad.
- **(III) Lagstiftning och regelverk**: Detta kluster mäter medlemsstaternas förmåga att införa nödvändiga rättsliga och tillsynsmässiga instrument för att åtgärda och motverka den ökande it-brottsligheten och relaterade cyberincidenter och för att skydda kritisk informationsinfrastruktur. I denna dimension görs också en bedömning av medlemsstaternas förmåga att skapa en rättslig ram för att skydda medborgare och företag, till exempel vad gäller att balansera säkerhet med integritet.
- **(IV) Samarbete:** Detta kluster utvärderar samarbetet och informationsutbytet mellan olika intressegrupper på nationell och internationell nivå och är ett viktigt verktyg för att bättre förstå och svara upp mot en ständigt föränderlig hotmiljö.

De mål som har tagits med i modellen är de som medlemsstaterna vanligtvis antar och har valts ut bland de mål som anges i avsnitt 2.2. I modellen bedöms särskilt följande mål:

- 1. Utveckla nationella it-beredskapsplaner (I)
- 2. Fastställa grundläggande säkerhetsåtgärder (I)
- 3. Förstärka säkerheten på området digital identitet och bygga förtroende för offentliga digitala tjänster (I)
- 4. Inrätta kapacitet för hantering av cyberincidenter (II)
- 5. Öka användarnas medvetenhet (II)
- 6. Organisera cybersäkerhetsövningar (II)
- 7. Stärka kompetensutveckling och utbildningsprogram (II)
- 8. Främja FoU (II)
- 9. Ge den privata sektorn incitament att investera i säkerhetsåtgärder (II)
- 10. Förbättra cybersäkerheten i leveranskedjan (II)
- 11. Skydda kritisk datainfrastruktur samt leverantörer av samhällsviktiga tjänster och digitala tjänster (III)
- 12. Åtgärda cyberbrott (III)
- 13. Inrätta mekanismer för rapportering av incidenter (III)
- 14. Stärka integritet och dataskydd (III)
- 15. Institutionalisera samarbetet mellan offentliga organ (IV)
- 16. Deltaga i internationellt samarbete (IV)
- 17. Inrätta ett offentlig-privat partnerskap (IV)

De fyra klustren och de underliggande målen kombineras i modellen för att få en helhetssyn på mognaden i fråga om medlemsstaternas cybersäkerhetskapacitet. Diagram 1 visar den

övergripande strukturen för självutvärderingsramen och visar hur dessa faktorer, dvs. mål, kluster och självutvärderingsramen, är kopplade till utvärderingen av ett lands prestation.

Diagram 1: Ramstruktur för självutvärdering

För varje mål som ingår i självutvärderingsramen finns en rad indikatorer som är uppdelade efter de fem mognadsnivåerna. Varje indikator baseras på en ja/nej-fråga. Indikatorn kan utgöra ett krav eller ha statusen icke-obligatorisk.

3.4 POÄNGSÄTTNINGSMEKANISM

Poängsättningsmekanismen i självutvärderingsramen tar hänsyn till de ovannämnda delarna och de principer som anges i avsnitt 3.5. Modellen ger poäng baserat på två parametrar, **mognadsnivå** och **täckningsgrad**. Var och en av dessa parametrar kan beräknas på olika nivåer: i) per mål, ii) per målkluster eller iii) övergripande.

Resultat på objektiv nivå

Mognadsnivåpoängen ger en överblick över mognadsnivån genom att visa vilken kapacitet och praxis som införts. Mognadsnivåpoängen beräknas som den högsta nivå för vilken respondenten uppfyllde alla krav (dvs. ja-svar på alla obligatoriska frågor), förutom att ha uppfyllt alla krav för de tidigare mognadsnivåerna.

Täckningsgraden visar omfattningen av täckningen i fråga om alla indikatorer för vilka svaret är positivt, oavsett nivå. Det är ett kompletterande värde som tar hänsyn till alla indikatorer som mäter ett mål. Täckningsgraden beräknas som andelen mellan det totala antalet frågor inom målet och antalet frågor för vilka svaret är positivt.

Det är viktigt att klargöra att för resten av dokumentet används ordet ***poäng*** för att hänvisa både till värdena på mognadsnivån och täckningsgraden.

Figur 2 – Poängsättningsmekanism per mål ger en bild av den utvärderingsmekanism som beskrivs i avsnitt 3.1 och som vidareutvecklas nedan.

Diagram 2: Poängsättningsmekanism per mål

Diagram 2 visar ett exempel på hur mognadsnivån beräknas per mål. Det är värt att notera att respondenten uppfyllde de tre första mognadsnivåernas krav men endast delvis uppfyllde kraven i nivå 4. Därför visar poängen att ***respondentens mognadsnivå uppfyller nivå 3 för målet "Organisera cybersäkerhetsövning"****.*

I det exempel som visas i Diagram 2 kan dock inte målets mognadsnivå fånga upp informationen från de indikatorer som har ett positivt resultat och som ligger över mognadsnivå 3. I så fall kan täckningsgraden ge en överblick över alla de faktorer som respondenten genomförde för att uppnå detta mål, trots dess faktiska mognadsnivå. Förhållandet mellan det totala antalet frågor inom målet och antalet frågor för vilka svaret är positivt är då 19/27, dvs. ***täckningsgradens värde är 70 procent.***

För att anpassa sig till varje medlemsstats egenart och samtidigt möjliggöra en enhetlig överblick beräknas poängen utifrån två olika urval på klusternivå och övergripande nivå:

- **Allmänna poäng:** Ett fullständigt urval som omfattar alla de mål som ingår i klustret eller inom den övergripande ramen (1–17).
- **Specifika poäng:** Ett särskilt urval som endast omfattar de mål som valts ut av medlemsstaten (vanligtvis motsvarar de sådana mål som anges i det specifika landets nationella cybersäkerhetsstrategi) inom klustret eller inom den övergripande ramen.

Poäng på klusternivå

Den allmänna mognadsnivån för varje kluster beräknas som mognadsnivåns aritmetiska medelvärde för alla mål inom klustret.

Den **specifika mognadsnivån för varje kluster** beräknas som mognadsnivåns aritmetiska medelvärde för de mål inom klustret som medlemsstaten valde att bedöma (vanligtvis motsvarande de mål som anges i den nationella cybersäkerhetsstrategin i det specifika landet).

Diagram 1 visar exempelvis att kluster (I) Styrning och standarder för cybersäkerhet består av tre mål. Om man antar att respondenten valde att bedöma endast de två första målen, men inte

det tredje, och om man antar att de två första målen uppvisar en mognadsnivå på 2 respektive 4, är mognadsnivån för klustret med beaktande av alla målen nivå 2 (allmän mognadsnivå för kluster (I) = (2+4)/3), medan mognadsnivån för klustret med beaktande av endast de specifika mål som väljs av bedömaren motsvarar nivå 3 (specifik mognadsnivå för kluster (I) = (2+4)/2).

Den **allmänna täckningsgraden för varje kluster** beräknas som förhållandet mellan det totala antalet frågor inom klustret och antalet frågor för vilka svaret är positivt.

Den **specifika täckningsgraden för varje kluster** beräknas som förhållandet mellan det totala antalet frågor inom klustret som hänför sig till mål som medlemsstaten valt att bedöma (vanligtvis motsvarar de mål som anges i den nationella cybersäkerhetsstrategin i det specifika landet) och det antal frågor för vilka svaret är positivt.

Poäng på övergripande nivå

Ett lands övergripande allmänna mognadsnivå beräknas som det aritmetiska medelvärdet av mognadsnivån för alla 17 mål inom ramen.

Ett lands övergripande specifika mognadsnivå beräknas som mognadsnivåns aritmetiska medelvärde för de mål inom ramen som medlemsstaten valt att bedöma (vanligtvis motsvarande de mål som anges i den nationella cybersäkerhetsstrategin i det specifika landet).

Ett lands övergripande allmänna täckningsgrad beräknas som förhållandet mellan det totala antalet frågor inom alla de mål som ingår i ramen (1–17) och det antal frågor för vilka svaret är positivt.

Den **övergripande specifika täckningsgraden för ett land** beräknas som förhållandet mellan det totala antalet frågor inom ramen för de mål som medlemsstaten valt att bedöma (vanligtvis de mål som anges i den nationella cybersäkerhetsstrategin för landet i fråga) och det antal frågor för vilka svaret är positivt.

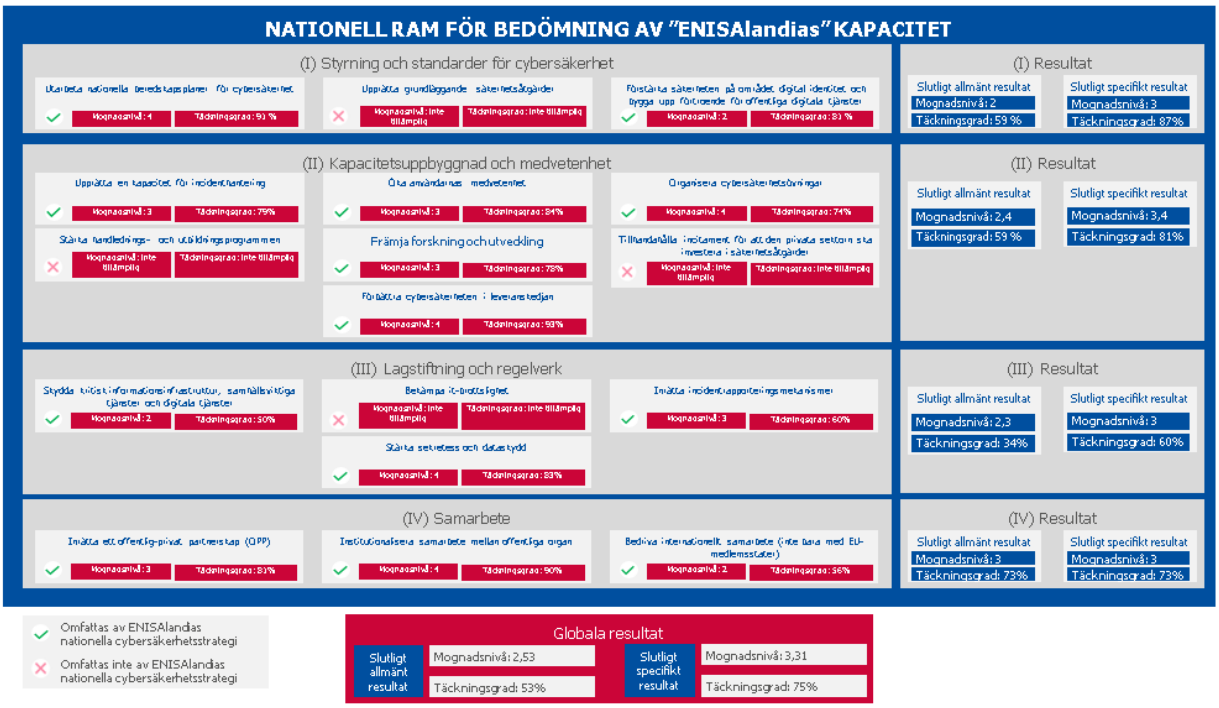
För varje indikator kan respondenterna välja ett tredje alternativ – ”vet inte/inte tillämpligt” – som svar. Om detta väljs utesluts indikatorn från den totala beräkningen av resultaten.

Mognadsnivåerna på klusternivå och övergripande nivå beräknas med ett aritmetiskt medelvärde för att visa framstegen mellan två bedömningar. Alternativet att beräkna klustret och den övergripande mognadsnivån som mognadsnivån för det minst mogna målet – även om det är relevant ur mognadssynpunkt – kan inte ta hänsyn till de framsteg som gjorts på områden som omfattas av andra mål.

Eftersom klusternivån och den övergripande nivån konsolideras för rapporteringsändamål har valet gjorts att använda det aritmetiska medelvärdet. För mer exakthet, använd poängen på objektiv nivå för rapporteringsändamål.

Bild 3 nedan sammanfattar poängsättningsmekanismerna för modellens olika nivåer (mål, kluster, övergripande).

Bild 3: Övergripande poängmekanism



3.5 KRAV PÅ SJÄLVUTVÄRDERINGSRAMEN

Den nationella ram för kapacitetsbedömning som presenteras i detta avsnitt grundar sig på de behov som framhålls av medlemsstaterna och bygger på ett antal krav, nämligen:

- Den nationella ramen för kapacitetsbedömning används frivilligt av medlemsstaten som en ram för självutvärdering.
- Den nationella ramen för kapacitetsbedömning syftar till att mäta medlemsstaternas cybersäkerhetskapacitet med avseende på de 17 målen. Medlemsstaten kan dock välja vilka mål den vill använda i sin bedömning och endast bedöma vissa av de 17 målen.
- Självutvärderingsramen syftar till att mäta mognadsgraden hos medlemsstatens cybersäkerhetskapacitet.
- Resultaten av bedömningen offentliggörs endast om medlemsstaten beslutar att göra det på eget initiativ.
- Medlemsstaten kan visa bedömningsresultaten genom att ange mognadsnivån för hela landets cybersäkerhetskapacitet, för ett kluster av mål eller för varje enskilt mål för sig.
- Alla utvärderade mål är lika relevanta inom ramen för bedömningen och har därför samma betydelse. Detsamma gäller de indikatorer som används inom systemet.
- Medlemsstaten kan följa sina framsteg över tid.

Självutvärderingsramen syftar till att stödja medlemsstaterna i uppbyggnaden av deras cybersäkerhetskapacitet och innehåller därför också en uppsättning rekommendationer eller riktlinjer för att vägleda de europeiska länderna när det gäller att förbättra deras mognadsnivå.

Anmärkning: Dessa rekommendationer eller riktlinjer är generella och bygger på Enisas publikationer och lärdomar från andra länder och kommer att baseras på resultatet av självutvärderingen.

4. INDIKATORER FÖR DEN NATIONELLA RAMEN FÖR KAPACITETSBEDÖMNING

4.1 RAMINDIKATORER

I detta avsnitt presenteras Enisas indikatorer för den nationella ramen för kapacitetsbedömning. Följande avsnitt är organiserade efter kluster.

För varje kluster presenteras i en tabell en omfattande uppsättning indikatorer i form av frågor som representerar en viss mognadsnivå. Frågeformuläret är det viktigaste instrumentet för självutvärderingen. För varje mål finns två uppsättningar indikatorer att notera:

- En uppsättning frågor om allmän strategimognad (nio allmänna frågor), markerade med ”a” till ”c” för varje mognadsnivå, upprepade för varje mål.
- En uppsättning frågor om cybersäkerhetskapacitet (319 frågor om cybersäkerhetskapacitet), numrerade från ”1” till ”10” för varje mognadsnivå, d'r frågorna är specifika för det område som målet täcker.

Varje fråga visas tillsammans med en etikett (0–1) som anger om frågan avser en obligatorisk indikator (1) eller en icke-obligatorisk indikator (0) för mognadsnivån.

Varje fråga kan identifieras med ett identifieringsnummer som består av

- målets nummer
- mognadsnivån och
- frågans nummer.

Exempelvis är fråga ID 1.2.4 den fjärde frågan på mognadsnivå 2 i det strategiska målet (I) ”Utarbeta nationella beredskapsplaner för cybersäkerhet”.

Det bör noteras att tillämpningsområdet för samtliga frågor i frågeformuläret är den nationella nivån om inget annat anges. I alla frågor hänvisar pronomenet ”ni” till medlemsstaten på ett allmänt sätt och inte till en enskild person eller till det statliga organ som utför bedömningen.

Definitionen av varje mål finns i kapitel 2.2 – Gemensamma mål som identifierats i nationella cybersäkerhetsstrategier i EU.

4.1.1 Kluster 1: Styrning och standarder för cybersäkerhet

Den nationella cybersäkerhetsstrategins mål	#	Nivå 1	R	Nivå 2	R	Nivå 3	R	Nivå 4	R	Nivå 5	R
1 – Utarbeta nationella it-beredskapsplaner	a	Behandlas målet i nuvarande nationella cybersäkerhetsstrategi eller planerar ni att behandla det i nästa version av strategin?	1	Finns det informella metoder eller aktiviteter som bidrar till att uppnå målet på ett icke samordnat sätt?	1	Finns det en handlingsplan som är formellt definierad och dokumenterad?	1	Granskar ni handlingsplanen avseende målet, för att testa dess resultat?	1	Finns det mekanismer på plats för att se till att handlingsplanen på ett dynamiskt sätt anpassas till omvärldsutvecklingen?	1
	b			Har ni definierat avsedda resultat, vägledande principer eller central verksamhet i er handlingsplan?	1	Finns det en handlingsplan med en tydlig resursfördelning och styrning?	1	Granskar ni handlingsplanen för att säkerställa att den är effektiv och har rätt prioritering?	1		
	c			Om det är relevant, genomförs er handlingsplan och är den redan i kraft i en begränsad omfattning?	0						
	1	Har ni börjat arbeta med att bygga nationella it-beredskapsplaner? Det kan till exempel handla om att ange allmänna mål, omfattningen och/eller principerna för beredskapsplanerna.	1	Finns det en doktrin eller nationell strategi som inbegriper cybersäkerhet som en krisfaktor (dvs. en plan, en politik etc.)?	1	Finns det en plan för cyberkrishantering på nationell nivå?	1	Är ni nöjda med antalet eller procentandelen kritiska sektorer som ingår i den nationella beredskapsplanen för cybersäkerhet?	1	Har ni en etablerad inlärningsprocess (dragna lärdomar) att tillämpa i samband med cybersäkerhetsövningar eller faktiska kriser på nationell nivå?	1
	2	Finns det en allmän insikt om att cyberincidenter utgör en krisfaktor som kan hota den nationella säkerheten?	0	Finns det ett nav för att sprida in information och underrätta beslutsfattare? ”Nav” syftar på alla metoder, plattformar eller platser som bidrar till att säkerställa att alla krishanteringsaktörer får tillgång till samma cyberkrisinformation i realtid.	1	Har nationella cyberkrisspecifika förfaranden fastställts?	1	Anordnar ni tillräckligt ofta aktiviteter (dvs. övningar) kopplade till nationell it-beredskapsplanering?	1	Finns det ett fastställt förfarande för att regelbundet testa den nationella planen?	1
	3	Har studier (tekniska, operativa, politiska) genomförts på området it-beredskapsplanering?	0	Har relevanta resurser avsatts för att övervaka utarbetandet och genomförandet av nationella beredskapsplaner för cybersäkerhet?	1	Finns det ett kommunikationsteam som är särskilt utbildat för att agera vid cyberkriser och informera allmänheten?	1	Finns det tillräckligt många som arbetar med krisplanering, som analyserar erfarenheter och lärdomar och genomför förändringar?	1	Finns det lämpliga verktyg och plattformar för att skapa situationsmedvetenhet?	1
	4	-		Finns det en metod för bedömning av cyberhot på nationell nivå som omfattar förfaranden för konsekvensbedömning?	0	Engagerar ni alla relevanta nationella intressenter (nationell säkerhet, försvar, civilskydd, brottsbekämpning, ministerier, myndigheter osv.)?	1	Finns det tillräckligt med utbildad personal som kan agera vid cyberkriser på nationell nivå?	1	Följer ni en specifik mognadsmodell för att övervaka och förbättra beredskapsplanen för cybersäkerhet?	0
	5	-		-		Finns det tillräckligt med lämpliga krishanteringsanläggningar och lägesrum?	1	-		Finns det resurser som är specialiserade på att förutse hot eller arbetar för att hantera framtida kriser eller morgondagens utmaningar i fråga om cybersäkerhet?	0

Den nationella cybersäkerhetsstrategins mål	#	Nivå 1	R	Nivå 2	R	Nivå 3	R	Nivå 4	R	Nivå 5	R
	6	-		-		Kontaktar ni internationella intressenter inom EU vid om så krävs?	0	-		-	
	7	-		-		Kontaktar ni internationella intressenter i länder utanför EU om så krävs?	0	-		-	
2 – Upprätta grundläggande säkerhetsåtgärder	a	Behandlas målet i nuvarande nationella cybersäkerhetsstrategi eller planerar ni att behandla det i nästa version av strategin?	1	Finns det informella metoder eller aktiviteter som bidrar till att uppnå målet på ett icke samordnat sätt?	1	Finns det en handlingsplan som är formellt definierad och dokumenterad?	1	Granskar ni handlingsplanen avseende målet, för att testa dess resultat?	1	Finns det mekanismer på plats för att se till att handlingsplanen på ett dynamiskt sätt anpassas till omvärldsutvecklingen?	1
	b			Har ni definierat avsedda resultat, vägledande principer eller central verksamhet i er handlingsplan?	1	Finns det en handlingsplan med en tydlig resursfördelning och styrning?	1	Granskar ni handlingsplanen för att säkerställa att den är effektiv och har rätt prioritering?	1		
	c			Om det är relevant, genomförs er handlingsplan och är den redan i kraft i en begränsad omfattning?	0						
	1	Har ni genomfört en undersökning för att identifiera krav och luckor för **offentliga** organisationer utifrån internationellt erkända standarder? Exempel: ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC, CIS m.fl.	1	Överensstämmer säkerhetsåtgärderna med internationella/nationella standarder?	1	Är grundläggande säkerhetsåtgärder obligatoriska?	1	Finns det en process för att ofta uppdatera grundläggande säkerhetsåtgärder?	1	Finns det en process för att förstärka IKT när incidenter inte åtgärdas genom insatserna?	1
	2	Har ni genomfört en undersökning för att identifiera krav och luckor för **privata** organisationer utifrån internationellt erkända standarder? Exempel: ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC, CIS m.fl.	1	Rådfrågas den privata sektorn och andra berörda parter vid fastställandet av grundläggande säkerhetsåtgärder?	1	Genomförs övergripande säkerhetsåtgärder inom kritiska sektorer?	1	Finns det någon övervakningsmekanism för att undersöka införandet av grundläggande säkerhetsåtgärder?	1	Utvärderar ni relevansen av nya standarder som tas fram som svar på den senaste utvecklingen av hotbilden?	1
	3	-		-		Genomför ni sektorsspecifika säkerhetsåtgärder inom kritiska sektorer?	1	Finns det någon nationell myndighet som kontrollerar om grundläggande säkerhetsåtgärder tillämpas eller inte?	1	Har eller främjar ni en nationell process för samordnad information om sårbarheter?	1

Den nationella cybersäkerhetsstrategins mål	#	Nivå 1	R	Nivå 2	R	Nivå 3	R	Nivå 4	R	Nivå 5	R
	4	-				Är de grundläggande säkerhetsåtgärderna förenliga med relevanta certifieringssystem?	1	Finns det en process på plats för att identifiera organisationer som inte uppfyller kraven inom en viss tidsperiod?	1	-	
	5	-		-		Finns det en självriskbedömningsprocess för grundläggande säkerhetsåtgärder?	1	Finns det en revisionsprocess på plats för att säkerställa att säkerhetsåtgärderna tillämpas korrekt?	1	-	
2 – Upprätta grundläggande säkerhetsåtgärder	6	-		-		Granskar ni obligatoriska grundläggande säkerhetsåtgärder i samband med statliga organs upphandlingsförfaranden?	0	Definierar eller uppmuntrar ni aktivt införandet av säkra standarder för utveckling av kritiska it-produkter eller driftstekniska produkter (medicinsk utrustning, anslutna och autonoma fordon, professionell radio, tung industriutrustning etc.)?	0	-	
3 – Förstärka säkerheten på området digital identitet och bygga förtroende för offentliga digitala tjänster	a	Behandlas målet i nuvarande nationella cybersäkerhetsstrategi eller planerar ni att behandla det i nästa upplaga?	1	Finns det informella metoder eller aktiviteter som bidrar till att uppnå målet på ett icke samordnat sätt?	1	Finns det en handlingsplan som är formellt definierad och dokumenterad?	1	Granskar ni handlingsplanen avseende målet, för att testa dess resultat?	1	Finns det mekanismer på plats för att se till att handlingsplanen på ett dynamiskt sätt anpassas till omvärldsutvecklingen?	1
	b			Har ni definierat avsedda resultat, vägledande principer eller central verksamhet i er handlingsplan?	1	Finns det en handlingsplan med en tydlig resursfördelning och styrning?	1	Granskar ni handlingsplanen för att säkerställa att den är effektiv och har rätt prioritering?	1		
	c			Om det är relevant, genomförs er handlingsplan och är den redan i kraft i en begränsad omfattning?	0						
	1	Har ni genomfört studier eller bristanalyser för att identifiera behovet av att säkra offentliga digitala tjänster till medborgare och företag?	1	Utför ni riskanalyser för att fastställa riskprofilen för tillgångarna eller tjänsterna innan ni flyttar dem till molnet eller inleder digitala omvandlingsprojekt?	1	Främjar ni inbyggda skyddsmekanismer för att skydda den personliga integriteten i alla e-förvaltningsprojekt?	1	Samlar ni in indikatorer på cybersäkerhetsincidenter som innebär intrång i offentliga digitala tjänster?	1	Deltar ni i europeiska arbetsgrupper för att upprätthålla standarder och/eller utforma nya krav för elektroniska betrodda tjänster (e-signaturer, e-sigill, e-registrerade leveranstjänster, tidsstämpling, webbplatsautentisering)? Exempel: ETSI/CEN/CENELEC, ISO, IETF, NIST, ITU.	1

Den nationella cybersäkerhetsstrategins mål	#	Nivå 1	R	Nivå 2	R	Nivå 3	R	Nivå 4	R	Nivå 5	R
3 – Förstärka säkerheten på området digital identitet och bygga förtroende för offentliga digitala tjänster	2	-		Finns det en strategi för att bygga upp eller främja säkra nationella system för elektronisk identifiering (eID) för medborgare och företag?	1	Inkluderar ni privata intressenter i utformningen och leveransen av säkra offentliga digitala tjänster?	1	Har ni infört ett system för ömsesidigt erkännande av metoder för e-identifiering med andra medlemsstater?	1	Medverkar ni aktivt i sakkunnigbedömningar (peer reviews) som en del av anmälan av system för elektronisk identifiering (eID) till Europeiska kommissionen?	1
	3	-		Finns det en strategi för att bygga upp eller främja säkra nationella elektroniska betrodda tjänster (e-signaturer, e-sigill, e-registrerade leveranstjänster, tidsstämpling, autentisering av webbplatser) för medborgare och företag?	1	Tillämpas en lägsta tillåtna gräns i fråga om säkerhetsnivå för offentliga digitala tjänster?	1	-		-	
	4	-		Finns det en strategi avseende dedikerade moln för myndighetsanvändning (en molnbaserad datastrategi riktad mot staten och offentliga organ som ministerier, statliga organ och offentliga förvaltningar) som inbegriper säkerhetsaspekter?	0	Finns det några system för elektronisk identifiering tillgängliga för medborgare och företag med en betydande eller hög säkerhetsnivå enligt definitionen i bilagan till förordning (EU) nr 910/2014 (eIDA-förordningen)?	1	-		-	
	5	-		-		Tillhandahåller ni offentliga digitala tjänster som kräver system för elektronisk identifiering med en betydande eller hög säkerhetsnivå enligt definitionen i bilagan till förordning (EU) nr 910/2014 (eIDA-förordningen)?	1	-		-	
	6	-		-		Har ni leverantörer av betrodda tjänster för medborgare och företag (e-signaturer, e-sigill, e-registrerade leveranstjänster, tidsstämpling, webbplatsautentisering)?	1	-		-	
	7	-		-		Främjar ni tillämpning av grundläggande säkerhetsåtgärder för all användning av molnbaserade modeller (t.ex. privata, offentliga, hybridvarianter, IaaS, PaaS, SaaS)?	0	-		-	

4.1.2 Kluster 2: Kapacitetsuppbyggnad och medvetenhet

Den nationella cybersäkerhetsstrategins mål	nr	Nivå 1	R	Nivå 2	R	Nivå 3	R	Nivå 4	R	Nivå 5	R
4 – Upprätta en kapacitet för incidenthantering	a	Behandlas målet i nuvarande nationella cybersäkerhetsstrategi eller planerar ni att behandla det i nästa upplaga?	1	Finns det informella metoder eller aktiviteter som bidrar till att uppnå målet på ett icke samordnat sätt?	1	Finns det en handlingsplan som är formellt definierad och dokumenterad?	1	Granskar ni handlingsplanen avseende målet, för att testa dess resultat?	1	Finns det mekanismer på plats för att se till att handlingsplanen på ett dynamiskt sätt anpassas till omvärldsutvecklingen?	1
	b			Har ni definierat avsedda resultat, vägledande principer eller central verksamhet i er handlingsplan?	1	Finns det en handlingsplan med en tydlig resursfördelning och styrning?	1	Granskar ni handlingsplanen för att säkerställa att den är effektiv och har rätt prioritering?	1		
	c			Om det är relevant, genomförs er handlingsplan och är den redan i kraft i en begränsad omfattning?	0						
	1	Har ni informell kapacitet för att hantera incidenter inom eller mellan den offentliga och den privata sektorn?	1	Finns det minst ett officiellt nationellt it-incidentcentrum (CSIRT) i landet?	1	Finns det kapacitet för att hantera incidenter inom de sektorer som anges i bilaga II till nätverks- och informationssäkerhetsdirektivet?	1	Har ni definierat och främjat standardiserade rutiner för incidenthanteringsförfaranden och klassificeringssystem för incidenter?	1	Finns det mekanismer på plats för tidig upptäckt, identifiering, förebyggande, hantering och begränsning av dag noll-sårbarhet?	1
	2	-		Har ert/era nationella it-incidentcentrum (CSIRT) ett tydligt definierat tillämpningsområde (till exempel beroende typ av sektor, typ av incident eller konsekvenserna av incidenten)?	1	Finns det någon mekanism för CSIRT-samarbete i ert land gällande svarsinsatser vid incidenter?	1	Utvärderar ni er insatsförmåga för att säkerställa att ni har tillräckliga resurser och färdigheter för att utföra de uppgifter som anges i punkt 2 i bilaga I till nätverks- och informationssäkerhetsdirektivet?	1	-	
	3	-		Har er/era nationella it-incidentcentrum (CSIRT) klart definierade relationer med andra nationella intressenter vad gäller den nationella cybersäkerhetsbilden och incidenthanteringspraxis (t.ex. brottsbekämpande myndigheter, försvaret, internetleverantörer, organ för cybersäkerhetsövervakning)?	0	Har ert/era nationella it-incidentcentrum (CSIRT) kapacitet för incidenthantering i enlighet med bilaga I till nätverks- och informationssäkerhetsdirektivet (NIS)? Det rör sig om aspekter som tillgänglighet, fysisk säkerhet, affärskontinuitet, internationellt samarbete, incidentövervakning, kapacitet för tidiga varningar, incidenthantering, riskanalys och situationsmedvetenhet, samarbete med den privata sektorn, standardpraxis.	1	-		-	
	4	-				Finns det någon samarbetsmekanism med grannländerna när det gäller incidenthantering?	1	-		-	

Den nationella cybersäkerhetsstrategins mål	nr	Nivå 1	R	Nivå 2	R	Nivå 3	R	Nivå 4	R	Nivå 5	R
4 – Upprätta en kapacitet för incidenthantering	5	-		-		Har ni formellt definierat tydliga riktlinjer och procedurer för incidenthanteringen?	1	-		-	
	6	-		-		Deltar ert/era nationella it-incidentcentrum (CSIRT) i cybersäkerhetsövningar på såväl nationell som internationell nivå?	1	-		-	
	7	-		-		Är ert/era nationella it-incidentcentrum (CSIRT) anslutna till FIRST (Forum of Incident Response and Security Teams)?	0	-		-	
5 – Öka användarmedvetenheten	a	Behandlas målet i nuvarande nationella cybersäkerhetsstrategi eller planerar ni att behandla det i nästa upplaga?	1	Finns det informella metoder eller aktiviteter som bidrar till att uppnå målet på ett icke samordnat sätt?	1	Finns det en handlingsplan som är formellt definierad och dokumenterad?	1	Granskar ni handlingsplanen avseende målet, för att testa dess resultat?	1	Finns det mekanismer på plats för att se till att handlingsplanen på ett dynamiskt sätt anpassas till omvärldsutvecklingen?	1
	b			Har ni definierat avsedda resultat, vägledande principer eller central verksamhet i er handlingsplan?	1	Finns det en handlingsplan med en tydlig resursfördelning och styrning?	1	Granskar ni handlingsplanen för att säkerställa att den är effektiv och har rätt prioritering?	1		
	c			Om det är relevant, genomförs er handlingsplan och är den redan i kraft i en begränsad omfattning?	0						
	1	Föreligger det något som helst erkännande från statligt håll, den privata sektorn eller användare om att det finns ett behov av att öka medvetenheten om cybersäkerhet och integritetsfrågor?	1	Har ni identifierat en specifik målgrupp för användarmedvetenhet? Exempel: allmänna användare, ungdomar, företagsanvändare (som kan delas upp ytterligare i små och medelstora företag, leverantörer av samhällsviktiga tjänster och av digitala tjänster etc.).	1	Har ni tagit fram kommunikationsplaner/en strategi för informationskampanjerna?	1	Tar ni fram statistik för att utvärdera er kampanj under planeringsstadiet?	1	Finns det mekanismer på plats för att säkerställa att informationskampanjer är kontinuerligt relevanta i fråga om tekniska framsteg, förändrad hotbild, rättsliga bestämmelser och nationella säkerhetsdirektiv?	1
	2	Genomför offentliga myndigheter informationskampanjer om cybersäkerhet inom sin organisation på ad hoc-basis, till exempel efter en cybersäkerhetsincident?	0	Tar ni fram projektplaner för att öka medvetenheten om informationssäkerhet och integritetsfrågor?	1	Finns det en process för att skapa innehåll på statlig nivå?	1	Utvärderar ni era kampanjer efter utrullningen?	1	Utför ni regelbundna utvärderingar eller studier för att mäta attitydförändringar eller beteendeförändringar i fråga om cybersäkerhet och integritetsfrågor inom såväl den privata som den offentliga sektorn?	1

Den nationella cybersäkerhetsstrategins mål	nr	Nivå 1	R	Nivå 2	R	Nivå 3	R	Nivå 4	R	Nivå 5	R
5 – Öka användarmedvetenheten	3	Genomför offentliga myndigheter informationskampanjer om cybersäkerhet riktade till allmänheten på ad hoc-basis, exempelvis efter en cybersäkerhetsincident?	0	Finns det resurser tillgängliga som är lätta att identifiera (t.ex. en gemensam onlineportal, informationspaket) för alla användare som vill utbilda sig inom cybersäkerhet och integritetsfrågor?	1	Har ni fastställda mekanismer för att identifiera målområden för att öka medvetenheten (t.ex. Enisa-hotbilder, nationella och internationella hotbilder, återkoppling från nationella cyberbrottscentrum)?	1	Finns det mekanismer på plats för att identifiera de mest relevanta medierna eller kommunikationskanalerna beroende på målgrupp för att maximera informationsspridning och engagemang? Exempel: olika typer av digitala medier, broschyrer, e-post, undervisningsmaterial, affischer på tättrafikerade platser, tv, radio.	1	Rådgör ni med beteendeexperter för att skräddarsy er kampanj för målgruppen?	1
	4	-		-		Sammanför ni intressenter med experter och kommunikationsteam för att skapa innehåll?	1			-	
	5	-		-		Involverar och engagerar ni den privata sektorn i era medvetandehöjande insatser för att främja och sprida budskapen till en bredare publik?	1	-		-	
	6	-		-		Förbereder ni särskilda initiativ för att öka medvetenheten bland chefer inom de offentliga, privata, akademiska eller civila sektorerna?	1	-		-	
	7	-		-		Deltar ni i Enisas kampanjer i samband med Europeiska informationssäkerhetsmånaden?	0	-		-	
6 – Organisera cybersäkerhetsövningar	a	Behandlas målet i nuvarande nationella cybersäkerhetsstrategi eller planerar ni att behandla det i nästa version av strategin?	1	Finns det informella metoder eller aktiviteter som bidrar till att uppnå målet på ett icke samordnat sätt?	1	Finns det en handlingsplan som är formellt definierad och dokumenterad?	1	Granskar ni handlingsplanen avseende målet, för att testa dess resultat?	1	Finns det mekanismer på plats för att se till att handlingsplanen på ett dynamiskt sätt anpassas till omvärldsutvecklingen?	1
	b			Har ni definierat avsedda resultat, vägledande principer eller central verksamhet i er handlingsplan?	1	Finns det en handlingsplan med en tydlig resursfördelning och styrning?	1	Granskar ni handlingsplanen för att säkerställa att den är effektiv och har rätt prioritering?	1		
	c			Om det är relevant, genomförs er handlingsplan och är den redan i kraft i en begränsad omfattning?	0						

Den nationella cybersäkerhetsstrategins mål	nr	Nivå 1	R	Nivå 2	R	Nivå 3	R	Nivå 4	R	Nivå 5	R
6 – Organisera cybersäkerhetsövningar	1	Genomför ni krisövningar på andra områden (utöver cybersäkerhet) på nationell eller europeisk nivå?	1	Har ni ett program för cybersäkerhetsövningar på nationell nivå?	1	Involverar ni alla relevanta myndigheter inom den offentliga förvaltningen? (även om scenariot är sektorsspecifikt)	1	Upprättar ni åtgärdsuppföljningsrapporter /utvärderingsrapporter?	1	Har ni en analyskapacitet rörande de lärdomar som dras i fråga om cyberteknik (rapporteringsprocesser, analys, skadebegränsning)?	1
	2	Har ni avsatt resurser för utformning och planering av krishanteringsövningar?	1	Genomförs eller prioriteras sådana övningar för cyberkrishantering som gäller viktiga samhällsfunktioner och kritisk infrastruktur?	1	Involverar ni den privata sektorn i planeringen och genomförandet av övningarna?	1	Testar ni nationella planer och rutiner?	1	Har ni en etablerad inlärningsprocess (för dragna lärdomar)?	1
	3	-		Har ni fastställt ett samordnande organ som ska övervaka utformningen och planeringen av cybersäkerhetsövningar (t.ex. en myndighet eller en konsultbyrå)?	0	Organiserar ni sektorsspecifika övningar på nationell och/eller internationell nivå?	1	Deltar ni i cybersäkerhetsövningar på europeisk nivå?	1	Anpassar ni övningsscenarierna utifrån den senaste utvecklingen (tekniska framsteg, globala konflikter, hotbild m.m.)?	1
	4	-		-		Anordnar ni övningar inom alla de kritiska sektorer som nämns i bilaga II till direktivet om nät- och informationssäkerhet (NIS-direktivet)?	1	-		Anpassar ni krishanteringsrutinerna efter andra medlemsstater för att säkerställa en effektiv krishantering på europeisk nivå?	1
	5	-		-		Anordnar ni intersektoriella och/eller tvärsektoriella cybersäkerhetsövningar?	1	-		Finns det en mekanism på plats för att snabbt anpassa strategin, planerna och förfarandena utifrån de lärdomar som dragits under övningarna?	0
	6	-		-		Organiseras cybersäkerhetsövningar som är specifika för de olika nivåerna? (Teknisk och operativ nivå, procedurnivå, beslutsnivå, politisk nivå etc.)	0	-		-	
7 – Stärka kompetensutveckling och utbildningsprogram	a	Behandlas målet i nuvarande nationella cybersäkerhetsstrategi eller planerar ni att behandla det i nästa upplaga?	1	Finns det informella metoder eller aktiviteter som bidrar till att uppnå målet på ett icke samordnat sätt?	1	Finns det en handlingsplan som är formellt definierad och dokumenterad?	1	Granskar ni handlingsplanen avseende målet, för att testa dess resultat?	1	Finns det mekanismer på plats för att se till att handlingsplanen på ett dynamiskt sätt anpassas till omvärldsutvecklingen?	1
	b			Har ni definierat avsedda resultat, vägledande principer eller central verksamhet i er handlingsplan?	1	Finns det en handlingsplan med en tydlig resursfördelning och styrning?	1	Granskar ni handlingsplanen för att säkerställa att den är effektiv och har rätt prioritering?	1		
	c			Om det är relevant, genomförs er handlingsplan och är den redan i kraft i en begränsad omfattning?	0						

Den nationella cybersäkerhetsstrategins mål	nr	Nivå 1	R	Nivå 2	R	Nivå 3	R	Nivå 4	R	Nivå 5	R
	1	Överväger ni att utveckla kompetens och utbildningsprogram för cybersäkerhet?	1	Anordnar ni kurser inriktade på cybersäkerhet?	1	Förmedlas det en cybersäkerhetskultur i ett tidigt skede av studenters utbildning i ert land? Främjas exempelvis cybersäkerhet som en del av högstadie- och gymnasieundervisningen?	1	Uppmanar ni personal inom den privata och offentliga sektorn att bli ackrediterad eller certifierad?	1	Finns det mekanismer på plats för att säkerställa att utbildningar och utbildningsprogram hela tiden är relevanta när det gäller den tekniska utvecklingen, hotbildsförändringar, rättsliga bestämmelser och nationella säkerhetsdirektiv?	1
	2	-		Erbjuder universiteten i ert land doktorsexamen i cybersäkerhet som en fristående disciplin och inte som ett datavetenskapsämne?	1	Finns det nationella forskningslaboratorier och läroanstalter som är specialiserade på cybersäkerhet?	1	Har ert land utvecklat utbildnings- eller mentorprogram inom cybersäkerhet för att stödja nationella nystartade företag och små och medelstora företag?	1	Har ni inrättat akademiska kompetenscentrum inom cybersäkerhet för användning som nav för forskning och utbildning?	1
	3	-		Planerar ni att utbilda utbildare, oberoende av deras område, i informationssäkerhet och integritetsfrågor? Det kan till exempel gälla onlinesäkerhet, skydd av personuppgifter, nätmobbning etc.	1	Uppmuntrar/finansierar ni särskilda cybersäkerhetskurser och utbildningsplaner för anställda vid medlemsstatens arbetsförmedlingar?	1	Främjar ni aktivt tillägg av informationssäkerhetskurser inom högre utbildning, inte bara för datavetenskapsstudenter utan även för andra specialinriktningar? Det kan till exempel gälla kurser som är anpassade efter ett yrkes särskilda behov.	1	Deltar akademiska institutioner i ledande internationella diskussioner på området för utbildning och forskning om cybersäkerhet?	0
	4	-		-		Finns det kurser i cybersäkerhet och/eller en specialiserad läroplan för nivå 5–8 i den europeiska referensramen för kvalifikationer?	1	Bedömer ni regelbundet kompetensbristen (bristen på cybersäkerhetspersonal) på området informationssäkerhet?	1	-	
	5	-		-		Uppmuntrar och/eller stödjer ni initiativ för att inkludera kurser i internetsäkerhet i grundskole- och gymnasieutbildning?	1	Främjar ni nätverk och informationsutbyte mellan akademiska institutioner på såväl nationell som internationell nivå?	1		

Den nationella cybersäkerhetsstrategins mål	nr	Nivå 1	R	Nivå 2	R	Nivå 3	R	Nivå 4	R	Nivå 5	R
7 - Stärka kompetensutveckling och utbildningsprogram	6	-		-		Finansierar eller erbjuder ni gratis grundläggande cybersäkerhetsutbildningar till medborgarna?	0	Engagerar ni den privata sektorn i någon form av utbildningsinitiativ inom cybersäkerhet? Exempel: kursutformning och leverans, praktikplatser, arbetspraktik.	1	-	
	7	-		-		Organiserar ni årliga informationssäkerhetseveneman g (t.ex. hackertävlingar eller hackaton)?	0	Genomför ni finansieringsmekanismer för att uppmuntra införandet av cybersäkerhetsexamina? Exempel: stipendier, garanterad lärlingsutbildning/praktik, garanterade arbetstillfällen inom en viss bransch eller befattning inom den offentliga sektorn.	0	-	
8 – Främjande av FoU	a	Behandlas målet i nuvarande nationella cybersäkerhetsstrategi eller planerar ni att behandla det i nästa upplaga?	1	Finns det informella metoder eller aktiviteter som bidrar till att uppnå målet på ett icke samordnat sätt?	1	Finns det en handlingsplan som är formellt definierad och dokumenterad?	1	Granskar ni handlingsplanen avseende målet, för att testa dess resultat?	1	Finns det mekanismer på plats för att se till att handlingsplanen på ett dynamiskt sätt anpassas till omvärldsutvecklingen?	1
	b			Har ni definierat avsedda resultat, vägledande principer eller central verksamhet i er handlingsplan?	1	Finns det en handlingsplan med en tydlig resursfördelning och styrning?	1	Granskar ni handlingsplanen för att säkerställa att den är effektiv och har rätt prioritering?	1		
	c			Om det är relevant, genomförs er handlingsplan och är den redan i kraft i en begränsad omfattning?	0						
	1	Har ni genomfört studier eller analyser för att identifiera FoU-prioriteringar inom cybersäkerhet?	1	Finns det en process för att definiera FoU-prioriteringar (t.ex. nya ämnesområden för att avskräcka, skydda, upptäcka och anpassa sig till nya typer av cyberattacker)?	1	Finns det någon plan för att koppla samman FoU-initiativ med realekonomi?	1	Är FoU-initiativen på cybersäkerhetsområdet förenliga med relevanta strategiska mål, t.ex. den digitala inre marknaden, Horisont 2020, en digital agenda för Europa och EU:s strategi för cybersäkerhet?	1	Samarbetar ni på nationell nivå med internationella FoU-initiativ som rör cybersäkerhet?	1
	2	-		Är den privata sektorn delaktig i fastställandet av FoU-prioriteringar?	1	Finns det några nationella projekt med anknytning till cybersäkerhet?	1	Finns det ett utvärderingssystem för FoU-initiativ?	1	Är FoU-prioriteringarna förenliga med gällande eller kommande lagstiftning (på nationell nivå)?	1

Den nationella cybersäkerhetsstrategins mål	nr	Nivå 1	R	Nivå 2	R	Nivå 3	R	Nivå 4	R	Nivå 5	R
8 – Främjande av forskning och utveckling	3	-		Är den akademiska världen delaktig i fastställandet av FoU-prioriteringar?	1	Finns det lokala/regionala ekosystem för nystart av företag och andra nätverkskanaler (t.ex. teknikparker, innovationskluster, nätverksevenemang/plattformar) för att främja innovation (även för nystartade cybersäkerhetsföretag)?	1	Finns det några samarbetsavtal med universitet och andra forskningsinstitutioner?	1	Deltar ni i framstående diskussioner på internationell nivå inom ett eller flera banbrytande FoU-områden?	0
	4	-		Finns det några nationella FoU-initiativ kopplade till cybersäkerhet?	0	Görs det investeringar i FoU-program för cybersäkerhet inom den akademiska världen och den privata sektorn?	1	Finns det ett erkänt institutionellt organ som övervakar FoU-verksamhet inom cybersäkerhet?	0	-	
	5	-		-		Finns det industriforskningsprofessurer vid universitet för att länka samman forskningsämnen och marknadsbehov?	1	-		-	
	6	-		-		Finns det särskilda FoU-finansieringsprogram för cybersäkerhet?	0	-		-	
9 – Tillhandahålla incitament för att den privata sektorn ska investera i säkerhetsåtgärder	a	Behandlas målet i nuvarande nationella cybersäkerhetsstrategi eller planerar ni att behandla det i nästa upplaga?	1	Finns det informella metoder eller aktiviteter som bidrar till att uppnå målet på ett icke samordnat sätt?	1	Finns det en handlingsplan som är formellt definierad och dokumenterad?	1	Granskar ni handlingsplanen avseende målet, för att testa dess resultat?	1	Finns det mekanismer på plats för att se till att handlingsplanen på ett dynamiskt sätt anpassas till omvärldsutvecklingen?	1
	b			Har ni definierat avsedda resultat, vägledande principer eller central verksamhet i er handlingsplan?	1	Finns det en handlingsplan med en tydlig resursfördelning och styrning?	1	Granskar ni handlingsplanen för att säkerställa att den är effektiv och har rätt prioritering?	1		
	c			Om det är relevant, genomförs er handlingsplan och är den redan i kraft i en begränsad omfattning?	0						
	1	Finns det någon näringslivspolitik eller politisk vilja att uppmuntra utvecklingen av cybersäkerhetsbranschen?	1	Är den privata sektorn involverad i utformningen av incitament?	1	Finns det ekonomiska/regleringsmässiga eller andra typer av incitament på plats för att främja investeringar i cybersäkerhet?	1	Finns det privata aktörer som reagerar på incitament genom att investera i säkerhetsåtgärder? Exempel: investerare som är specialiserade på cybersäkerhet och icke-specialiserade investerare.	1	Tillämpar ni riktade incitament för cybersäkerhet utifrån den aktuella hotutvecklingen?	1

Den nationella cybersäkerhetsstrategins mål	nr	Nivå 1	R	Nivå 2	R	Nivå 3	R	Nivå 4	R	Nivå 5	R
9 – Tillhandahålla incitament för att den privata sektorn ska investera i säkerhetsåtgärder	2	–		Har ni identifierat specifika cybersäkerhetsaspekter för vidare utveckling? Exempel: kryptografi, integritet, nya former av autentisering, AI tillämpad på cybersäkerhet.	0	Ger ni stöd (t.ex. skatteincitament) till nystartade cybersäkerhetsföretag och små och medelstora företag?	1	Ger ni incitament för att den privata sektorn ska fokusera på säkerheten i ny teknik? Exempel: 5G, artificiell intelligens, sakernas internet, kvantdatorer.	1	–	
	3	–		–		Tillhandahåller ni skatteincitament eller annan ekonomisk motivation för privata investerare i nystartade cybersäkerhetsföretag?	1	–		–	
	4	–		–		Underlättar ni tillträdet för nystartade cybersäkerhetsföretag och små och medelstora företag i den offentliga upphandlingsprocessen?	0	–		–	
	5	–		–		Finns det en budget för att stimulera den privata sektorn?	0	–		–	
10 – Förbättra cybersäkerheten i leveranskedjan	a	Behandlas målet i nuvarande nationella cybersäkerhetsstrategi eller planerar ni att behandla det i nästa upplaga?	1	Finns det informella metoder eller aktiviteter som bidrar till att uppnå målet på ett icke samordnat sätt?	1	Finns det en handlingsplan som är formellt definierad och dokumenterad?	1	Granskar ni handlingsplanen avseende målet, för att testa dess resultat?	1	Finns det mekanismer på plats för att se till att handlingsplanen på ett dynamiskt sätt anpassas till omvärldsutvecklingen?	1
	b			Har ni definierat avsedda resultat, vägledande principer eller central verksamhet i er handlingsplan?	1	Finns det en handlingsplan med en tydlig resursfördelning och styrning?	1	Granskar ni handlingsplanen för att säkerställa att den är effektiv och har rätt prioritering?	1		
	c			Om det är relevant, genomförs er handlingsplan och är den redan i kraft i en begränsad omfattning?	0						
	1	Har ni genomfört en studie om god säkerhetspraxis för hantering av leveranskedjan att använda vid upphandling inom olika industrisegment och/eller inom den offentliga sektorn?	1	Genomför ni cybersäkerhetsbedömningar i hela leveranskedjan för IKT-tjänster och IKT-produkter inom kritiska sektorer (enligt bilaga II till nätverks- och informationssäkerhetsdirektivet (2016/1148))?	1	Använder ni ett säkerhetscertifieringssystem för IKT-baserade produkter och tjänster? Exempel: SOG-IS MRA i Europa (Senior Officers Group for Information Systems' Security, Mutual Recognition Agreement), system för igenkänning av gemensamma kriterier (CCRA), nationella initiativ, sektorsinitiativ etc.	1	Finns en process för att uppdatera cybersäkerhetsbedömningarna av leveranskedjan för IKT-tjänster och IKT-produkter inom kritiska sektorer (enligt bilaga II till nätverks- och informationssäkerhetsdirektivet (2016/1148))?	1	Finns det detekteringssonder i leveranskedjans nyckelelement för att upptäcka tidiga tecken på säkerhetsproblem? Exempel: säkerhetskontroller på internetleverantörsnivå, säkerhetsdetektorer i större infrastrukturkomponenter etc.	1

Den nationella cybersäkerhetsstrategins mål	nr	Nivå 1	R	Nivå 2	R	Nivå 3	R	Nivå 4	R	Nivå 5	R
10 – Förbättra cybersäkerheten i leveranskedjan	2	-		Tillämpar ni standarder i samband med upphandlingspolicyer för offentliga förvaltningar när det gäller att säkerställa att leverantörer av IKT-produkter och IKT-tjänster uppfyller grundläggande informationssäkerhetskrav? Exempel: ISO/IEC 27001 och 27002, ISO/IEC 27036.	1	Främjar ni aktivt bästa praxis inom säkerhet och inbyggt integritetsskydd i samband med driftsättningen av IKT-produkter och utrullningen av IKT-tjänster? Exempel: säkra livscykler i samband med programvaruutveckling, och sakernas internet.	1	Finns det en process på plats för att identifiera svaga länkar i försörjningskedjan för kritiska sektorer (enligt bilaga II till nätverks- och informationssäkerhetsdirektivet (2016/1148))?	1	-	
	3	-		-		Utvecklar och tillhandahåller ni en centraliserad katalog med utökad information om befintliga standarder för informationssäkerhet och integritet som är skalbar för och tillämplig på små och medelstora företag?	1	Finns det mekanismer på plats för att säkerställa att IKT-produkter och IKT-tjänster som är kritiska, samhällsviktiga tjänster har cyberresiliens (dvs. förmåga att upprätthålla tillgänglighet och säkerhet vid en cyberincident)? Exempel: tester, regelbundna bedömningar, upptäckt av riskutsatta element.	1	-	
	4	-				Deltar ni aktivt i utformningen av EU:s certifieringsram för digitala IKT-produkter, IKT-tjänster och processer i enlighet med EU:s cybersäkerhetsakt (förordning (EU) 2019/881)? Exempel: deltagande i europeiska gruppen för cybersäkerhetscertifiering, främjande av tekniska standarder och förfaranden för IKT-produkters/IKT-tjänsters säkerhet.	0	Främjar ni utvecklingen av certifieringssystem riktade till små och medelstora företag för att främja införandet av standarder för informationssäkerhet och integritetsskydd?	0	-	
	5	-		-		Ger ni några typer av incitament för att hjälpa små och medelstora företag att införliva säkerhets- och integritetsstandarder?	0	Finns det bestämmelser på plats för att uppmuntra stora företag att öka cybersäkerheten för små företag i sina leveranskedjor? Exempel: cybersäkerhetsnav, utbildning och informationskampanjer.	0	-	

Den nationella cybersäkerhetsstrategins mål	nr	Nivå 1	R	Nivå 2	R	Nivå 3	R	Nivå 4	R	Nivå 5	R
	6	-		-		Uppmuntrar ni programvaruleverantörer att stödja små och medelstora företag genom att säkerställa säkra standardkonfigurationer i produkter som riktar sig till små organisationer?	0	-		-	

4.1.3 Kluster 3: Lagstiftning och regelverk

Den nationella cybersäkerhetsstrategins mål	#	Nivå 1	R	Nivå 2	R	Nivå 3	R	Nivå 4	R	Nivå 5	R
11 – Skydda kritisk informationsinfrastruktur, leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster	a	Behandlas målet i nuvarande nationella cybersäkerhetsstrategi eller planerar ni att behandla det i nästa upplaga?	1	Finns det informella metoder eller aktiviteter som bidrar till att uppnå målet på ett icke samordnat sätt?	1	Finns det en handlingsplan som är formellt definierad och dokumenterad?	1	Granskar ni handlingsplanen avseende målet, för att testa dess resultat?	1	Finns det mekanismer på plats för att se till att handlingsplanen på ett dynamiskt sätt anpassas till omvärldsutvecklingen?	1
	b			Har ni definierat avsedda resultat, vägledande principer eller central verksamhet i er handlingsplan?	1	Finns det en handlingsplan med en tydlig resursfördelning och styrning?	1	Granskar ni handlingsplanen för att säkerställa att den är effektiv och har rätt prioritering?	1		
	c			Om det är relevant, genomförs er handlingsplan och är den redan i kraft i en begränsad omfattning?	0						
	1	Finns det en allmän förståelse för att operatörer inom kritisk informationsinfrastruktur bidrar till den nationella säkerheten?	1	Finns det en fastställd metod för att identifiera samhällsviktiga tjänster?	1	Har ni genomfört nätverks- och informationssäkerhetsdirektivet (2016/1148)?	1	Finns det ett fastställt förfarande för att uppdatera riskregistret?	1	Upprättar och uppdaterar ni hotbildsrapporter?	1
	2	-		Finns det en metod för identifiering av kritisk informationsinfrastruktur?	1	Har ni genomfört direktiv 2008/114 om identifiering av, och klassificering som, europeisk kritisk infrastruktur och bedömning av behovet att stärka skyddet av denna?	1	Finns det andra fastställda mekanismer för att mäta om de tekniska och organisatoriska åtgärder som genomförs av leverantörer av samhällsviktiga tjänster är lämpliga för att hantera säkerhetsriskerna i nätverks- och informationssystem? Exempel: regelbundna cybersäkerhetsrevisioner, nationella ramar för genomförandet av standardåtgärder, tekniska verktyg som tillhandahålls av myndigheter, såsom detektionssonder eller systemspecifik konfigurationsöversyn.	1	Om den senaste utvecklingen av hotbilden kräver det, kan ni då ta med en ny sektor i er handlingsplan för kritisk informationsinfrastruktur?	1
	3	-		Finns det en metod för att identifiera leverantörer av samhällsviktiga tjänster?	1	Finns det ett nationellt register för identifierade leverantörer av samhällsviktiga tjänster för varje kritisk sektor?	1	Granskar och uppdaterar ni listan över identifierade leverantörer av samhällsviktiga tjänster minst vartannat år?	1	Om den senaste utvecklingen av hotbilden kräver det, kan ni då anpassa nya krav i er handlingsplan för kritisk informationsinfrastruktur?	1

Den nationella cybersäkerhetsstrategins mål	#	Nivå 1	R	Nivå 2	R	Nivå 3	R	Nivå 4	R	Nivå 5	R
11 – Skydda kritisk informationsinfrastruktur, leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster	4	-		Finns det fastställda metoder för att identifiera leverantörer av digitala tjänster?	1	Finns ett nationellt register över identifierade leverantörer av digitala tjänster?	1	Finns det andra fastställda mekanismer för att mäta om de tekniska och organisatoriska åtgärder som genomförs av leverantörer av digitala tjänster är lämpliga för att hantera riskerna för nätverks- och informationssystemens säkerhet? Exempel: regelbundna cybersäkerhetsrevisioner, nationella ramar för genomförandet av standardåtgärder, tekniska verktyg som tillhandahålls av myndigheter, såsom detektionssonder eller systemspecifik konfigurationsöversyn.	1	-	
	5	-		Finns det en eller flera nationella myndigheter som övervakar skyddet av kritisk informationsinfrastruktur och säkerheten i nät- och informationssystem? Exempel: i enlighet med NIS-direktivet (2016/1148).	1	Finns det ett nationellt riskregister för identifierade eller kända risker?	1	Granskar och uppdaterar ni listan över identifierade leverantörer av digitala tjänster minst vartannat år?	1	-	
	6	-		Utvecklar ni sektorsspecifika skyddsplaner? Detta kan inbegripa grundläggande cybersäkerhetsåtgärder (obligatoriska eller vägledande).	0	Finns det en metod för att kartlägga beroendeförhållanden när det gäller kritisk informationsinfrastruktur?	1	Använder ni ett säkerhetscertifieringssystem (nationellt eller internationellt) för att hjälpa leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster att identifiera säkra IKT-produkter? Exempel: SOG-IS MRA i Europa, nationella initiativ etc.	1	-	
	7	-		-		Använder ni riskhanteringspraxis för att identifiera, kvantifiera och hantera risker relaterade till kritisk informationsinfrastruktur på nationell nivå?	1	Använder ni ett säkerhetscertifieringssystem eller kvalificeringsförfarande för att bedöma tjänsteleverantörer som arbetar med samhällsviktiga tjänster? Exempel: tjänsteleverantörer inom området incidentdetektering, incidenthantering,	1	-	

Den nationella cybersäkerhetsstrategins mål	#	Nivå 1	R	Nivå 2	R	Nivå 3	R	Nivå 4	R	Nivå 5	R
								cybersäkerhetsrevision, molntjänster, smartkort etc.			
	8	-		-		Deltar ni i en samrådsprocess för att identifiera gränsöverskridande beroende?	1	Finns det mekanismer på plats för att mäta efterlevnadsnivån för leverantörer av samhällsnyttiga tjänster och av digitala tjänster när det gäller grundläggande cybersäkerhetsåtgärder?	0	-	
	9					Finns det en enda kontaktpunkt med ansvar för att samordna frågor som rör nät- och informationssystemens säkerhet på nationell nivå och gränsöverskridande samarbete på unionsnivå?	1	Finns det några åtgärder på plats för att säkerställa kontinuiteten i de tjänster på området kritisk informationsinfrastruktur som tillhandahålls? Exempel: förutseende av kriser, förfaranden för att återuppbygga kritiska informationssystem, affärskontinuitet utan it, säkerhetskopieringsförfaranden vid luftgap etc.	0		
11 – Skydda kritisk informationsinfrastruktur, leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster	10					Definierar ni grundläggande cybersäkerhetsåtgärder (obligatoriska eller vägledande) för leverantörer av digitala tjänster och alla sektorer som anges i bilaga II till nätverks- och informationssäkerhetsdirektivet (2016/1148)?	1				
	11	-		-		Tillhandahåller ni verktyg eller metoder för att upptäcka cyberincidenter?	1	-		-	
	a	Behandlas målet i nuvarande nationella cybersäkerhetsstrategi eller planerar ni att behandla det i nästa upplaga?	1	Finns det informella metoder eller aktiviteter som bidrar till att uppnå målet på ett icke samordnat sätt?	1	Finns det en handlingsplan som är formellt definierad och dokumenterad?	1	Granskar ni handlingsplanen avseende målet, för att testa dess resultat?	1	Finns det mekanismer på plats för att se till att handlingsplanen på ett dynamiskt sätt anpassas till omvärldsutvecklingen?	1
	b			Har ni definierat avsedda resultat, vägledande principer eller central verksamhet i er handlingsplan?	1	Finns det en handlingsplan med en tydlig resursfördelning och styrning?	1	Granskar ni handlingsplanen för att säkerställa att den är effektiv och har rätt prioritering?	1		
12 – Åtgärda it-brott	c			Om det är relevant, genomförs er handlingsplan och är den redan i kraft i en begränsad omfattning?	0						
	1	Har ni genomfört en undersökning för att identifiera krav i fråga om brottsbekämpning (t.ex. rättsliga grunder, resurser,	1	Överensstämmer er nationella rättsliga ram helt med EU:s relevanta rättsliga ram, inklusive direktiv 2013/40/EU om angrepp mot informationssystem?	1	Finns det enheter som är specialiserade på att hantera cyberbrottslighet vid åklagarmyndigheterna?	1	Samlas det in statistik i enlighet med bestämmelserna i artikel 14.1 i direktiv 2013/40/EU (direktivet om angrepp mot informationssystem)?	1	Erbjuder ni interinstitutionell utbildning eller utbildningsseminarier för brottsbekämpande myndigheter, domare, åklagare och	1

Den nationella cybersäkerhetsstrategins mål	#	Nivå 1	R	Nivå 2	R	Nivå 3	R	Nivå 4	R	Nivå 5	R
		kompetens) för att effektivt ta itu med it-brottslighet?		Exempel: olaglig tillgång till informationssystem, olaglig störning av informationssystem, olaglig datastörning, olaglig avlyssning, verktyg som används för att begå brott etc.						nationella/statliga CSIRT-enheter på nationell och/eller multilateral nivå?	
	2	Har ni genomfört en undersökning för att identifiera åklagares och domares krav (t.ex. rättsliga grunder, resurser, kompetens) för att effektivt ta itu med it-brottslighet?	1	Finns det någon lagfäst bestämmelse om identitetsstöld och stöld av personuppgifter online?	1	Har ni en ringmärkt budget för it-brottsenheter?	1	Samlar ni in särskild statistik om it-brottslighet? Exempel: operativ statistik, statistik över trender inom it-brottslighet, statistik över vinster från it-relaterad brottslighet och orsakade skador.	1	Deltar ni i samordnade åtgärder på internationell nivå för att störa kriminell verksamhet? Exempel: infiltration av kriminella hackningsforum, organiserade cyberbrottsgrupper, illegala marknader på darknet och undanröjning av botnät.	1
	3	Har ert land undertecknat Europarådets Budapestkonvention om it-brottslighet?	1	Finns det någon lagbestämmelse om intrång i immateriella rättigheter och upphovsrätt online?	1	Har ni inrättat ett centralt organ/en central enhet för att samordna verksamheten inom området för bekämpning av it-brottslighet?	1	Utvärderar ni lämpligheten i den utbildning som tillhandahålls brottsbekämpande myndigheter, rättsväsendet och nationell CSIRT-personal för att ta itu med it-brottslighet?	1	Görs det en tydlig åtskillnad mellan uppgifter från CSIRT-enheter, brottsbekämpande myndigheter respektive rättsväsendet (åklagare och domare) när de samarbetar för att bekämpa it-brottslighet?	1
	4			Finns det någon lagbestämmelse om trakasserier på nätet eller cybermobbning?	1	Har ni inrättat samarbetsmekanismer mellan relevanta nationella institutioner som är involverade i kampen mot it-brottslighet, inklusive nationella brottsbekämpande CSIRT-enheter?	1	Utför ni regelbundna utvärderingar för att säkerställa att ni har tillräckliga resurser (personal, budget och verktyg) avsedda för it-brottsenheter inom brottsbekämpande myndigheter?	1	Främjar landets regelverk samarbetet mellan CSIRT-enheter/brottsbekämpande myndigheter och rättsväsendet (åklagare och domare)?	1
12 – Bekämpa it-brottslighet	5			Finns det någon rättslig bestämmelse om datorrelaterade bedrägerier? Exempel: efterlevnad av bestämmelserna i Europarådets Budapestkonvention om it-brottslighet.	1	Samarbetar ni och delar ni information med andra medlemsstater när det gäller att bekämpa it-brottslighet?	1	Gör ni regelbundna utvärderingar för att säkerställa att ni har tillräckliga resurser (personal, budget och verktyg) avsedda för it-brottsenheter inom åklagarmyndigheten?	1	Deltar ni i uppbyggnaden och underhållet av standardiserade verktyg, metoder, formulär och förfaranden som ska delas med EU-intressenter (brottsbekämpande myndigheter, CSIRT-enheter, Enisa, Europols Europols it-brottscentrum (EC3) etc.)?	1
	6	-		Finns det någon lagbestämmelse om skydd av barn på nätet? Exempel: efterlevnad av bestämmelserna i direktiv 2011/93/EU och Europarådets Budapestkonvention om it-brottslighet.	1	Samarbetar och delar ni information med EU:s byråer (t.ex. Europols Europols it-brottscentrum EC3, Eurojust, Enisa) när det gäller att bekämpa it-brottslighet?	1	Finns det särskilda enhetsdomstolar eller domare som är specialiserade på att hantera cyberbrottsfall?	1	Finns det några avancerade mekanismer på plats för att avskräcka personer från att lockas till eller delta i cyberbrottslighet?	0

Den nationella cybersäkerhetsstrategins mål	#	Nivå 1	R	Nivå 2	R	Nivå 3	R	Nivå 4	R	Nivå 5	R
12 – Bekämpa it-brott	7	-		Har ni identifierat en operativ nationell kontaktpunkt för utbyte av information och för att besvara brådskande förfrågningar om information från andra medlemsstater om överträdelser enligt direktiv 2013/40/EU (direktivet om angrepp mot informationssystem)?	1	Finns det tillräckliga verktyg för att bekämpa it-brottslighet? Exempel: it-brottaxonomi och klassificering, verktyg för att samla in elektroniska bevis, kriminaltekniska datorverktyg, betrodda delningsplattformar.	1	Har ni infört åtgärder för att ge stöd och hjälp till offer för it-brott (allmänna användare, små och medelstora företag, stora företag)?	1	Använder ert land EU:s plan och/eller beredskapsprotokollet för EU:s brottsbekämpningsinsatser (EU LE ERP) för att agera effektivt vid storskaliga cyberincidenter?	0
	8			Ingår det en särskild enhet för it-brottslighet i er brottsbekämpande myndighet?	1	Finns det standardrutiner för att hantera e-bevis?	1	Har ni inrättat en interinstitutionell ram och samarbetsmekanismer mellan alla relevanta intressenter (t.ex. brottsbekämpande myndigheter, nationella CSIRT-enheter, rättsväsendet), inklusive den privata sektorn (t.ex. operatörer av viktiga tjänster, tjänsteleverantörer) där så är lämpligt, för att hantera cyberattacker?	1	-	
	9			Har ni, i enlighet med artikel 35 i Budapestkonventionen, utsett en kontaktpunkt som är nåbar dygnet runt, alla dagar i veckan?	1	Deltar ert land i utbildningsmöjligheter som erbjuds och/eller stöds av EU-organ (t.ex. Europol, Eurojust, Olaf, Cepol, Enisa)?	0	Underlättar ert regelverk samarbetet mellan CSIRT-enheter och brottsbekämpande myndigheter?	1	-	
	10	-		Har ni utsett en operativ nationell kontaktpunkt som är nåbar dygnet runt, året runt, för att hantera större it-attacker i samband med beredskapsprotokollet för EU:s brottsbekämpningsinsatser (EU LE ERP)?	1	Överväger ert land att anta det andra tilläggsprotokollet till Europarådets Budapestkonvention om it-brottslighet?	0	Finns det mekanismer på plats (t.ex. verktyg och förfaranden) för att underlätta informationsutbytet och samarbetet mellan CSIRT-enheter/brottsbekämpande myndigheter och eventuellt rättsväsendet (åklagare och domare) för att bekämpa it-brottslighet?	1	-	
	11			Tillhandahåller ni regelbunden specialiserad utbildning för intressenter som är involverade i att bekämpa it-brottslighet (brottsbekämpande myndigheter, rättsväsendet, CSIRT)? Exempel: utbildningar i arkivering/lagföring av it-relaterade brott, utbildning i insamling av elektroniska bevis	1						

Den nationella cybersäkerhetsstrategins mål	#	Nivå 1	R	Nivå 2	R	Nivå 3	R	Nivå 4	R	Nivå 5	R
				och säkerställande av integritet genom hela den digitala kedjan av förvaltning och datakriminalteknik.							
	12			Har ert land ratificerat eller anslutit sig till Europarådets Budapestkonvention om it-brottslighet?	1			-	-	-	
	13	-		Har ert land undertecknat och ratificerat tilläggsprotokollet (kriminalisering av rasistiska och främlingsfientliga handlingar som begås genom datorsystem) till Europarådets Budapestkonvention om it-brottslighet?	0	-	-	-		-	
13 – Inrätta mekanismer för incidentrapportering	a	Behandlas målet i nuvarande nationella cybersäkerhetsstrategi eller planerar ni att behandla det i nästa upplaga?	1	Finns det informella metoder eller aktiviteter som bidrar till att uppnå målet på ett icke samordnat sätt?	1	Finns det en handlingsplan som är formellt definierad och dokumenterad?	1	Granskar ni handlingsplanen avseende målet, för att testa dess resultat?	1	Finns det mekanismer på plats för att se till att handlingsplanen på ett dynamiskt sätt anpassas till omvärldsutvecklingen?	1
	b			Har ni definierat avsedda resultat, vägledande principer eller central verksamhet i er handlingsplan?	1	Finns det en handlingsplan med en tydlig resursfördelning och styrning?	1	Granskar ni handlingsplanen för att säkerställa att den är effektiv och har rätt prioritering?	1		
	c			Om det är relevant, genomförs er handlingsplan och är den redan i kraft i en begränsad omfattning?	0						
	1	Finns informella mekanismer för informationsutbyte om it-säkerhetincidenter mellan privata organisationer och nationella myndigheter?	1	Finns det ett system för rapportering av incidenter för alla sektorer enligt bilaga II till nätverks- och informationssäkerhetsdirektivet?	1	Finns det ett obligatoriskt incidentrapporteringssystem som fungerar i praktiken?	1	Finns det ett harmoniserat förfarande för sektorsspecifika system för rapportering av incidenter?	1	Skapar ni årliga incidentrapporter?	1

Den nationella cybersäkerhetsstrategins mål	#	Nivå 1	R	Nivå 2	R	Nivå 3	R	Nivå 4	R	Nivå 5	R
13 – Inrätta mekanismer för incidentrapportering	2	-		Har ni infört anmälningskraven för leverantörer av telekommunikationstjänster i enlighet med artikel 40 i direktivet (EU 2018/1972)? Enligt direktivet ska medlemsstaterna säkerställa att leverantörer av allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster utan onödigt dröjsmål underrättar den behöriga myndigheten om en säkerhetsincident som har haft en betydande inverkan på driften av nät eller tjänster.	1	Finns det en samordnings- eller samarbetsmekanism för incidentrapporteringsskyldigheter avseende dataskyddsförordningen, nätverks- och informationssäkerhetsdirektivet, artikel 40 (f.d. Artikel 13a) och eIDA-förordningen?	1	Finns det ett system för rapportering av incidenter för andra sektorer än de som omfattas av nätverks- och informationssäkerhetsdirektivet?	1	Görs det några hotbildsrapporter om cybersäkerhet eller andra typer av analyser som utarbetats av den enhet som tar emot incidentrapporterna?	1
	3	-		Har ni genomfört anmälningskraven för leverantörer av betrodda tjänster i enlighet med artikel 19 i eIDA-förordningen (förordning (EU) nr 910/2014)? I artikel 19 krävs det bland annat att tillhandahållare av betrodda tjänster underrättar tillsynsorganet om betydande incidenter eller överträdelser.	1	Finns tillräckliga verktyg för att säkerställa att information som delas via de olika rapporteringskanalerna förblir konfidentiell?	1	Mäter ni effektiviteten i incidentrapporteringsförfaranden ? Exempel: indikatorer på incidenter som har rapporterats via lämpliga kanaler, tidpunkten för incidentrapporten etc.	1	-	
	4	-		Har ni genomfört anmälningskraven för leverantörer av digitala tjänster i enlighet med artikel 16 i nätverks- och informationssäkerhetsdirektivet? Enligt artikel 16 ska leverantörer av digitala tjänster utan onödigt dröjsmål underrätta den behöriga myndigheten eller den nationella CSIRT-enheten om alla incidenter som har en väsentlig inverkan på tillhandahållandet av en tjänst som de erbjuder inom unionen, enligt bilaga III.	1	Finns det en plattform eller ett verktyg för att underlätta rapporteringsprocessen?	0	Finns det en gemensam taxonomi på nationell nivå för incidentklassificering och kategorier av grundläggande orsaker?	0	-	

Den nationella cybersäkerhetsstrategins mål	#	Nivå 1	R	Nivå 2	R	Nivå 3	R	Nivå 4	R	Nivå 5	R
14 – Stärka sekretess och dataskydd	a	Behandlas målet i nuvarande nationella cybersäkerhetsstrategi eller planerar ni att behandla det i nästa upplaga?	1	Finns det informella metoder eller aktiviteter som bidrar till att uppnå målet på ett icke samordnat sätt?	1	Finns det en handlingsplan som är formellt definierad och dokumenterad?	1	Granskar ni handlingsplanen avseende målet, för att testa dess resultat?	1	Finns det mekanismer på plats för att se till att handlingsplanen på ett dynamiskt sätt anpassas till omvärldsutvecklingen?	1
	b			Har ni definierat avsedda resultat, vägledande principer eller central verksamhet i er handlingsplan?	1	Finns det en handlingsplan med en tydlig resursfördelning och styrning?	1	Granskar ni handlingsplanen för att säkerställa att den är effektiv och har rätt prioritering?	1		
	c			Om det är relevant, genomförs er handlingsplan och är den redan i kraft i en begränsad omfattning?	0						
	1	Har ni genomfört studier eller analyser för att identifiera förbättringsområden för att bättre skydda medborgarnas privatliv?	1	Är den nationella dataskyddsmyndigheten involverad i frågor som rör cybersäkerhet (t.ex. utarbetande av nya lagar och förordningar om cybersäkerhet, fastställda minimiåtgärder för säkerhet)?	1	Främjar ni avsiktligt bästa praxis gällande säkerhetsåtgärder och dataskydd för den offentliga och/eller privata sektorn?	1	Gör ni regelbundna utvärderingar för att säkerställa att ni har tillräckliga resurser (personal, budget och verktyg) avsedda för dataskyddsmyndigheten?	1	Finns mekanismer på plats för att övervaka den senaste tekniska utvecklingen, i syfte att anpassa relevanta riktlinjer och lagbestämmelser/skyldigheter?	1
	2	Har ni utvecklat en rättslig grund på nationell nivå för att genomföra den allmänna dataskyddsförordningen (förordning EU nr 2016/679)? Exempel: anpassningar för att behålla eller införa mer specifika bestämmelser eller begränsningar i förhållande till kraven i förordningen.	0	-		Har ni infört medvetandehöjande åtgärder och utbildningsprogram kring detta ämne?	1	Uppmuntrar ni organisationer och företag att certifieras enligt ISO/IEC 27701:2019 beträffande hanteringssystem för personuppgifter (PIMS, Privacy Information Management Systems)?	1	Deltar eller främjar ni aktivt FoU-initiativ om integritetsfrämjande teknik?	0
	3	-		-		Samordnar ni era incidentrapporteringsrutiner med dataskyddsmyndigheten?	1	-		-	
	4	-		-		Främjar och stödjer ni utvecklingen av tekniska standarder för informationssäkerhet och integritet? Är de särskilt anpassade till små och medelstora företag?	0	-		-	

Den nationella cybersäkerhetsstrategins mål	#	Nivå 1	R	Nivå 2	R	Nivå 3	R	Nivå 4	R	Nivå 5	R
	5	-		-		Tillhandahåller ni praktiska och skalbara riktlinjer för att stödja olika typer av personuppgiftsansvariga när det gäller att uppfylla de rättsliga kraven och skyldigheterna i fråga om integritet och dataskydd?	0	-		-	

4.1.4 Kluster 4: Samarbete

Den nationella cybersäkerhetsstrategins mål	#	Nivå 1	R	Nivå 2	R	Nivå 3	R	Nivå 4	R	Nivå 5	R
15 – Inrätta ett offentlig-privat partnerskap (OPP)	a	Behandlas målet i nuvarande nationella cybersäkerhetsstrategi eller planerar ni att behandla det i nästa upplaga?	1	Finns det informella metoder eller aktiviteter som bidrar till att uppnå målet på ett icke samordnat sätt?	1	Finns det en handlingsplan som är formellt definierad och dokumenterad?	1	Granskar ni handlingsplanen avseende målet, för att testa dess resultat?	1	Finns det mekanismer på plats för att se till att handlingsplanen på ett dynamiskt sätt anpassas till omvärldsutvecklingen?	1
	b			Har ni definierat avsedda resultat, vägledande principer eller central verksamhet i er handlingsplan?	1	Finns det en handlingsplan med en tydlig resursfördelning och styrning?	1	Granskar ni handlingsplanen för att säkerställa att den är effektiv och har rätt prioritering?	1		
	c			Om det är relevant, genomförs er handlingsplan och är den redan i kraft i en begränsad omfattning?	0						
	1	Är det allmänt känt att offentlig-privata partnerskap på flera sätt bidrar till att höja nivån på cybersäkerheten i landet? Exempel: gemensamma intressen i tillväxten av cybersäkerhetsindustrin, samarbete för att bygga upp ett relevant regelverk för cybersäkerhet, främja FoU.	1	Finns det en nationell handlingsplan för att inrätta offentlig-privata partnerskap?	1	Har ni inrättat nationella offentlig-privata partnerskap?	1	Har ni inrättat sektorsövergripande offentlig-privata partnerskap?	1	Kan ni anpassa eller skapa offentlig-privata partnerskap beroende på hur den senaste tekniska och regleringsmässiga utvecklingen förändras?	1
	2	-		Fastställer ni en rättslig eller avtalsenlig grund (särskilda lagar, icke-spridningsavtal, immateriella rättigheter) för tillämpningsområdet för offentlig-privata partnerskap?	1	Har sektorsspecifika offentlig-privata partnerskap upprättats?	1	Fokuserar ni i de etablerade offentlig-privata partnerskapen också på samarbete inom den offentliga sektorn och samarbete mellan privata företag?	1		
	3	-		–		Tillhandahåller ni finansiering för inrättandet av offentlig-privata partnerskap?	1	Främjar ni offentlig-privata partnerskap bland små och medelstora företag?	1	-	

Den nationella cybersäkerhetsstrategins mål	#	Nivå 1	R	Nivå 2	R	Nivå 3	R	Nivå 4	R	Nivå 5	R
15 – Inrätta ett offentlig-privat partnerskap (OPP)	4	-		–		Leder offentliga institutioner som regel de offentlig-privata partnerskapen? Detta innebär att en gemensam kontaktpunkt inom den offentliga sektorn styr och samordnar offentlig-privata partnerskap och att offentliga organ i förväg kommer överens om vad de vill uppnå, med tydliga riktlinjer från offentliga förvaltningar om deras behov och begränsningar för den privata sektorn etc.	1	Mäter ni resultaten av offentlig-privata partnerskap?	1	-	
	5	-		–		Är ni medlem i i Europeiska cybersäkerhetsorganisationens (Ecso) avtalsbaserade offentlig-privata partnerskap?	0	-		-	
	6	-		-		Finns det ett eller flera offentlig-privata partnerskap som arbetar med CSIRT-verksamhet?	0	-		-	
	7					Finns det ett eller flera offentlig-privata partnerskap som arbetar med frågor som rör skydd av kritisk informationsinfrastruktur?	0				
	8	-		-		Finns det ett eller flera offentlig-privata partnerskap som arbetar med att öka medvetenheten om cybersäkerhet och kompetensutveckling?	0	-		-	
16 – Institutionalisera samarbete mellan offentliga organ	a	Behandlas målet i nuvarande nationella cybersäkerhetsstrategi eller planerar ni att behandla det i nästa upplaga?	1	Finns det informella metoder eller aktiviteter som bidrar till att uppnå målet på ett icke samordnat sätt?	1	Finns det en handlingsplan som är formellt definierad och dokumenterad?	1	Granskar ni handlingsplanen avseende målet, för att testa dess resultat?	1	Finns det mekanismer på plats för att se till att handlingsplanen på ett dynamiskt sätt anpassas till omvärldsutvecklingen?	1
	b			Har ni definierat avsedda resultat, vägledande principer eller central verksamhet i er handlingsplan?	1	Finns det en handlingsplan med en tydlig resursfördelning och styrning?	1	Granskar ni handlingsplanen för att säkerställa att den är effektiv och har rätt prioritering?	1		
	c			Om det är relevant, genomförs er handlingsplan och är den redan i kraft i en begränsad omfattning?	0						

Den nationella cybersäkerhetsstrategins mål	#	Nivå 1	R	Nivå 2	R	Nivå 3	R	Nivå 4	R	Nivå 5	R
	1	Finns det informella samarbetskanaler mellan offentliga myndigheter?	1	Finns det ett nationellt samarbetsprogram som är inriktat på cybersäkerhet? Exempel: rådgivande nämnder, styrgrupper, forum, råd, cybersäkerhetscentrum eller expertmötesgrupper.	1	Deltar offentliga myndigheter i samarbetsprogrammet?	1	Säkerställer ni att det åtminstone finns samarbetskanaler för cybersäkerhet mellan följande offentliga organ: underrättelsetjänster, nationella brottsbekämpande myndigheter, åklagarmyndigheter, statliga aktörer, nationella CSIRT-enheter och försvaret?	1	Får offentliga myndigheter enhetlig minimiinformation om den senaste utvecklingen av hotbilden och är den därmed medveten om det rådande cybersäkerhetsläget?	1
	2	-		-		Har ni inrättat samarbetsplattformar för informationsutbyte?	1	Mäter ni framgångarna och gränserna för de olika samarbetsprogrammen för att främja ett effektivt samarbete?	1	-	
16 – Institutionalisera samarbete mellan offentliga organ	3	-		-		Har ni definierat omfattningen av samarbetsplattformar (t.ex. uppgifter och ansvar, antal frågeområden)?	1	-		-	
	4	-		-		Organiserar ni årliga möten?	1	-		-	
	5	-		-		Finns det samarbetsmekanismer mellan behöriga myndigheter i olika geografiska regioner? Exempel: nätverk av säkerhetskorrespondenter per region, cybersäkerhetsansvarig i regionala ekonomiska kammare etc.	1	-		-	
17 – Bedriva internationellt samarbete (inte bara med EU:s medlemsstater)	a	Behandlas målet i nuvarande nationella cybersäkerhetsstrategi eller planerar ni att behandla det i nästa upplaga?	1	Finns det informella metoder eller aktiviteter som bidrar till att uppnå målet på ett icke samordnat sätt?	1	Finns det en handlingsplan som är formellt definierad och dokumenterad?	1	Granskar ni handlingsplanen avseende målet, för att testa dess resultat?	1	Finns det mekanismer på plats för att se till att handlingsplanen på ett dynamiskt sätt anpassas till omvärldsutvecklingen?	1
	b			Har ni definierat avsedda resultat, vägledande principer eller central verksamhet i er handlingsplan?	1	Finns det en handlingsplan med en tydlig resursfördelning och styrning?	1	Granskar ni handlingsplanen för att säkerställa att den är effektiv och har rätt prioritering?	1		
	c			Om det är relevant, genomförs er handlingsplan och är den redan i kraft i en begränsad omfattning?	0						

Den nationella cybersäkerhetsstrategins mål	#	Nivå 1	R	Nivå 2	R	Nivå 3	R	Nivå 4	R	Nivå 5	R
17 – Bedriva internationellt samarbete (inte bara med EU:s medlemsstater)	1	Har ni en strategi för internationellt samarbete?	1	Har ni samarbetsavtal med andra länder (bilaterala, multilaterala) eller partner i andra länder? Exempel: informationsutbyte, kapacitetsuppbyggnad, bistånd etc.	1	Utbyter ni information på strategisk nivå? Exempel: politik på hög nivå, riskuppfattning etc.	1	Är de nationella cybersäkerhetsmyndigheterna i ert land involverade i internationella samarbetsprogram?	1	Leder ni diskussioner på ett eller flera områden inom ramen för multilaterala avtal?	1
	2	Finns det informella samarbetskanaler med andra länder?	1	Har ni en gemensam kontaktpunkt som kan utgöra en kontaktfunktion för att säkerställa gränsöverskridande samarbete med medlemsstaternas olika myndigheter (samarbetsgruppen, CSIRT-nätverket etc.)?	1	Utbyter ni information på taktisk nivå? Exempel: hotbilder, centrum för informationsutbyte och analys (ISAC), taktiker, tekniker och procedurer (TTP).	1	Bedömer ni regelbundet resultaten av internationella samarbetsinitiativ?	1	Leder ni diskussioner på ett eller flera områden inom ramen för internationella fördrag eller konventioner?	1
	3	Har det offentliga ledarskapet uttryckt sin avsikt att inleda ett internationellt samarbete inom cybersäkerhetsområdet?	1	Har ni särskilt utsedda personer involverade i internationellt samarbete?	1	Utbyter ni information på operativ nivå? Exempel: operativ samordningsinformation, pågående incidenter, angreppsindikatorer (IOC).	1	-		Leder ni diskussioner eller förhandlingar inom ett eller flera områden inom ramen för internationella expertgrupper? Exempel: globala kommissionen för cyberrymdens stabilitet (GCSC), Enisas samarbetsgrupp för nät- och informationssäkerhet, FN:s grupp av statliga experter på informationssäkerhet (GGE).	1
	4	-		-		Deltar ni i internationella cybersäkerhetsövningar?	1	-		-	
	5	-		-		Deltar ni i internationella kapacitetsuppbyggnadsinitiativ? Exempel: utbildning, kompetensutveckling, utarbetande av standardrutiner.	0	-		-	
	6	-		-		Har ni upprättat avtal om ömsesidigt bistånd med andra länder? Exempel: brottsbekämpande myndigheters verksamhet, rättsliga förfaranden, ömsesidig incidenthanteringskapacitet, utbyte av cybersäkerhetstillgångar etc.	0	-		-	

Den nationella cybersäkerhetsstrategins mål	#	Nivå 1	R	Nivå 2	R	Nivå 3	R	Nivå 4	R	Nivå 5	R
	7	-		-		Har ni undertecknat eller ratificerat internationella fördrag eller konventioner på området cybersäkerhet? Exempel: Internationell uppförandekod för informationssäkerhet, konvention om it-brottslighet.	0	-		-	

4.2 RIKTLINJER FÖR ANVÄNDNING AV RAMVERKET

Syftet med detta avsnitt är att tillhandahålla medlemsstaterna riktlinjer och rekommendationer för att införliva ramen och för att fylla i frågeformuläret. Rekommendationerna nedan härrör huvudsakligen från den återkoppling som samlats in under intervjuerna med medlemsstaternas företrädare:

- **Föregripa samordningsaktiviteter för att samla in och konsolidera data.** De flesta medlemsstater bekräftar att en sådan självutvärdering bör ta cirka 15 persondagar. För att kunna utföra självutvärderingen måste ett stort antal olika intressenter anlitas. Det rekommenderas därför att avsätta tid för förberedelsefasen i syfte att identifiera alla relevanta intressenter inom statliga organ, offentliga organ och den privata sektorn.
- **Identifiera ett centralt organ med ansvar för att genomföra självutvärderingen på nationell nivå.** Eftersom många intressenter kan vara delaktiga i insamlingen av material för alla indikatorer i den nationella ramen för kapacitetsbedömning rekommenderas att ett centralt organ eller en central myndighet får i uppdrag att genomföra självutvärderingen genom att samarbeta och samordna med alla relevanta intressenter.
- **Använda utvärderingsinsatsen som ett sätt att dela information och kommunicera om cybersäkerhetsfrågor.** Erfarenheter som delats av medlemsstaterna visade att diskussioner (antingen i form av individuella intervjuer eller kollektiva seminarier) är ett bra tillfälle att främja dialog om cybersäkerhetsfrågor och att utbyta åsikter och identifiera förbättringsområden. Utöver att belysa viktiga prestationer kan utbyte av resultat också bidra till att främja cybersäkerhetsfrågorna.
- **Använd den nationella cybersäkerhetsstrategin som tillämpningsområde för att välja de mål som självutvärderingen ska gälla.** De 17 mål som ingår i den nationella ramen för kapacitetsbedömning har tagits fram med utgångspunkt i de mål som medlemsstaterna gemensamt täcker i sina nationella strategier för cybersäkerhet. De mål som omfattas av den nationella cybersäkerhetsstrategin bör användas som ett medel för att avgränsa utvärderingen. Den nationella cybersäkerhetsstrategin bör dock inte begränsa utvärderingen. Eftersom de nationella strategierna för cybersäkerhet inriktar sig på prioriteringar utelämnas vissa områden avsiktligt. Det innebär dock inte att en viss kapacitet saknas på dessa utelämnade områden. I de fall där ett specifikt mål utelämnas från den nationella cybersäkerhetsstrategin, men där landet har cybersäkerhetskapacitet med anknytning till målet i fråga, kan utvärderingen av det målet ske.
- **Säkerställa att poängtolkningen förblir förenlig med utvecklingen av den nationella cybersäkerhetsstrategin allteftersom dess tillämpningsområde förändras.** Livscykeln för en nationell cybersäkerhetsstrategi är flerårig. Vissa medlemsstaters nationella cybersäkerhetsstrategier genomförs som regel genom en 3–5 år lång färdplan med ändringar av tillämpningsområdet mellan två på varandra följande versioner av strategin. Därför måste man vara särskilt försiktig vid presentationen av resultaten av självutvärderingen mellan två versioner av strategin, då ändringar av omfattningen kan påverka den slutliga mognadspoängen. Det rekommenderas att poängen för alla ingående strategiska mål jämförs från ett år till ett annat (dvs. den övergripande, allmänna poängen).

Påminnelse om poängsättningsmekanismen – exempel på täckningsgrad
Poängsättningsmekanismen består av två poängnivåer:
(i) **En övergripande allmän täckningsgrad** på grundval av den fullständiga förteckningen över strategiska mål som ingår i självutvärderingsramen.
(ii) **En övergripande specifik täckningsgrad** baserad på strategiska mål som valts ut av medlemsstaten (vanligtvis de mål som landet valt i sin nationella cybersäkerhetsstrategi).

Mekanismen är utformad på så sätt (se avsnitt 3.1 om poängsättningsmekanismen) att den övergripande specifika täckningsgraden kommer att uppgå till eller vara högre än den

övergripande allmänna täckningsgraden, eftersom den senare kan omfatta mål som inte tas med av medlemsstaten, vilket sänker den övergripande allmänna täckningsgraden. När en medlemsstat lägger till ett nytt mål kommer den övergripande täckningsgraden att öka (dvs. fler mognadsindikatorer kommer att täckas), medan den övergripande specifika mognaden kan minska (om det nya målet är i ett inledningsskede och därmed har en låg mognadsnivå).

- **När ni fyller i frågeformuläret för självutvärdering, kom ihåg att det primära målet är att stödja medlemsstaterna i kapacitetsuppbyggnaden inom cybersäkerhet.** Även om det i vissa situationer kan vara svårt att besvara frågan på ett bestämt sätt vid ifyllandet av självutvärderingen rekommenderas att ni väljer det svar som är mest allmänt accepterat. Om svaret på en fråga till exempel är ”ja” till en viss omfattning men ”nej” till en annan bör medlemsstaterna komma ihåg att ett nej-svar kräver en åtgärd: antingen en korrigeringsplan eller en plan för att agera inom ett förbättringsområde som måste beaktas under framtida utvecklingsarbeten.

5. VÄGEN FRAMÅT

5.1 FRAMTIDA FÖRBÄTTRINGAR

Under intervjuer med medlemsstaternas företrädare och under skrivbordsundersökningsfasen identifierades också följande rekommendationer för att förbättra den nuvarande nationella ramen för kapacitetsbedömning och som potentiella framtida förbättringsområden:

- **Utveckla poängsystemet för att möjliggöra större noggrannhet.** Till exempel skulle en procentandel av täckningen kunna anges i stället för det binära svaret ja/nej, för att bättre beakta komplexiteten när det gäller att konsolidera kapaciteten på nationell nivå. Som ett första steg valdes ett enkelt tillvägagångssätt med ja/nej-svar.
- **Införa kvantitativa mått för att mäta effektiviteten i medlemsstaternas nationella cybersäkerhetsstrategier.** Den nationella ramen för kapacitetsbedömning är inriktad på att utvärdera mognadsnivån för medlemsstaternas cybersäkerhetskapacitet. Detta skulle kunna kompletteras med måttstockar för att mäta effektiviteten i den verksamhet och de handlingsplaner som medlemsstaterna genomför för att bygga upp denna kapacitet. Det föreföll inte realistiskt att bygga sådana effektivitetsmått i det nuvarande skedet med tanke på den knapphändiga återkopplingen från fältet, svårigheterna att hitta meningsfulla indikatorer som kopplar resultaten till genomförandet av den nationella cybersäkerhetsstrategin samt svårigheter att ta fram realistiska indikatorer för senare mätning. Detta är dock en fråga som kräver fortsatt framtida arbete.
- **Övergång från en självutvärdering till en bedömningsmetod.** En potentiell framtida utveckling av ramen skulle kunna vara övergången till en bedömningsmetod för att fastställa medlemsstaternas cybersäkerhetskapacitet på ett mer konsekvent sätt. Att låta en tredje part utföra bedömningen kan göra det möjligt att minimera potentiell brist på objektivitet.

BILAGA A – ÖVERSIKT ÖVER RESULTATET FRÅN SKRIVBORDSUNDERSÖKNINGEN

Bilaga A innehåller en sammanfattning av Enisas tidigare arbete med nationella cybersäkerhetsstrategier och en översyn av relevanta offentligt tillgängliga mognadsmodeller för cybersäkerhetskapacitet. Följande antaganden beaktas vid urval och översyn av modellerna:

- Det är inte alla modeller som bygger på en rigorös forskningsmetod.
- Modellernas struktur och resultat förklaras inte alltid grundligt med tydliga kopplingar mellan de olika faktorer som kännetecknar varje modell.
- Vissa modeller innehåller inga detaljerade uppgifter om utvecklingsprocessen, strukturen och bedömningsmetoden.
- Andra modeller och verktyg som vi hittade erbjuder inga detaljer om strukturen och innehållet och listas därför inte.
- Dessutom baseras valet av modeller för granskning på geografisk täckning. Fokus kommer i första hand att ligga på mognadsmodeller för cybersäkerhetskapacitet som byggts upp för att bedöma de europeiska ländernas resultat. Det är dock viktigt att utvidga den geografiska täckningen för att analysera god praxis vad gäller utbyggnaden av mognadsmodeller runt om i världen.

Denna systematiska översyn av relevanta offentligt tillgängliga mognadsmodeller för cybersäkerhetskapacitet genomfördes med hjälp av ett skräddarsytt analysramverk baserat på den metod som Becker definierat för utveckling av mognadsmodeller[22]. Följande faktorer analyserades för varje befintlig mognadsmodell:

- **Mognadsmodellens namn:** Mognadsmodellens namn och huvudreferenser.
- **Institution/källa:** Den offentliga eller privata institution som ansvarar för utformningen av modellen.
- **Allmänt syfte och mål:** Modellens övergripande räckvidd och avsedda mål.
- **Antal nivåer och dess definitioner:** Antal mognadsnivåer samt en allmän beskrivning av modellens mognadsnivåer.
- **Attributens nummer och namn:** Antal och namn på attribut som mognadsmodellen använder. Attributanalysen har följande tre syften:
  - Att dela upp mognadsmodellen i lättbegripliga avsnitt.
  - Att aggregera flera attribut i attributkluster som uppfyller samma mål.
  - Att ge olika perspektiv på föremålet för mognadsnivån.
- **Bedömningsmetod:** Bedömningsmetoden för mognadsmodellen.

[22] J. Becker, R. Knackstedt, och J. Pöppelbuß, ”Developing Maturity Models for IT Management: A Procedure Model and its Application,” Business & Information Systems Engineering, vol. 1, nr 3, s. 213–222, juni 2009.

- **Resultatrepresentation**: Definiera visualiseringsmetoden för mognadsmodellens resultat. Logiken bakom detta steg är att mognadsmodellerna tenderar att misslyckas om de är alltför komplexa. Därför måste representationssättet tillgodose praktiska behov.

Tidigare arbete med nationella cybersäkerhetsstrategier

Under 2012 offentliggjorde Enisa två dokument om nationella cybersäkerhetsstrategier som en del i sina tidiga insatser. För det första föreslogs i ”Practical guide on the development and execution phase of NCSS” (praktisk vägledning om utvecklings- och genomförandefasen för nationella cybersäkerhetsstrategier[23] flera konkreta åtgärder för ett effektivt genomförande av den nationella cybersäkerhetsstrategin, där dess livscykel presenteras i fyra faser: strategiutveckling, strategigenomförande, strategiutvärdering och strategiunderhåll. För det andra redogjordes det kortfattat för cybersäkerhetsstrategiernas status 2012 inom och utanför EU, i ett dokument med titeln ”Setting the course for national efforts to strengthen security in cyberspace” (färdplan för nationella insatser i syfte att förstärka cybersäkerheten)[24]. I detta föreslogs att medlemsstaterna skulle fastställa gemensamma temaområden och skillnader mellan sina nationella cybersäkerhetsstrategier.

År 2014 offentliggjorde Enisas sin första ram för utvärdering av medlemsstaters nationella cybersäkerhetsstrategier[25]. Denna ram innehåller rekommendationer och exempel på god praxis samt verktyg för kapacitetsuppbyggnad för att utvärdera nationella cybersäkerhetsstrategier (t.ex. identifierade mål, indata, utdata, centrala resultatindikatorer etc.). Dessa verktyg är anpassade till de olika behoven i länder med olika mognadsnivå i sin strategiska planering. Samma år offentliggjorde Enisa ”Interaktiv onlinekarta över nationella cybersäkerhetsstrategier”[26], som gör det möjligt för användare att snabbt ta del av alla medlemsstaters och Eftaländers nationella cybersäkerhetsstrategier, inklusive deras strategiska mål och exempel på god praxis i genomförandet. Kartans förlaga var en katalog som utkom 2014 och som uppdaterades med exempel på genomförande 2018. Sedan 2019 fungerar den som ett informationsnav för att centralisera uppgifter från medlemsstaterna om deras insatser för att förbättra den nationella cybersäkerheten.

I ”NCSS Good Practice Guide” (vägledning för bästa praxis i fråga om nationella cybersäkerhetsstrategier)[27], som offentliggjordes 2016, fastställs 15 strategiska mål. I denna vägledning analyseras också genomförandestatusen för varje medlemsstats cybersäkerhetsstrategi och olika luckor och utmaningar identifieras i fråga om genomförandet.

År 2018 offentliggjorde Enisa ”National Cybersecurity Strategies Evaluation Tool” (utvärderingsverktyg för nationella cybersäkerhetsstrategier)[28]. Detta är ett interaktivt

[23] NCSS: Practical Guide on Development and Execution (Enisa, 2012)
https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
[24] NCSS: Setting the course for national efforts to strengthen security in cyberspace (Enisa, 2012)
https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
[25] An evaluation framework for NCSS (Enisa, 2014)
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
[26] National Cybersecurity Strategies – Interactive Map (Enisa, 2014, uppdaterad 2019)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[27] Detta dokument är en uppdaterad version av 2012 års vägledning: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide
[28] National Cybersecurity Strategies Evaluation Tool (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

självutvärderingsverktyg som syftar till att hjälpa medlemsstaterna att utvärdera sina strategiska prioriteringar och de mål som är kopplade till de nationella cybersäkerhetsstrategierna. Genom en rad enkla frågor ger detta verktyg medlemsstaterna specifika rekommendationer för genomförandet av varje mål. Slutligen presenteras i “Good practices in innovation on Cybersecurity under the NCSS” (bästa praxis för innovation inom cybersäkerhet inom ramen för nationella cybersäkerhetsstrategier)[29], som offentliggjordes 2019, frågan om innovation på cybersäkerhetsområdet inom ramen för nationella cybersäkerhetsstrategier. I det här dokumentet beskrivs utmaningar och god praxis för de olika innovationsdimensionerna, såsom de uppfattas av ämnesexperter, för att underlätta utarbetandet av innovativa strategiska mål i framtiden.

A.1 Mognadsmodell för nationell cybersäkerhetskapacitet (CMM)

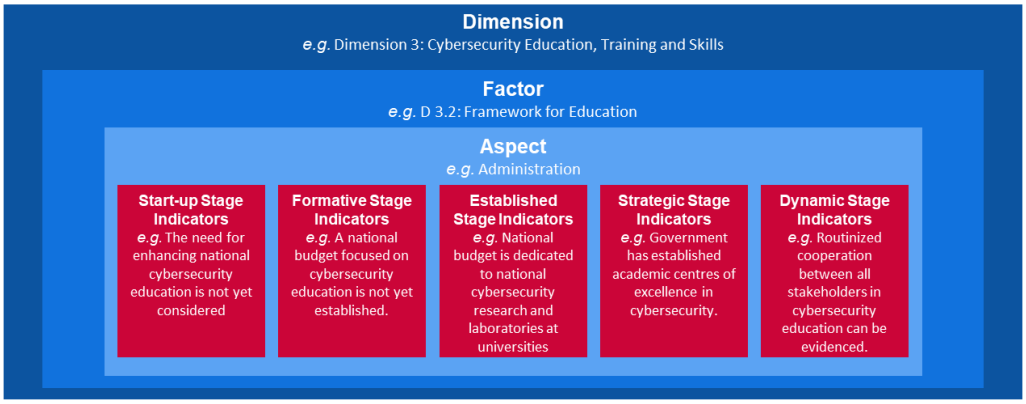
Mognadsmodellen för nationell cybersäkerhetskapacitet (CMM) har utvecklats av Global Cyber Security Capacity Centre (kapacitetscentrumet för global cybersäkerhet), som är en del av Oxford Martin School vid universitet i Oxford. Kapacitetscentrumet har som mål att öka kapacitetsuppbyggnadens omfattning och effektivitet i fråga om cybersäkerhet både i Storbritannien och internationellt, genom att införa mognadsmodellen för cybersäkerhetskapacitet (CMM). CMM riktar sig direkt till länder som vill utöka sin nationella cybersäkerhetskapacitet. CMM, som ursprungligen infördes 2014, reviderades 2016 efter att ha använts i översynen av elva nationella cybersäkerhetskapaciteter.

Attribut och dimensioner

CMM anser att cybersäkerhetskapaciteten består av **fem dimensioner** som speglas genom olika kluster av cybersäkerhetskapacitet. Varje kluster representerar en s.k. ”lins” (lens) genom vilken cybersäkerhetskapacitet kan undersökas och förstås. Inom de fem dimensionerna beskriver de olika **faktorerna** detaljerna med att inneha cybersäkerhetskapaciteten. Dessa detaljer är delar som bidrar till att öka cybersäkerhetskapaciteten inom varje dimension. För varje faktor finns ett flertal **aspekter** som återger olika delar av faktorn. Aspekterna representerar en organisatorisk metod för att dela upp indikatorer i mindre kluster som är lättare att förstå. Varje aspekt utvärderas sedan genom **indikatorer** för att beskriva de steg, åtgärder eller byggstenar som är indikativa för ett visst mognadsstadium (detta definieras i nästa avsnitt) inom en viss aspekt, faktor och dimension.

De termer som nämns ovan kan skiktas enligt bilden nedan.

Bild 4: CMM-indikatorer



[29] https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1

Dimension e.g. Dimension 3: Cybersecurity Education, Training and Skills	Dimension t.ex. dimension 3: Utbildning och färdigheter inom cybersäkerhet
Factor e.g. D 3.2: Framework for Education	Faktor t.ex. D 3.2: Ramverk för utbildning
Aspect e.g. Administration	Aspekt t.ex. administration
Start-up Stage Indicators e.g. The for enhancing national cybersecurity education is not yet considered	Indikatorer för uppstartsstadiet, t.ex. ”att förbättra den nationella cybersäkerhetsutbildningen har ännu inte beaktats”
Formative Stage Indictors e.g. A national budget focused on cybersecurity education is not yet established	Indikatorer avseende formativa stadier t.ex. ”en nationell budget inriktad på utbildning i cybersäkerhet har ännu inte fastställts”
Established Stage Indicators e.g. National budget is dedicated to national cybersecurity research and laboratories at universities	Indikatorer avseende etablerade stadier t.ex. ”en nationell budget är avsedd för nationell cybersäkerhetsforskning och universitetslaboratorier”
Strategic Stage Indicators e.g. Government has established academic center of excellence in cybersecurity education can be evidenced.	Indikatorer avseende strategiska stadier t.ex. ”regeringens etablerande av ett akademiskt centrum för spetskompetens inom cybersäkerhetsutbildning kan påvisas”
Dynamic Stage Indicators e.g. Routinized cooperation between all stakeholder	Indikatorer avseende dynamiska stadier t.ex. ”rutinmässigt samarbete mellan alla berörda parter”

De fem dimensionerna beskrivs nedan:

i Utforma strategier och politik för cybersäkerhet (6 faktorer).
ii Uppmuntra en ansvarsfull cybersäkerhetskultur i samhället (5 faktorer).
iii Utveckla kunskaper om cybersäkerhet (3 faktorer).
iv Skapa effektiva rättsliga ramar (3 faktorer).
v Kontrollera risker genom standarder, organisationer och tekniker (7 faktorer).

Mognadsnivåer

I CMM används **fem mognadsnivåer** för att avgöra i vilken utsträckning ett land har gjort framsteg i förhållande till en viss faktor/aspekt av cybersäkerhetskapaciteten. Dessa nivåer utgör ögonblicksbilder av den befintliga cybersäkerhetskapaciteten:

- **Uppstartsstadium:** I detta skede har cybersäkerheten ännu inte mognat eller så är den mycket outvecklad. Det kan förekomma inledande diskussioner om kapacitetsuppbyggnad inom cybersäkerhet, men inga konkreta åtgärder har ännu vidtagits. Det saknas observerbara bevis i detta skede.
- **Formativt stadium:** Vissa aspektinslag har börjat växa fram och formuleras men kan fortfarande vara tillfälliga, oorganiserade, illa definierade eller helt enkelt ”nya”. Bevis för denna verksamhet kan dock tydligt påvisas.
- **Etablerat stadium:** Aspekternas olika delar är på plats och fungerar. Det tas dock ingen väl genomtänkt hänsyn till den relativa fördelningen av resurser. Det har inte gjorts någon större avvägning i beslutsfattandet när det gäller de ”relativa” investeringarna i de olika delarna av aspekten. Aspekten är dock funktionell och definierad.
- **Strategiskt stadium:** Val har gjorts avseende vilka delar av aspekten som är viktiga och vilka som är mindre viktiga för den aktuella organisationen eller det aktuella landet.

Det strategiska stadiet återspeglar det faktum att dessa val har gjorts villkorat på landets eller organisationens särskilda omständigheter.

- **Dynamiskt stadium:** I detta skede finns det tydliga mekanismer för att ändra strategin beroende på de rådande omständigheterna, såsom den aktuella hotbildens teknik, globala konflikter eller en betydande förändring inom ett problemområde (t.ex. it-brottslighet eller integritet). Dynamiska organisationer har utvecklat metoder för att stegvis förändra strategier. Snabba beslut, omfördelning av resurser och ständig uppmärksamhet på den föränderliga omvärlden utmärker detta skede.

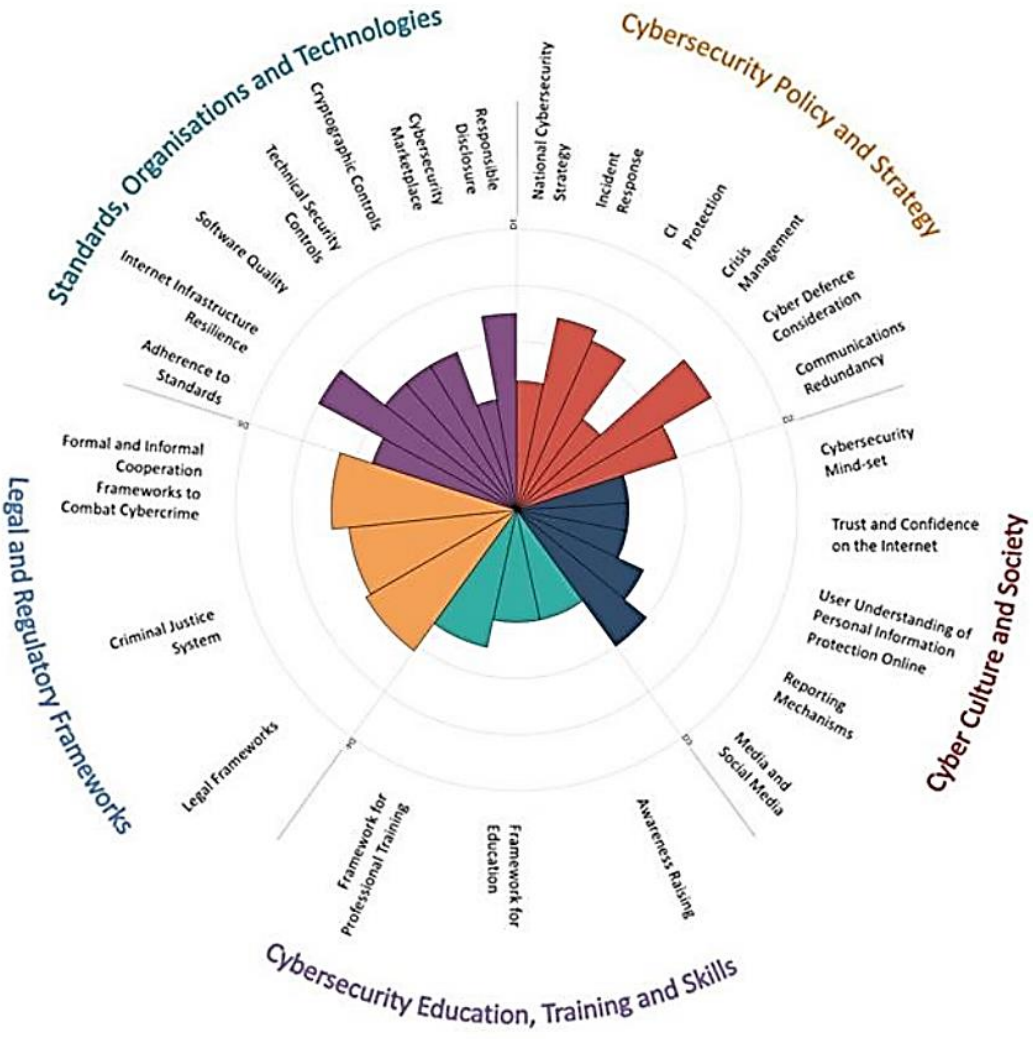
Bedömningsmetod

Eftersom kapacitetscentrumet (Capacity Centre) inte har en grundlig och djupgående förståelse för varje inhemskt sammanhang i vilket modellen ska användas, arbetar det tillsammans med internationella organisationer, värdministerier eller organisationer i respektive land för att se över mognaden för cybersäkerhetskapaciteten. För att bedöma mognadsnivån för de fem dimensioner som ingår i CMM träffar kapacitetscentrumet och värdorganisationen relevanta nationella intressenter inom den offentliga och privata sektorn under två eller tre dagar för att anordna fokusgrupper om CMM:s dimensioner. Varje dimension diskuteras vid minst två tillfällen av olika intressegrupper. Detta utgör den preliminära datapoolen för den efterföljande bedömningen.

Modus eller återgivning av resultaten

CCM ger en översikt över varje lands mognadsnivå genom en ”radar” som består av fem sektioner, en för varje dimension. Varje dimension utgör en femtedel av bilden och de fem mognadsstadierna för varje faktor sträcker sig utåt från bildens mitt enligt bilden nedan. Nivån ”uppstart” är närmast mitten, medan nivån ”dynamisk” återfinns längst ut på kanten.

Bild 5 CMM: Resultatöversikt



Standards, Organisations and Technologies	Standarder, organisationer och teknik
Legal Regulatory Frameworks	Lagstiftningsramar
Cybersecurity Education, Training and Skills	Utbildning och färdigheter inom cybersäkerhet
Cybersecurity Policy and Strategy	Politik och strategier för cybersäkerhet
Cyber Culture and Society	Cybersäkerhet i kultur och samhälle
Responsible Disclosure	Ansvarsfullt utlämnande av uppgifter
Cybersecurity market place	Marknadsplats för cybersäkerhet
Cryptographic Controls	Kryptografiska kontroller
Technical Security Controls	Tekniska säkerhetskontroller
Software Quality	Mjukvarukvalitet
Internet Infrastructure Resilience	Internetinfrastrukturens motståndskraft
Adherence to Standards	Efterlevnad av standarder
Formal and Informal Cooperation Frameworks to Combat Cybercrime	Formella och informella samarbetsramar för bekämpning av it-brottslighet
Criminal Justice System	Det straffrättsliga systemet
Legal Frameworks	Rättsliga ramar
Framework for Professional Training	Ramverk för yrkesutbildning
Framework for Education	Ramverk för utbildning
Awareness Raising	Medvetandehöjande åtgärder
Media and Social Medai	Medier och sociala medier
Reporting Mechanisms	Rapporteringsmekanismer
User Understanding of Personal Information Protection Online	Användarförståelse för skydd av personuppgifter online
Trust and Confidence on the Internet	Förtroende och säkerhet på internet
Cybersecurity Mind-set	Att tänka i termer av cybersäkerhet
Communications Redundancy	Kommunikationsredundans
Cyber Defence Consideration	Överväganden vid it-försvar

Crisis Management	Krishantering
CI Protection	Skydd av kritisk infrastruktur
Incident Response	Incidenthantering
National Cybersecurity Strategy	Nationell strategi för cybersäkerhet

Global Cyber Security Capacity Centre, Oxford Martin School, University of Oxford, 2017.

A.2 Mognadsmodell för cybersäkerhetskapacitet (C2M2)

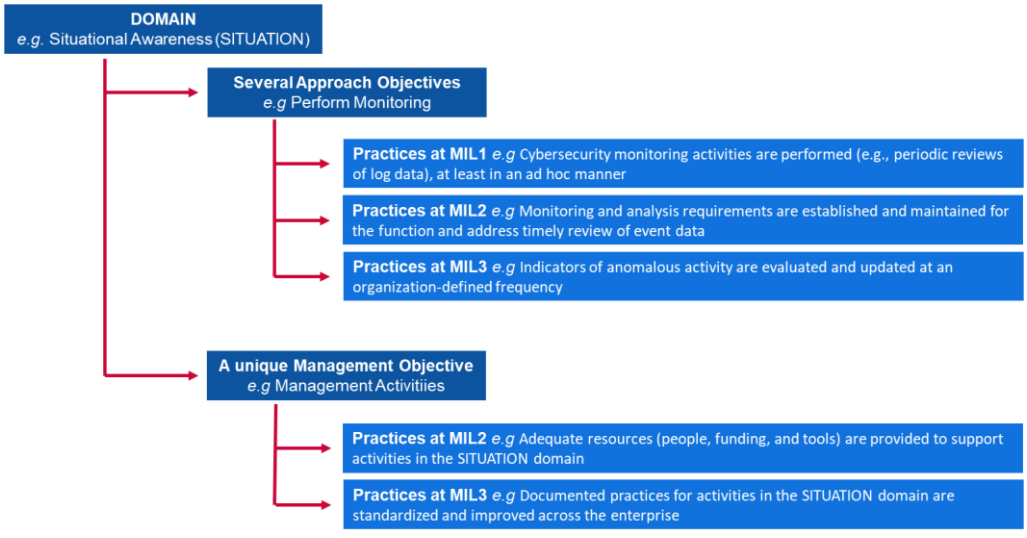
Mognadsmodellen för cyberkapacitet (C2M2) utvecklades av det amerikanska energidepartementet i samarbete med experter från privat och offentlig sektor. Kapacitetscentrumets mål är att hjälpa organisationer inom alla sektorer, av alla typer och i alla storlekar att utvärdera och förbättra sina cybersäkerhetsprogram och stärka sin operativa motståndskraft. C2M2 inriktar sig på implementering och hantering av cybersäkerhetsrutiner kopplade till uppgifts-, informationstekniska- (it) och driftstekniska tillgångar och de miljöer där de finns. I C2M2 definieras mognadsmodeller som ”en uppsättning egenskaper, attribut, indikatorer eller mönster som återger kapacitet och framsteg inom ett visst område”. C2M2, togs ursprungligen i bruk 2014 och reviderades 2019.

Attribut och dimensioner

I C2M2 används **tio domäner** som omfattar en logisk gruppering av cybersäkerhetsmetoder. Varje uppsättning rutiner representerar de aktiviteter som en organisation kan utföra för att etablera och höja sin kapacitet inom domänen. Varje domän är sedan kopplad till **ett unikt förvaltningsmål** och **flera mål som avser tillvägagångssätt**. Inom både tillvägagångsmålen och förvaltningsmålet redovisas **flera metoder**för att beskriva institutionaliserad verksamhet.

Förhållandet mellan dessa begrepp sammanfattas nedan:

Bild 6: C2M2-indikatorer



Domain eg Situational Awareness (SITUATION)	**Domän:** t.ex. situationsmedvetenhet (SITUATION)
Several Approaches Objectives e.g. Perform Monitoring	**Flera tillvägagångsmål:** t.ex. utföra övervakning
Practices at MIL1 e.g Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data), at least in an ad hoc manner	**Metod vid MIN1**: t.ex. cybersäkerhetsövervakning utförs (t.ex. periodiska granskningar av loggdata), åtminstone tillfälligt och för ändamålet
Practices at MIL2 e.g Monitoring and analysis requirement are established and maintained for the function and adress timely review of event data	**Metod vid MIN2:** t.ex. övervaknings- och analyskrav upprättas och upprätthålls för funktionen och en granskning av händelsedata i rätt tid genomförs

Practices at MIL3 e.g Indicators of anomalous activity are evaluated and updated at an organization-defined frequency	**Metod vid MIN3:** t.ex. indikatorer för onormal aktivitet utvärderas och uppdateras vid en organisationsdefinierad frekvens
A unique Management Objectve e.g. Management Activities **Practices at MIL2** e.g Adequate resources (people, funding, and tools) are provided to support activities in the SITUATION domain	Ett unikt förvaltningsmål, t.ex. förvaltningsaktiviteter **Metod vid MIN2:** t.ex. tillräckliga resurser (personal, finansiering och verktyg) tillhandahålls för att stödja aktiviteter inom situationsområdet
Practices at MIL3 e.g Documented practices for activities in the SITUATION domain are standardized and improved across the entreprise	**Metod vid MIN3:** t.ex. dokumenterad praxis för aktiviteter inom situationsområdet standardiseras och förbättras inom hela företaget

De tio domänerna är följande:

i Riskhantering (RISK)
ii Tillgångs-, ändrings- och konfigurationshantering (TILLGÅNG)
iii Identitets- och åtkomsthantering (ÅTKOMST)
iv Hantering av hot och sårbarhet (HOT)
v Situationsmedvetenhet (SITUATION)
vi Respons vid händelser och incidenthantering (RESPONS)
vii Hantering av leveranskedjan och externa beroendeförhållanden (BEROENDE)
viii Personalförvaltning (PERSONAL)
ix Cybersäkerhetsarkitektur (ARKITEKTUR)
x Hantering av cybersäkerhetsprogram (PROGRAM)

Mognadsnivåer

C2M2 använder **fyra mognadsnivåer** (s.k. mognadsindikatornivåer – ”MIN”) för att fastställa en dubbel mognadsprogression: en progression i tillvägagångssätt och en progression i hantering eller förvaltning. Mognadsindikatornivåerna varierar från MIN0 till MIN3 och är avsedda att tillämpas på ett oberoende sätt för varje domän.

- **MIN0:** Inga förfaranden utförs.
- **MIN1:** Inledande förfaranden utförs, men kan vara av tillfällig art.
- **MIN2:** Förvaltningens egenskaper:
  - Förfarandena dokumenteras.
  - Tillräckliga resurser tillhandahålls för att stödja processen.
  - Personal som utför förfarandena har tillräckliga färdigheter och kunskaper.
  - Ansvar och behörighet för att utföra förfarandena tilldelas.

  Tillvägagångssättets egenskaper:
  - Metoderna är mer fullständiga eller avancerade än vid MIN1.
- **MIN3:** Förvaltningens egenskaper:
  - Verksamheten styrs av policyer (eller andra organisationsdirektiv).
  - Prestationsmål för domänaktiviteter fastställs och övervakas för att spåra uppnådda resultat.
  - Dokumenterade förfaranden för domänaktiviteter standardiseras och förbättras inom hela organisationen.

  Tillvägagångssättets egenskaper:
  - Övningarna är mer fullständiga eller avancerade än vid MIN2.

Bedömningsmetod

C2M2 är utformad för att användas med **en självutvärderingsmetod** och en verktygslåda (tillgänglig på begäran) för en organisation för att mäta och förbättra dess cybersäkerhetsprogram. En självutvärdering med hjälp av verktygslådan kan slutföras på en dag, men verktygslådan kan anpassas för en strängare utvärderingsinsats. Dessutom kan C2M2 användas för att vägleda utvecklingen av ett nytt cybersäkerhetsprogram.

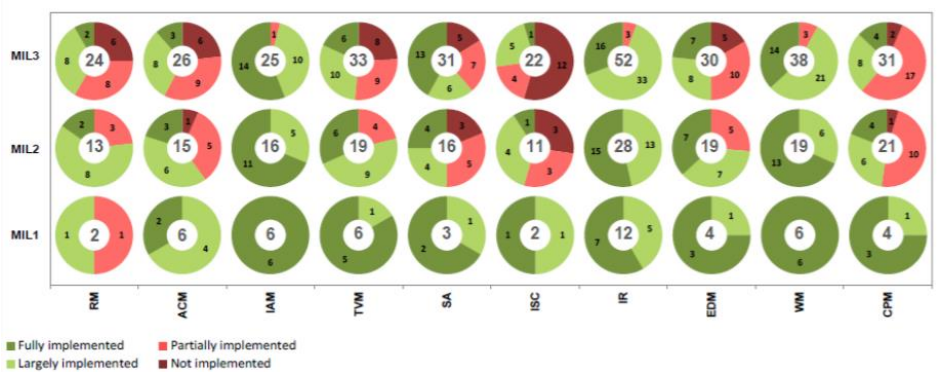
Modellens innehåll presenteras på en hög abstraktionsnivå så att det kan tolkas av organisationer av olika typer, struktur, storlek och från olika sektorer. Bred användning av modellen inom en viss sektor kan stödja benchmarking av sektorns cybersäkerhetskapacitet.

Modus eller återgivning av resultaten

C2M2 tillhandahåller en utvärderingsrapport som skapas utifrån undersökningsresultaten. I rapporten presenteras resultaten i två vyer: den objektiva vyn, som visar svaren på verksamhetsfrågor från varje domän och dess mål, och domänvyn, som visar svaren från samtliga områden och mognadsindikatornivåer. Båda vyerna baseras på ett representationssystem som kännetecknas av cirkeldiagram, ett per svar, och en poängsättningsmekanism utformad som trafikljus. Som visas i Bild 7 anger de röda sektorerna i ett cirkeldiagram en angivelse av antalet frågor där enkätsvaret var ”Inte genomförd” (mörkrött) eller ”Delvis genomförd” (ljusrött). De gröna sektorerna visar antalet frågor där respondenterna angett svaret ”Till stor del genomförd” (ljusgrönt) eller ”Fullständigt genomförd” (mörkgrönt).

Bild 7 nedan är ett exempel på ett poängkort i slutet av en mognadsbedömning. X-axeln visar de 10 domänerna i C2M2, medan Y-axeln anger mognadsnivåerna (MIN). Om man tittar på riskhanteringsdomänen (RM) i diagrammet kan man se tre cirkeldiagram, där vart och ett motsvarar mognadsnivåerna ML1, ML2 och ML3. Vad gäller riskhanteringsdomänen (RM) visar diagrammet att det finns två poster som måste utvärderas för att nå den första mognadsnivån, ML1. I det här fallet gäller det omdömena ”Till stor del genomförd” och omdömet ”Delvis genomförd”. För den andra mognadsnivån, ML2, förutser modellen 13 poster som måste utvärderas. Två av dessa 13 poster tillhör den första nivån, ML1, och 11 tillhör den andra nivån, ML2. Detsamma gäller för den tredje nivån ML3.

Bild 7: C2M2 – Exempel på domänvy



Fully implemented	Har genomförts fullt ut
Largely implemented	Till stor del genomförd
Partially implemented	Delvis genomförd
Not implemented	Inte genomförd
MIL1	MIN1
MIL2	MIN2
MIL3	MIN3
RM	RM
ACM	ACM
IAM	IAM
TVM	TVM
SA	SA
ISC	ISC
IR	IR
EDM	EDM
WM	WM
CPM	CPM

Källa: US Department of Energy, Office of Electricity Delivery and Energy reliability, 2015.

A.3 Ramen för förbättring av cybersäkerheten i kritisk infrastruktur

Ramen för förbättring av cybersäkerheten i kritisk infrastruktur (Framework for Improving Critical Infrastructure Cybersecurity) har utvecklats av National Institute of Standards and Technology – NIST (nationella institutet för standarder och teknik). Det inriktar sig på att vägleda cybersäkerhetsaktiviteter och hantera risker inom en organisation. Ramen riktar sig till alla typer av organisationer oavsett storlek, grad av cybersäkerhetsrisk eller hur avancerad dess cybersäkerhet är. Eftersom detta är ett ramverk och inte en modell, är den uppbyggd på ett annat sätt än de modeller som analyserats tidigare.

Ramverket består av tre delar: ramkärnan, genomförandeskikten och ramprofilerna:

- **Ramkärnan** är en samling cybersäkerhetsaktiviteter, önskade resultat och tillämpliga referenser som är gemensamma för sektorer med kritisk infrastruktur. Dessa liknar de attribut eller dimensioner som finns i modellerna för cybersäkerhetskapacitet.
- **Ramgenomförandeskikt** (eller bara ”skikt”) ger en kontext kring hur ett företag eller organisation ser på en cybersäkerhetsrisk och de processer som finns för att hantera risken. Skikten sträcker sig från partiell (skikt 1) till anpassningsbar (skikt 4) och beskriver en ökande grad av noggrannhet och avancerad hantering av cybersäkerhetsrisker. Skikten återger inte mognadsnivåer utan är snarare avsedda att stödja organisatoriskt beslutsfattande i fråga om hur cybersäkerhetsrisker ska hanteras, samt vilka dimensioner av organisationen som har högre prioritet och kan tilldelas ytterligare resurser.
- En **ramprofil** (eller bara ”profil”) representerar de resultat som baseras på de affärsbehov som en organisation har valt från ramkategorierna och underkategorierna. Profilen kan beskrivas utifrån anpassning av standarder, riktlinjer och praxis till ramkärnan i ett visst implementeringsscenario. Profiler kan användas för att identifiera möjligheter att förbättra cybersäkerhetsnivån genom att jämföra en ”aktuell” profil (i befintligt skick) med en ”målprofil”.

Ramkärna

Ramkärnan består av fem **funktioner**. När de betraktas tillsammans ger dessa funktioner en strategisk överblick över livscykeln för en organisations hantering av cybersäkerhetsrisker. Ramkärnan identifierar sedan underliggande **nyckelkategorier** och **underkategorier** för varje funktion och matchar dem med exempel på informativa referenser såsom befintliga standarder, riktlinjer och praxis för varje underkategori.

Funktioner och kategorier beskrivs nedan:

i **Identifiera:** Utveckla en organisatorisk förståelse för hur man hanterar cybersäkerhetsrisker för system, människor, tillgångar, data och kapacitet.
- Underkategorier: förvaltning av tillgångar, affärsmiljö, styrning, riskbedömning och riskhanteringsstrategi.

ii **Skydda:** Utveckla och genomföra lämpliga skyddsåtgärder för att säkerställa tillhandahållandet av kritiska tjänster.
- Underkategorier: Identitetshantering och tillträdeskontroll, medvetenhet och utbildning; datasäkerhet, informationsskyddsprocesser och -rutiner, underhåll, skyddsteknik.

iii **Upptäcka:** Utveckla och genomföra lämpliga aktiviteter för att identifiera förekomsten av en cybersäkerhetshändelse.
- Underkategorier: Anomalier och händelser, kontinuerlig säkerhetsövervakning och detektionsprocesser.

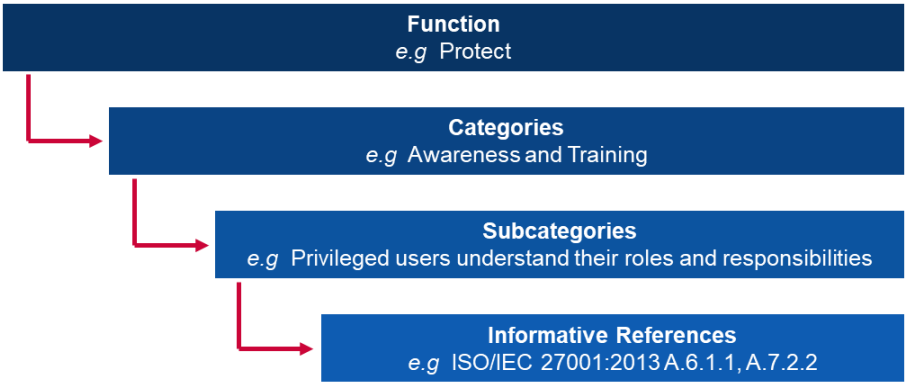
iv **Hantera:** Utveckla och genomföra lämpliga aktiviteter för att vidta åtgärder vid upptäckt av en cybersäkerhetsincident.

- Underkategorier: Insatsplanering, kommunikation, analys, begränsning och förbättringar.

v **Återställa:** Utveckla och genomföra lämpliga aktiviteter för att upprätthålla planer för resiliens och för att återställa eventuell kapacitet eller tjänster som försämrats på grund av en cybersäkerhetsincident.

- Underkategorier: Återhämtningsplanering, förbättringar och kommunikation.

Bild 8: Exempel på ramverket för förbättring av den kritiska infrastrukturens cybersäkerhet



Function e.g Project
Categories e.g Awarness and Training
Subcategories e.g Privileged useres understand their roles and responsibilities
Informative References e.g ISO/IEC 27001:2013 A.6.1.1,A.7.2.2

Funktion: t.ex. projekt
Kategorier: t.ex. medvetenhet och utbildning
Underkategorier: t.ex. konfidentiella användare förstår sina roller och sitt ansvar
Informativa referenser: t.ex. ISO/IEC 27001:2013 A.6.1.1,A.7.2.2

Skikt

Ramen för förbättring av cybersäkerheten i kritisk infrastruktur bygger på **fyra skikt**, som vart och ett definieras med hjälp av tre faktorer: en riskhanteringsprocess, ett integrerat riskhanteringsprogram och externt deltagande. Skikten ska inte betraktas som mognadsnivåer utan som en ram för att organisationer ska kunna kontextualisera sin syn på cybersäkerhetsrisker och de processer som finns för att hantera riskerna.

- **Skikt 1: Partiell**
  - **Riskhanteringsprocess**: Organisatoriska rutiner för hantering av cybersäkerhetsrisker är inte formaliserade och risken hanteras på ett tillfälligt (ad hoc) och ibland reaktivt sätt.
  - **Integrerat riskhanteringsprogram**: Det finns en begränsad medvetenhet om cybersäkerhetsriskerna på organisationsnivå. Organisationen implementerar cybersäkerhetsriskhantering på en oregelbunden basis från fall till fall och har kanske inte rutiner som möjliggör delning av cybersäkerhetsinformation inom organisationen.
  - **Externt deltagande:** Organisationen förstår inte sin roll i det större sammanhanget, vare sig när det gäller dess beroendeförhållanden eller beroendegrupper. Organisationen är i allmänhet omedveten om riskerna med cyberleveranskedjan för de produkter och tjänster som den tillhandahåller och som den använder.
- **Skikt 2: Riskinformerad**
  - **Riskhanteringsprocess**: Riskhanteringspraxis godkänns av ledningen men får inte fastställas som organisationsövergripande policy.
  - **Integrerat riskhanteringsprogram**: Det finns en medvetenhet om cybersäkerhetsrisker på organisationsnivå, men en organisationsövergripande strategi för att hantera cybersäkerhetsrisker har inte fastställts. Cyberriskbedömningar av organisatoriska och externa tillgångar görs men är vanligtvis inte repeterbara eller återkommande.

- **Externt deltagande**: I allmänhet förstår organisationen sin roll i ett större sammanhang med avseende på antingen sina egna beroendeförhållanden eller beroendegrupper, men inte både och. Dessutom är organisationen medveten om riskerna med cyberleveranskedjan, som är förknippade med de produkter och tjänster som den tillhandahåller och använder, men agerar inte konsekvent eller formellt på dessa risker.

- **Skikt 3: Repeterbar**
  - **Riskhanteringsprocess**: Organisationens riskhanteringspraxis är formellt godkänd och uttryckt som policy. Organisatoriska cybersäkerhetsrutiner uppdateras regelbundet baserat på tillämpningen av riskhanteringsprocesser på förändringar i affärs-/uppdragskrav och ett föränderligt hot- och tekniklandskap.
  - **Integrerat riskhanteringsprogram**: Det finns en organisationsövergripande strategi för att hantera cybersäkerhetsrisker. Riskbaserade policyer, processer och rutiner definieras och införs som avsett och granskas sedan. Högre chefer säkerställer att hänsyn tas till cybersäkerhet inom samtliga verksamhetsområden i organisationen.
  - **Externt deltagande**: Organisationen förstår sin roll, sina beroendeförhållanden och beroendegrupper inom ramen för ett större sammanhang och kan bidra till samhällets bredare förståelse av risker. Organisationen är medveten om riskerna med cyberleveranskedjan som är förknippade med de produkter och tjänster som den tillhandahåller och använder.

- **Skikt 4: Anpassningsbar**
  - **Riskhanteringsprocess**: Organisationen anpassar sina cybersäkerhetsrutiner baserat på tidigare och nuvarande cybersäkerhetsaktiviteter, inklusive lärdomar och prediktiva indikatorer.
  - **Integrerat riskhanteringsprogram**: Det finns en organisationsövergripande strategi för att hantera cybersäkerhetsrisker som använder riskinformerade policyer, processer och förfaranden för att hantera potentiella cybersäkerhetshändelser.
  - Organisationen förstår sin roll, sina beroendeförhållanden och beroendegrupper i det större sammanhanget och bidrar till samhällets bredare förståelse av risker.

Bedömningsmetod

Ramen för förbättring av cybersäkerheten i kritisk infrastruktur är avsedd för att organisationer själva ska bedöma sina risker för att göra sin strategi och sina investeringar i cybersäkerhet mer rationella, effektiva och värdefulla. För att undersöka investeringarnas effektivitet måste en organisation först ha en god förståelse för sina organisatoriska mål, förhållandet mellan dessa mål och stödjande cybersäkerhetsresultat. Resultaten av ramkärnan för cybersäkerhet stödjer självutvärdering av investeringseffektivitet och cybersäkerhetshantering.

A.4 Qatars mognadsmodell för cybersäkerhetskapacitet (Q-C2M2)

Qatars mognadsmodell för cybersäkerhetskapacitet (Qatar Cybersecurity Capability Maturity Model), eller Q-C2M2, utvecklades 2018 av College of Law vid universitetet i Qatar. Q-C2M2 bygger på olika befintliga modeller som tillsammans formar en omfattande bedömningsmetodik som syftar till att förbättra Qatars cybersäkerhetsram.

Attribut och dimensioner

Q-C2M2 antar NIST-ramverkets (National Institute of Standards and Technology) tillvägagångssätt, som bygger på att använda fem huvudfunktioner som modellens huvuddomäner. De fem huvudfunktionerna är tillämpliga i Qatarkontexten eftersom de är gemensamma inom kritiska infrastruktursektorer, vilket är en viktig del i Qatars cybersäkerhetsram. Q-C2M2 bygger på **fem domäner**. Varje domän är sedan uppdelad i flera **underdomäner** för att täcka hela skalan av kapacitetsmognad inom cybersäkerhet.

De fem domänerna är följande:

i **Domänen Förstå (Understand)** omfattar fyra underdomäner: cyberstyrning, tillgångar, risker och utbildning.

ii Underdomänerna som tillhör **domänen Säkra (Secure)** inkluderar säkerhet för data, teknik, tillträdeskontroll, kommunikation och personal.
iii **Domänen Exponera (Expose)** omfattar underdomänerna övervakning, incidenthantering, detektering, analys och exponering.
iv **Domänen Hantera (Respond)** inkluderar responsplanering, begränsning och responskommunikation.
v **Domänen Underhålla (Sustain)** inbegriper återhämtningsplanering, kontinuitetshantering, förbättring och externa beroenden.

Mognadsnivåer

Q-C2M2 använder **fem mognadsnivåer** som mäter en myndighets eller en icke-statlig organisations mognadsnivå på huvudfunktionsnivå. Dessa nivåer syftar till att bedöma mognaden inom de fem områden som beskrivs i föregående avsnitt.

- **Inledningsstadiet:** Använder ad hoc-förfaranden och -processer för cybersäkerhet inom vissa av domänerna.
- **Genomförandestadiet:** Antagande av strategier för att genomföra all cybersäkerhetsverksamhet inom områdena i syfte att slutföra genomförandet vid en viss tidpunkt.
- **Utvecklingsstadiet**; Genomförande av policyer och metoder för att utveckla och förbättra cybersäkerhetsverksamhet inom områdena i syfte att föreslå nya åtgärder att genomföra.
- **Anpassningsstadiet:** Tillbakablick och översyn av cybersäkerhetsåtgärder och antagande av metoder baserade på prediktiva indikatorer som hämtats från tidigare erfarenheter och åtgärder.
- **Det flexibla stadiet:** Förlängning av anpassningsfasen med särskild betoning på smidighet och snabbhet vid genomförandet av åtgärder inom domänerna.

Bedömningsmetod

Q-C2M2 befinner sig i ett tidigt skede av forskningen och är ännu inte klar för att användas. Det är en ram som skulle kunna användas för att införa en detaljerad bedömningsmodell för qatariska organisationer i framtiden.

A.5 Certifiering av mognadsmodell för cybersäkerhet (CMMC)

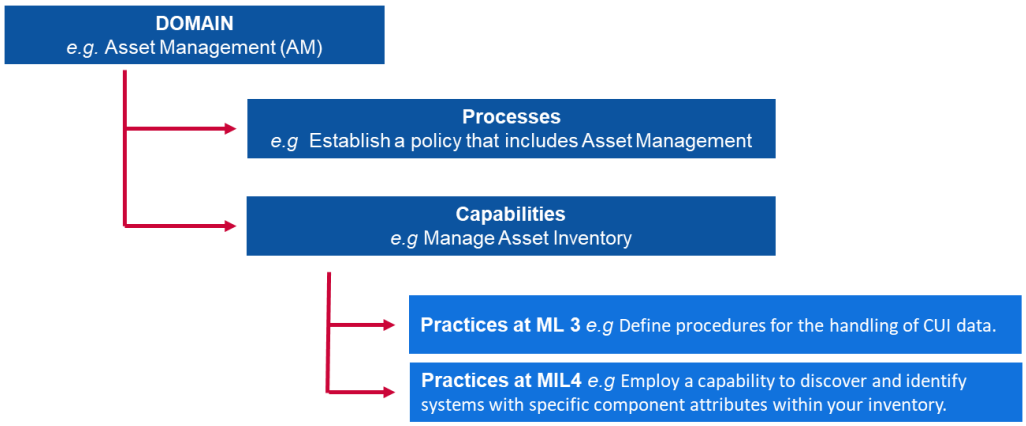
Certifiering av mognadsmodell för cybersäkerhet (Cybersecurity Maturity Model Certification), eller CMMC, utvecklades av USA:s försvarsdepartement i samarbete med Carnegie Mellon University och Johns Hopkins University Applied Physics Laboratory. Försvarsdepartementets huvudsyfte med utformningen av denna modell var att skydda information inom försvarsindustrins bassektor. Den information som CMMC riktar in sig på klassificeras som antingen ”federala kontraktsuppgifter”, information som tillhandahålls av eller skapas för statliga ändamål enligt avtal som inte är avsedda för offentliggörande, eller ”kontrollerad oklassificerad information”, dvs. information som kräver skydd eller spridningskontroller i enlighet och i överensstämmelse med lagar, förordningar och statliga riktlinjer. CMMC mäter cybersäkerhetsmognad och tillhandahåller bästa praxis tillsammans med ett certifieringselement för att säkerställa genomförandet av förfaranden som är kopplade till varje mognadsnivå. Den senaste versionen av CMMC släpptes 2020.

Attribut och dimensioner

CMMC beaktar **17 domäner** som representerar kluster av cybersäkerhetsprocesser och kapaciteter. Varje domän delas sedan upp i flera **processer**, som är likartade oavsett domän, och ett stort antal **funktioner** som sträcker sig över fem mognadsnivåer. Kapaciteten (eller förmågan) redovisas sedan i **förfaranden** för varje relevant mognadsnivå.

Förhållandet mellan dessa begrepp sammanfattas nedan:

Bild 9: CMMC-indikatorer



DOMAIN e.g. Asset Management (AM)	**DOMÄN**: t.ex. tillgångsförvaltning (AM – från Asset Management)
Processes e.g Establish a policy that includes Asset Management	**Processer**: t.ex. att etablera en policy som inkluderar tillgångsförvaltning
Capabilities e.g Manage Asset Inventory	**Kapaciteter**: t.ex. att hantering av tillgångslager
Practices at ML 3 e.g Define procedures for the handling of CUI data	**Förfaranden vid MIN3:** t.ex. att definiera förfaranden för hantering av kontrollerade oklassificerade uppgifter
Practices at MIL4 e.g Employ a capability to discover and identify systems with specific component attributes within inventory	**Övningar på MIN4:** t.ex. att använda kapacitet att upptäcka och identifiera system med specifika komponentattribut inom lagerhantering

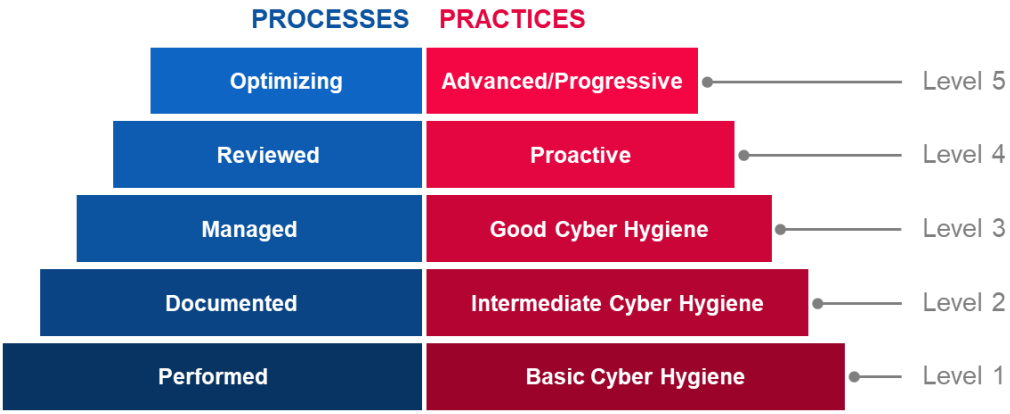
De 17 domänerna är följande:

i Tillträdeskontroll (AC – Access Control)
ii Tillgångsförvaltning (AM – Asset Management)
iii Revision och ansvarsskyldighet (AU – Audit and Accountability)
iv Medvetenhet och utbildning (AT – Awareness and Training)
v Konfigurationsledning (CM – Configuration Management)
vi Identifiering och autentisering (IA – Identification and Authentication)
vii Incidenthantering (IR – Incident Response)
viii Underhåll (MA – Maintenance)
ix Medieskydd (MP – Media Protection)
x Personalsäkerhet (PS – Personnel Security)
xi Fysiskt skydd (PE – Physical Protection)
xii Återhämtning (RE – Recovery)
xiii Riskhantering (RM)
xiv Säkerhetsbedömning (CA – Security Assessment)
xv Situationsmedvetenhet (SA – Situational Awareness)
xvi System- och kommunikationsskydd (SC – System and Communications Protection).
xvii System- och informationsintegritet (SI – System and Information Integrity).

Mognadsnivåer

I CMMC används **fem mognadsnivåer** som definieras utifrån processer och förfaranden. För att nå en viss mognadsnivå i CMMC måste en organisation uppfylla de nödvändiga förutsättningarna för processer och förfaranden på nivån i fråga. Det innebär också att alla nödvändiga förutsättningar för alla nivåer under den nivån har uppfyllts.

Bild 10: Mognadsnivåer i CMMC



PROCESSES	PROCESSER
Optimizing	Optimering
Reviewed	Granskade
Managed	Hanterade
Documented	Dokumenterade
Performed	Genomförda
PRACTICES	FÖRFARANDEN
Advanced/Progressive	Avancerade/progressiva
Proactive	Proaktiva
Good Cyber Hygiene	God cyberhygien
Intermediate Cyber Hygiene	Medelgod cyberhygien
Basic Cyber Hygiene	Grundläggande cyberhygien
Level 5	Nivå 5
Level 4	Nivå 4
Level 3	Nivå 3
Level 2	Nivå 2
Level 1	Nivå 1

- **Nivå 1**
  - **Processer – utförda**: Organisationen kanske bara kan utföra dessa metoder på ad hoc-basis och det är osäkert om den kan förlita sig på dokumentation. Processens mognad bedöms inte för nivå 1.
  - **Förfaranden – grundläggande cyberhygien**: Nivå 1 är inriktad på skyddet av federala kontraktsuppgifter och består endast av förfaranden som motsvarar de grundläggande skyddskraven.
- **Nivå 2**
  - **Processer – dokumenterade**: Nivå 2 kräver att en organisation fastställer och dokumenterar förfaranden och policyer för att vägleda genomförandet av sina CMMC-insatser. Dokumentationen över förfaranden gör det möjligt för enskilda att utföra dem på ett sätt som kan upprepas. Organisationerna utvecklar mogen kapacitet genom att dokumentera sina processer och sedan tillämpa dem som dokumenterade processer.
  - **Förfaranden – medelgod cyberhygien**: Nivå 2 fungerar som ett utvecklingssteg mellan nivå 1 och nivå 3 och består dels av en undergrupp av de säkerhetskrav som specificeras i NIST SP 800–171, och dels av förfaranden från andra standarder och referenser.
- **Nivå 3**
  - **Processer – hanterade**: Nivå 3 kräver att en organisation upprättar, upprätthåller och levererar en plan som visar hur åtgärderna styrs för att genomföras rent praktiskt. Planen kan innehålla information om uppdrag, mål, projektplaner, resurser, nödvändig utbildning och berörda intressenters deltagande.
  - **Förfaranden – god cyberhygien**: Nivå 3 är inriktad på skydd av kontrollerade oklassificerade uppgifter och omfattar alla säkerhetskrav som beskrivs i NIST SP

800–171 samt ytterligare praxis från andra standarder och hänvisningar för att mildra hoten.

- **Nivå 4**
  - **Processer – granskade**: Nivå 4 kräver att en organisation granskar och mäter hur effektiva förfarandena är. Förutom att mäta förfarandenas effektivitet kan organisationer på denna nivå vid behov vidta korrigerande åtgärder och regelbundet informera ledningen på högre nivå om status eller frågor.
  - **Förfaranden – proaktiva**: Nivå 4 är inriktad på skyddet av kontrollerade oklassificerade uppgifter och omfattar en undergrupp av de skärpta säkerhetskraven. Dessa metoder stärker en organisations förmåga att upptäcka och åtgärda brister i syfte att hantera och anpassa sig till ändrade taktiker, tekniker och förfaranden.
- **Nivå 5**
  - Nivå 5 kräver att en organisation standardiserar och optimerar genomförandet av processen inom hela organisationen.
  - **Metoder – avancerade/proaktiva**: Nivå 5 inriktar sig på skyddet av kontrollerade oklassificerade uppgifter. Övriga förfaranden säkerställer att cybersäkerhetsförmågan blir mer avancerad och grundligt genomförd.

Bedömningsmetod

CMMC är en relativt ny modell som färdigställdes under första kvartalet 2020. Hittills har den inte använts inom någon organisation. Underleverantörerna till USA:s försvarsdepartement förväntar sig emellertid att kontakta certifierade tredjepartsinspektörer för utförande av revisioner. DoD förväntar sig att sina entreprenörer att de ska tillämpa bästa praxis för att främja cybersäkerhet och skydd av känslig information.

A.6 Samhällsmodell för cybersäkerhetsmognad (CCSMM)

Community Cyber Security Maturity Model (CCSMM) utvecklades av Centre for Infrastructure Assurance and Security vid University of Texas. Målet med CCSMM är att bättre definiera metoder för att fastställa ett samhälles aktuella status i fråga om dess cyberberedskap och tillhandahålla en färdplan som de kan att följa under sina beredskapsinsatser. CCSMM riktar sig huvudsakligen till kommunala, lokala eller statliga myndigheter. CCSMM utformades 2007.

Attribut och dimensioner

Mognadsnivåerna definieras enligt **följande sex huvuddimensioner**, vilka täcker de olika aspekterna av cybersäkerhet inom olika samhällen och organisationer. Dessa dimensioner är tydligt definierade för varje mognadsnivå (beskrivs i Bild 31: Sammanfattning av CCSMM-dimensionerna). De 6 dimensionerna är följande:

i Hot som hanterats/åtgärdats
ii Mått
iii Informationsutbyte
iv Teknik
v Utbildning
vi Test

Mognadsnivåer

CCSMM bygger på **fem mognadsnivåer** som grundar sig på de huvudsakliga typer av hot och aktiviteter som hanteras på nivån:

- **Nivå 1: Säkerhetsmedvetenhet**
  Det viktigaste ämnet för aktiviteter på denna nivå är att öka medvetenheten hos människor och organisationer om hot, problem och frågor relaterade till cybersäkerhet.

- **Nivå 2: Processutveckling**
  Nivån är utformad för att hjälpa samhällen att etablera och förbättra de säkerhetsprocesser som krävs för att effektivt bekämpa cybersäkerhetsproblem.
- **Nivå 3: Möjliggöra informationsutbyte**
  Utformad för att förbättra mekanismerna för informationsutbyte inom samhället, för att göra det möjligt för samhället att effektivt korrelera information som till synes inte har samband.
- **Nivå 4: Taktikutveckling**
  Elementen på denna nivån är utformade för att utveckla bättre och mer proaktiva metoder för att upptäcka och hantera attacker. På denna nivå bör de flesta förebyggande metoder finnas på plats.
- **Nivå 5: Full operativ säkerhetskapacitet**
  Denna nivå representerar de element som bör vara på plats för att en organisation ska kunna anses vara fullt operativt redo att gripa sig an alla typer av cyberhot.

Bild 31: Sammanfattning av CCSMM-dimensionerna per nivå

	Level 1 Security Aware	**Level 2** Process Development	**Level 3** Information Enabled	**Level 4** Tactics Development	**Level 5** Full Security Operational Capability
Threats Addressed	Unstructured	Unstructured	Structured	Structured	Highly Structured
Metrics	Government Industry Citizens	Government Industry Citizens	Government Industry Citizens	Government Industry Citizens	Government Industry Citizens
Information Sharing	Information Sharing Committee	Community Security Web Site	Information Correlation Center	State/Fed Correlation	Complete Info Vision
Technology	Rosters, GETS, Access Controls, Encryption	Secure Web Site Firewalls, Backups	Event Correlation SW IDS/IPS	24/7 manned operations	Automated Operations
Training	1-day Community Seminar	Conducting a CCSE	Vulnerability Assessments	Operational Security	Multi-Discipline Red Teaming
Test	Dark Screen - EOC	Community Dark Screen	Operational Dark Screen	Limited Black Demon	Black Demon

Level 1	Nivå 1
Security Aware	Säkerhetsmedvetenhet
Level 2	Nivå 2
Process Development	Processutveckling
Level 3	Nivå 3
Information Enabled	Möjliggörande av informationsutbyte
Level 4	Nivå 4
Tactics Development	Taktikutveckling
Level 5	Nivå 5
Full Security Operational Capability	Full operativ säkerhetskapacitet
Threats Addressed	Hot som hanterats/åtgärdats
Metrics	Mått
Information sharing	Informationsutbyte
Technology	Teknik
Training	Utbildning
Test	Test
Unstructured	Ostrukturerad
Governement	Stat
Industry	Industri
Citizens	Medborgare
Information Sharing Committee	Kommittén för informationsutbyte
Rosters, GETS, Assess Controls, Encryption	Listor, GETS, tillträdeskontroll, kryptering

1-dat Community Seminar	1-dat samhällsseminarium
Dark Screen – EOC	Dark Screen – EOC
Unstructured	Ostrukturerad
Governement	Stat
Industry	Industri
Citizens	Medborgare
Community Security Web site	Webbplats för samhällssäkerhet
Secure Web Site Firewalls, Backups	Säkra webbplatsbrandväggar, säkerhetskopior
Conudcting a CCSE	Genomföra en CCSE
Community Dark Screen	Community Dark Screen
Structured	Strukturerad
Governement	Stat
Industry	Industri
Citizens	Medborgare
Information Correlation Center	Informationskorrelationscenter
Event Correlation SW IDS/IPS	Händelsekorrelation SW IDS/IPS
Vulnerability Assessment	Sårbarhetsanalys
Operational Dark Screen	Operativ dark screen
Structured	Strukturerad
Governement	Stat
Industry	Industri
Citizens	Medborgare
State/Fed Correlation	Stat korrelation
24/7 manned operations	Bemannade insatser 24/7
Operational Security	Operativ säkerhet
Limited Black Demon	Limited Black Demon
Highly Structured	Hög grad av strukturering
Governement	Stat
Industry	Industri
Citizens	Medborgare
Complete Info Vision	Fullständig infovy
Automated Operations	Automatiserade förfaranden
Multi-Discipline Red Teaming	Tvärvetenskapliga red team-test
Black Demon	Black Demon-övning

Bedömningsmetod

CCSMM som bedömningsmetod är avsedd att användas av samhällen med bidrag från statliga och federala brottsbekämpande organ. Den syftar till att hjälpa samhället att definiera vad som är viktigast, vilka som är de mest sannolika målen och vad som behöver skyddas (och i vilken utsträckning). Med dessa mål i åtanke kan planer utarbetas för att få varje aspekt av samhället till den nivå av cybersäkerhet som krävs. Den specifika information som genereras av CCSMM hjälper till att definiera målen för olika tester och övningar som kan användas för att mäta effektiviteten hos redan inrättade program.

A.7 Mognadsmodell för informationssäkerhet för NIST:s cybersäkerhetsramverk (ISMM)

Mognadsmodellen för informationssäkerhet (ISMM) har utvecklats på College of Computer Sciences and Engineering vid King Fahd University of Petroleum and Minerals, i Saudiarabien. Den utgör en ny kapacitetsmognadsmodell för att mäta genomförandet av cybersäkerhetsåtgärder. Målet med ISMM är att göra det möjligt för organisationer att mäta implementeringsframstegen över tid genom att använda samma mätverktyg regelbundet för att säkerställa att den önskade säkerhetshållningen upprätthålls. ISMM togs fram 2017.

Attribut och dimensioner

ISMM bygger vidare på de befintliga utvärderade områdena i NIST-ramverket och till det läggs ytterligare en dimension som rör utvärdering av överensstämmelse. Modellen består av **23 bedömda områden** gällande en organisations säkerhetsnivå. De 23 bedömda områdena är följande:

- Tillgångsförvaltning

ii Företagsmiljö
iii Styrning
iv Riskbedömning
v Riskhanteringsstrategi
vi Bedömning av överensstämmelse
vii Tillträdeskontroll
viii Medvetenhet och utbildning
ix Datasäkerhet
x Informationsskyddsprocesser och -förfaranden
xi Underhåll
xii Skyddande teknologi
xiii Anomalier och händelser
xiv Kontinuerlig säkerhetsövervakning
xv Detekteringsprocesser
xvi Responsplanering
xvii Responskommunikation
xviii Responsanalys
xix Nedsatt respons
xx Responsförbättringar
xxi Återhämtningsplanering
xxii Återhämtningsförbättringar
xxiii Återhämtningskommunikation

Mognadsnivåer

ISMM bygger på **fem mognadsnivåer**, som tyvärr inte redovisas i den tillgängliga dokumentationen.

- **Nivå 1:** Genomförd process.
- **Nivå 2:** Hanterad process.
- **Nivå 3:** Etablerad process.
- **Nivå 4:** Förutsägbar process.
- **Nivå 5:** Optimeringsprocess.

Bedömningsmetod

I ISMM föreslås ingen särskild metod för att genomföra bedömningen för organisationer.

A.8 Modell för internrevisionskapacitet (IA-CM) för den offentliga sektorn

Modellen för internrevisionskapacitet (IA-CM) har utvecklats av Institute of Internal Auditors Research Foundation i syfte att bygga upp kapacitet och skydd genom självutvärdering inom den offentliga sektorn. IA-CM vänder sig till revisionspersonal och ger en översikt över själva modellen tillsammans med en tillämpningsguide för att underlätta användningen av modellen som ett verktyg för självutvärdering.

Trots att internrevisionsmekanismen är inriktad på internrevisionskapacitet snarare än på kapacitetsuppbyggnad inom cybersäkerhet, är modellen byggd som ett verktyg för självutvärdering av mognad för enheter inom den offentliga sektorn och kan tillämpas globalt för att förbättra processer och effektivitet. Eftersom den inte är inriktad på cybersäkerhet kommer attributen inte att analyseras. IA-CM togs fram 2009.

Mognadsnivåer

Modellen för internrevisionskapacitet (IA-CM) omfattar **fem mognadsnivåer**, som var och en beskriver egenskaperna och förmågan hos en internrevisionsverksamhet på den nivån. Kapacitetsnivåerna i modellen ger en färdplan för kontinuerlig förbättring.

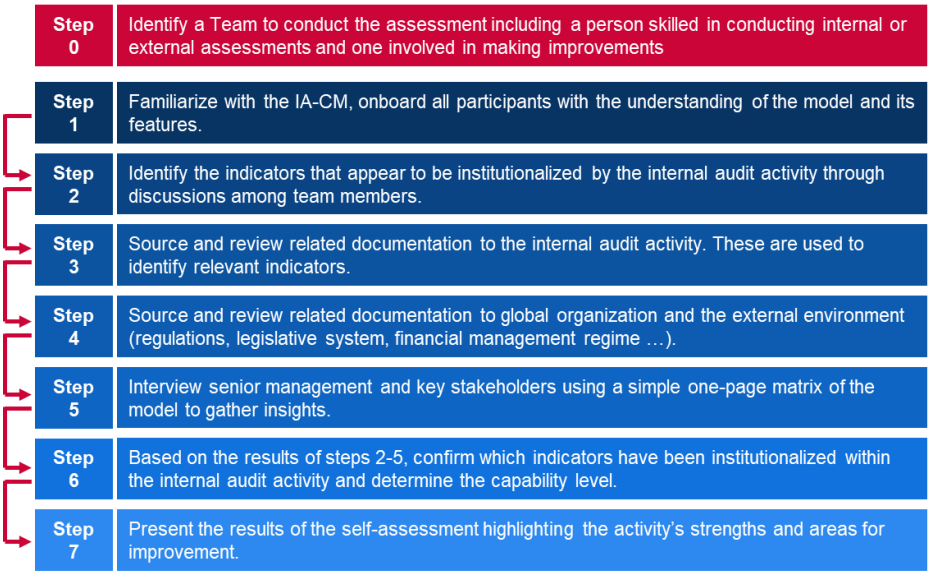
- **Nivå 1: Inledande**
  Ingen hållbar, repeterbar kapacitet – beroende av personliga insatser
  - Ad hoc eller ostrukturerad.
  - Enstaka revisioner eller granskningar av dokument och transaktioner för att kontrollera noggrannhet och efterlevnad.
  - Resultat som är beroende av kompetensen hos den specifika person som innehar tjänsten.
  - Inga andra etablerade yrkesmetoder än de som tillhandahålls av yrkessammanslutningar.
  - Finansieringsgodkännande av ledningen vid behov.
  - Avsaknad av infrastruktur.
  - Revisorer ingår troligen i en större organisatorisk enhet.
  - Den institutionella kapaciteten är inte utvecklad.
- **Nivå 2: Infrastruktur**
  Hållbara och repeterbara metoder och förfaranden
  - Nyckelfråga eller utmaning för nivå 2 är hur man etablerar och upprätthåller repeterbarhet av processer och därmed en repeterbar kapacitet.
  - Internrevisionsrapporteringsrelationer, lednings- och förvaltningsinfrastrukturer samt professionella rutiner och processer håller på att upprättas (intern revisionsvägledning, processer och förfaranden).
  - Revisionsplanering baserad huvudsakligen på förvaltningsprioriteringar.
  - Fortsatt beroende av huvudsakligen specifika personers färdigheter och kompetens.
  - Delvis överensstämmelse med standarderna.
- **Nivå 3: Integrerad**
  Förvaltning och yrkespraktik tillämpas enhetligt
  - Internrevisionspolicyer, processer och rutiner definieras, dokumenteras och integreras i varandra och i organisationens infrastruktur.
  - Internrevisionsstyrning och yrkespraktik är väl etablerade och tillämpas på ett enhetligt sätt i hela internrevisionsverksamheten.
  - Internrevisionen börjar anpassa sig till organisationens verksamhet och de risker den står inför.
  - Internrevisionen utvecklas från att endast utföra traditionell internrevision till att integreras som en lagspelare och ge råd om resultat och riskhantering.
  - Fokus ligger på teambuilding och internrevisionens kapacitet samt dess oberoende och objektivitet.
  - Överensstämmer generellt med standarderna.
- **Nivå 4: Hanterad**
  Integrerar information från hela organisationen för att förbättra styrning och riskhantering
  - Internrevisionen och de viktigaste intressenternas förväntningar stämmer överens.
  - Resultatmått finns på plats för att mäta och övervaka interna revisionsprocesser och resultat.
  - Internrevisionen anses ge betydande bidrag till organisationen.
  - Internrevisionen fungerar som en integrerad del av organisationens styrning och riskhantering.
  - Internrevisionen är en välskött affärsenhet.
  - Risker mäts och hanteras kvantitativt.
  - Obligatoriska färdigheter och kompetenser finns på plats med kapacitet för förnyelse och kunskapsutbyte (inom internrevision och genom hela organisationen).
- **Nivå 5: Optimering**
  Lärdomar hämtas inifrån och utifrån organisationen för kontinuerlig förbättring
  - Internrevision är en lärande organisation med ständiga processförbättringar och innovation.
  - Internrevisionen använder information inifrån och utifrån organisationen för att bidra till att uppnå strategiska mål.
  - Högklassiga resultat/rekommenderad praxis/bästa praxis.
  - Internrevision är en kritisk del av organisationens styrningsstruktur.
  - Professionella och specialiserade färdigheter på toppnivå.
  - Individuella, enhetsmässiga och organisatoriska resultatmått är helt integrerade

- för att driva på prestandaförbättringar.

Bedömningsmetod

Modellen för internrevisionskapacitet är tydligt utformad för självutvärdering. Den ger detaljerade steg att följa vid användningen av IA-CM och ett bildspel med provbilder att anpassa. Innan självutvärderingen inleds ska en särskild grupp identifieras, inklusive minst en person som är kvalificerad att genomföra interna eller externa bedömningar av interna revisioner och en person som har till uppgift att genomföra förbättringar inom detta område.

Bild 12: IC-AM självutvärderingssteg



Step 0
Step 1
Step 2
Step 3
Step 4
Step 5
Step 6
Step 7

Identify a Team to conduct the assessment includiong a person skilled in conducting internal of external assessments and one involved in making improvments.

Familiarize with the IA-CM, onboard all participants with the understanding of the model and its features.
Identify the indicators that appear to be institutionalized by the internal audit activity through discussion among team members.

Source and review related documentation to the internal audit activity. These are used to identify relevant indicators.

Source and review realted documentation to global organisation and the external environment (regulations, legislative system, financial management regime …).
Interview senior management and key stakeholders using a simple one-page matrix of the model to gather insights.

Based on the results of steps 2-5, confirm which indicators have been institutionalized within the internal audit activity and determine the capacity level.
Present the results of the self-assessment highlighting the activity's strenghts and areas for improvement.

Steg 0
Steg 1
Steg 2
Steg 3
Steg 4
Steg 5
Steg 6
Steg 7

Identifiera en arbetsgrupp som ska göra bedömningen, inklusive en person som är skicklig på att genomföra interna och externa bedömningar och en annan person som har till uppgift att genomföra förbättringar.
Göra gruppen väl förtrogen med IA-CM och klargöra modellen och dess funktioner för alla deltagare.
Identifiera de indikatorer som verkar ha institutionaliserats av de interna revisionsaktiviteterna genom samtal mellan gruppmedlemmarna.
Lokalisera och granska dokumentation relaterad till den interna revisionsverksamheten. De används för att identifiera relevanta indikatorer.
Lokalisera och granska dokumentation relaterad till den globala organisationen och den externa miljön (förordningar, lagstiftningssystem, finansiell förvaltning etc.).
Intervjua ledande befattningshavare och viktiga intressenter med hjälp av en enkel, ensidig matris av modellen för att samla insikter.
Bekräfta vilka indikatorer som har institutionaliserats inom den interna revisionsverksamheten och fastställa kapacitetsnivån baserat på resultaten från steg 2-5.
Presentera resultaten av självutvärderingen som belyser verksamhetens styrkor och förbättringsområden.

A.9 Globalt cybersäkerhetsindex (GCI)

Global Cybersecurity Index (GCI) är ett initiativ från Internationella teleunionen (ITU) som syftar till att se över cybersäkerhetsåtagandet och -situationen i alla ITU-regioner: Afrika, Nord- och Sydamerika, arabländerna, Asien-Stillahavsområdet, OSS och Europa, och sätter strålkastaren på länder med ett omfattande åtagande och rekommenderbara metoder. Målet med GCI är att hjälpa länder att identifiera områden som kan förbättras på cybersäkerhetsområdet samt att motivera dem att vidta åtgärder för att förbättra sin ställning och på så sätt bidra till att höja den övergripande it-cybersäkerhetnivån globalt.

Eftersom GCI är ett index och inte en mognadsmodell använder det inte mognadsnivåer utan snarare poäng för att rangordna och jämföra nationer och regioner globala cybersäkerhetsengagemang.

Attribut och dimensioner

Det globala cybersäkerhetsindexet (GCI) bygger på de fem pelarna i den globala cybersäkerhetsagendan (GCA – Global Cybersecurity Agenda). Dessa pelare utgör de fem underkategorierna av GCI:s index, som var och en inbegriper en grupp indikatorer. De fem pelarna och indikatorerna är:

i **De juridiska:** åtgärder baserade på förekomsten av rättsliga institutioner och ramar som hanterar cybersäkerhet och it-brottslighet,
- cyberbrottslagstiftning,
- reglering av cybersäkerhet,
- kontroll/begränsning av skräppostlagstiftning.

ii **De tekniska:** åtgärder som grundar sig på förekomsten av tekniska institutioner och ramar för cybersäkerhet,
- CERT/CIRT/CSRIT,
- ramverk för genomförande av standarder,
- standardiseringsorgan,
- tekniska mekanismer och resurser som används för att hantera spam/skräppost,
- användning av moln för cybersäkerhetsändamål,
- mekanismer för att skydda barn på nätet.

iii **De organisatoriska:** åtgärder som grundar sig på förekomsten av institutioner för politisk samordning och strategier för utveckling av cybersäkerhet på nationell nivå,
- nationell strategi för cybersäkerhet,
- ansvarigt organ,
- cybersäkerhet.

iv **Kapacitetsuppbyggnad:** åtgärder som grundar sig på att det finns program för forskning och utveckling, utbildning, certifierade yrkesutövare och offentliga organ som främjar kapacitetsuppbyggnad,
- informationskampanjer för allmänheten,
- ram för certifiering och ackreditering av yrkesverksamma inom cybersäkerhet,
- yrkesutbildningskurser i cybersäkerhet,
- utbildningsprogram eller akademiska läroplaner i cybersäkerhet,
- FoU-program för cybersäkerhet,
- incitamentsmekanismer.

v **Samarbete:** Åtgärder som grundar sig på partnerskap, samarbetsramar och nätverk för informationsutbyte.
- Bilaterala avtal.
- Multilaterala avtal.
- Medverkan i internationella forum/sammanslutningar.
- Offentlig-privata partnerskap.
- Partnerskap inom och mellan organ.
- Bästa praxis.

Bedömningsmetod

GCI är ett självutvärderingsverktyg uppbyggt med hjälp av[30] binära, förkodade och öppna undersökningsfrågor. Användningen av binära svar eliminerar opinionsbaserad utvärdering och eventuella fördomar mot vissa typer av svar. De förkodade svaren sparar tid och möjliggör en mer exakt dataanalys. Dessutom möjliggör en enkel, dikotom skala en snabbare och mer komplex utvärdering eftersom den inte kräver långa svar. På så sätt kan svars- och utvärderingsprocessen bli snabbare, effektivare och mer strömlinjeformad. Respondenten bör endast bekräfta förekomsten eller avsaknaden av vissa i förväg identifierade cybersäkerhetslösningar. En onlinemekanism för enkäter, som används för att samla in svar och ladda upp relevant material, gör det möjligt för en expertpanel att ta fram god praxis och tematiska, kvalitativa utvärderingar.

Den övergripande GCI-processen genomförs på följande sätt:

- En inbjudan skickas till alla deltagare med information om initiativet och en begäran om en kontaktpunkt med ansvar för att samla in alla relevanta uppgifter och fylla i GCI-frågeformuläret online. Under onlineundersökningen inbjuds den godkända kontaktpunkten officiellt av ITU att besvara frågeformuläret.
- Insamling av primära uppgifter (för länder som inte besvarat frågeformuläret):
  - ITU utarbetar ett första utkast till svar på frågeformuläret med hjälp av offentligt tillgängliga uppgifter och efterforskningar på nätet.
  - Utkastet till frågeformuläret skickas till kontaktpunkterna för granskning.
  - Kontaktpunkterna korrigerar eventuella felaktigheter och returnerar sedan utkastet.
  - Det korrigerade utkastet till frågeformulär skickas till varje kontaktpunkt för slutligt godkännande.
  - Det godkända frågeformuläret används för analys, poängsättning och rangordning.
- Sekundär datainsamling (för länder som besvarat frågeformuläret):
  - ITU identifierar eventuella uteblivna svar, styrkande dokument, länkar etc.
  - Kontaktpunkten rättar felaktiga svar vid behov.
  - Det korrigerade utkastet till frågeformulär skickas till varje kontaktpunkt för slutligt godkännande.
  - Det godkända frågeformuläret används för analys, poängsättning och rangordning.

A.10 Cyber Power Index (CPI)

Cyber Power Index (CPI) skapades genom forskningsprogrammet Economist Intelligence Unit och finansierades av Booz Allen Hamilton 2011. CPI är en ”dynamisk kvantitativ och kvalitativ modell, […] som mäter specifika cybermiljöattribut via fyra drivkrafter för cyberkraft: rättsliga och reglerande ramar, ekonomisk och social kontext, teknisk infrastruktur och industriell tillämpning, som undersöker digitala framsteg inom nyckelindustrier”[31] . Målet med Cyber Power Index är att jämföra G20-ländernas förmåga att stå emot cyberattacker och bygga ut den digitala infrastruktur som krävs för en blomstrande och säker ekonomi. Den referenspunkt som tillhandahålls av CPI är inriktat på 19 G20-länder (exklusive EU). Indexet rangordnar sedan länderna för varje indikator.

Attribut och dimensioner

Cyber Power Index (CPI) är baserat på fyra drivkrafter för cyberkraft. Varje kategori mäts sedan med hjälp av flera indikatorer för att ge varje land en specifik poäng. De kategorier och pelare som används är:

- **Rättslig ram och regelverk**
  - Statligt cyberutvecklingsåtagande

[30] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv4/GCIv4_English.pdf
[31] www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/EIU%20-%20Cyber%20Power%20Index%20Findings%20and%20Methodology.pdf

- Föreskrifter för it-skydd
- Cybercensur (eller brist på sådan)
- Politisk effektivitet
- Skydd av immateriella rättigheter

ii **Ekonomisk och social kontext**

- Utbildningsnivåer
- Tekniska färdigheter
- Öppenhet inom handeln
- Grad av innovation i företagsklimatet

iii **Teknisk infrastruktur**

- Tillgång till informations- och kommunikationsteknik
- Informations- och kommunikationsteknikens kvalitet
- Informations- och kommunikationsteknikens överkomlighet
- Utgifter för informationsteknik
- Antal säkra servrar

iv **Branschtillämpning**

- Smarta nät
- E-hälsa
- E-handel
- Intelligenta transporter
- E-förvaltning

Bedömningsmetod

CPI är en kvantitativ och kvalitativ poängsättningsmodell. Bedömningen gjordes av Economist Intelligence Unit (EIU) med hjälp av kvantitativa indikatorer från tillgängliga statistiska källor. Uppskattningar gjordes när uppgifter saknades. De viktigaste källorna som används är Economist Intelligence Unit, Förenta nationernas organisation för utbildning, vetenskap och kultur, (Unesco), Internationella teleunionen (ITU) och Världsbanken.

A.11 Cyber Power Index (CPI)

Det här avsnittet sammanfattar de viktigaste analysresultaten av de befintliga mognadsmodellerna. Tabell 5: Översikt över analyserade mognadsmodeller ger en översikt över de viktigaste egenskaperna hos varje modell enligt den modifierade Beckermodellen. 6 Tabelljämförelse av mognadsnivåer högnivådefinitioner av de analyserade modellernas mognadsnivåer. Tabell 7 ger en översikt över de dimensioner eller attribut som används i varje modell.

Tabell 5: Översikt över analyserade mognadsmodeller

Modellens namn	Institution	Syfte	Mål	Antal nivåer	Antal attribut	Bedömningsmetod	Resultatrepresentation
Mognadsmodell för nationell cybersäkerhetskapacitet (CMM)	Globalt kompetenscentrum för cybersäkerhet (Global Cybersecurity Capacity Centre) Universitet i Oxford	Öka kapacitetsuppbyggnadens omfattning och effektivitet inom cybersäkerhet internationellt	Länder	5	5 huvuddimensioner	Samarbete med en lokal organisation för att finjustera modellen innan den tillämpas i en nationell kontext	Femsektionsradar
Mognadsmodell för cybersäkerhetskapacitet (C2M2)	USA:s energidepartement	Hjälpa organisationer att utvärdera och förbättra sina cybersäkerhetsprogram och stärka sin operativa motståndskraft	Organisationer inom alla sektorer, av alla typer och storlekar	4	10 huvuddomäner	Metod för självutvärdering och verktygslåda	Poängkort med cirkeldiagram
Ramen för förbättring av cybersäkerheten i kritisk infrastruktur	Nationella standardiserings- och teknikinstitutet (NIST – National Institute of Standards and Technology)	Ramverk som syftar till att vägleda cybersäkerhetsaktiviteter och hantera risker inom organisationer	Organisationer	Inte tillämpligt (4 skikt)	5 kärnfunktioner	Självutvärdering	-
Qatars mognadsmodell för cybersäkerhetskapacitet (Q-C2M2)	College of Law vid Qatars universitet	Tillhandahåller en fungerande modell som kan användas för benchmarking, mätning och utveckling av Qatars cybersäkerhetsram	Organisationer i Qatar	5	5 huvuddomäner	–	-
Certifiering av mognadsmodell för cybersäkerhet (CMMC)	USA:s försvarsdepartement	Främja cybersäkerhet och bästa praxis för att skydda information	Organisationer inom försvarsindustrins bassektor	5	17 huvuddomäner	Bedömning av utomstående revisorer	-
Samhällsmodell för cybersäkerhetsmognad (CCSMM)	Centre for Infrastructure Assurance and Security University of Texas	Fastställa den nuvarande statusen för ett samhälle i fråga om dess cyberberedskap och tillhandahålla en färdplan för samhällen att följa i sina förberedelseinsatser	Samhällen (kommuner eller regeringar)	5	6 huvuddimensioner	Bedömning inom samhällen med stöd från statliga och federala brottsbekämpande organ	-
Mognadsmodell för informationssäkerhet för NIST cybersäkerhetsramverk (ISMM)	College of Computer Sciences and Engineering King Fahd University of Petroleum and Minerals, Dhahran, Saudiarabien	Att göra det möjligt för organisationer att mäta framstegen i genomförandet över tid för att säkerställa att de upprätthåller önskad säkerhetshållning	Organisationer	5	23 utvärderade områden	–	-
Modell för internrevisionskapacitet (IA-CM) för den offentliga sektorn	Institutet för internrevisorers forskningsstiftelse (The Institute of Internal auditors Research Foundation)	Bygga upp intern revisionskapacitet och opinionsbildning genom internutvärdering inom den offentliga sektorn	Organisationer inom den offentliga sektorn	5	6 element	Självutvärdering	-
Globalt cybersäkerhetsindex (GCI)	Internationella teleunionen (ITU)	Att se över åtagandet och situationen när det gäller cybersäkerhet och hjälpa länder att identifiera	Länder	Inte tillämpligt	5 pelare	Självutvärdering	Rangordningstabell

		cybersäkerhetsområden som kan förbättras.					
Cyber Power Index (CPI)	The Economist Intelligence Unit & Booz, Allen Hamilton	Att jämföra G20-ländernas förmåga att stå emot cyberattacker och bygga ut den digitala infrastruktur som krävs för en blomstrande och säker ekonomi.	G20-länderna	Inte tillämpligt	4 kategorier	Benchmarking av Economist Intelligence Unit	Rangordningstabell

6 Tabelljämförelse av mognadsnivåer

Modell	Nivå 1	Nivå 2	Nivå 3	Nivå 4	Nivå 5
Mognadsmodell för nationell cybersäkerhetskapacitet (CMM)	**Uppstartsfas** Antingen har cybersäkerheten ännu inte mognat eller så är den ännu mycket outvecklad. Det kan förekomma inledande diskussioner om kapacitetsuppbyggnad inom cybersäkerhet, men inga konkreta åtgärder har ännu vidtagits. Det saknas i detta skede observerbara bevis.	**Formativ fas** Vissa aspektinslag har börjat växa fram och formuleras men kan fortfarande vara tillfälliga, oorganiserade, illa definierade eller helt enkelt ”nya”. Det kan dock tydligt påvisas att det finns bevis för denna verksamhet.	**Etablerad fas** Aspekternas olika delar är på plats och fungerar. Det tas dock ingen väl genomtänkt hänsyn till den relativa fördelningen av resurser. Det har inte gjorts någon större avvägning i beslutsfattandet när det gäller de ”relativa” investeringarna i de olika delarna av aspekten. Denna aspekt är dock funktionell och definierad.	**Strategisk fas** Val har gjorts avseende vilka delar av aspekten som är viktiga och vilka som är mindre viktiga för den aktuella organisationen eller det aktuella landet. Det strategiska stadiet återspeglar det faktum att dessa val har gjorts, beroende på nationens eller organisationens omständigheter.	**Dynamisk fas** Det finns tydliga mekanismer för att ändra strategin beroende på de rådande omständigheterna, såsom hotmiljöns teknik, globala konflikter eller en betydande förändring inom ett visst problemområde (t.ex. it-brottslighet eller integritetsskydd). Dynamiska organisationer har utvecklat metoder för att stegvis förändra strategier. Snabba beslut, omfördelning av resurser och ständig uppmärksamhet på den föränderliga miljön är en del av detta skede.
Mognadsmodell för cybersäkerhetskapacitet (C2M2)	**MIN0** Inga förfaranden utförs.	**MIN1** Inledande förfaranden utförs, men kan vara av tillfällig art.	**MIN2** Förvaltningens egenskaper: Förfarandena dokumenteras. Tillräckliga resurser tillhandahålls för att stödja processen. Personal som utför förfarandena har tillräckliga färdigheter och kunskaper. Ansvar och behörighet för att utföra förfarandena tilldelas. Tillvägagångssättets egenskaper: Metoderna är mer fullständiga eller avancerade än vid MIN1.	**MIN3** Förvaltningens egenskaper: Verksamheten styrs av policyer (eller andra organisationsdirektiv). Prestationsmål för domänaktiviteter fastställs och övervakas för att spåra uppnådda resultat. Dokumenterade förfaranden för domänaktiviteter standardiseras och förbättras inom hela organisationen. Tillvägagångssättets egenskaper: Övningarna är mer fullständiga eller avancerade än vid MIN2.	–

Mognadsmodell för informationssäkerhet för NIST:s cybersäkerhetsramverk (ISMM)	Genomförd process	Hanterad process	Etablerad process	Förutsägbar process	Optimeringsprocess
Qatars mognadsmodell för cybersäkerhetskapacitet (Q-C2M2)	**Initieringsstadiet** Ad hoc-förfaranden och -processer för cybersäkerhet har använts inom vissa av domänerna.	**Utvecklingsstadiet** Policyer och metoder har införts för att utveckla och förbättra cybersäkerhetsåtgärder inom domänområdena i syfte att föreslå nya åtgärder att implementera.	**Genomförandestadiet** Strategier har antagits för att genomföra all cybersäkerhetsverksamhet inom domänerna i syfte att slutföra genomförandet vid en viss tidpunkt.	**Det anpassningsbara stadiet** Går tillbaka och ser över cybersäkerhetsåtgärder och antar metoder baserade på prediktiva indikatorer som hämtats från tidigare erfarenheter och åtgärder.	**Det flexibla stadiet** Fortsätter att praktisera anpassningsfasen med extra tonvikt på smidighet och snabbhet i genomförandet av aktiviteter inom områdena.
Certifiering av mognadsmodell för cybersäkerhet (CMMC)	**Processer: Genomförda** Eftersom organisationen kanske endast kan utföra dessa rutiner på ett ad hoc sätt och kan eller inte kan förlita sig på dokumentationsprocessens mognad bedöms den inte för nivå 1. **Praxis: Grundläggande cyberhygien** Nivå 1 är inriktad på skyddet av federal kontraktainformation och består endast av metoder som motsvarar de grundläggande skyddskraven.	**Processer: Dokumenterade** Nivå 2 kräver att en organisation fastställer och dokumenterar metoder och policyer för att vägleda genomförandet av sina CMMC-insatser. Dokumentationen över förfaranden gör det möjligt för enskilda att utföra dem på ett sätt som kan upprepas. Organisationerna utvecklar mogen kapacitet genom att dokumentera sina processer och sedan tillämpa dem som dokumenterade. **Praxis: Medelgod cyberhygien** Nivå 2 som ett utvecklingssteg mellan nivå 1 och nivå 3 som ett utvecklingssteg mellan nivå 1 och nivå 3 i NIST SP 800–171 samt praxis från andra standarder och referenser.	**Processer: Hanterade** Nivå 3 kräver att en organisation upprättar, upprätthåller och levererar en plan som visar hur åtgärderna styrs för att genomföras rent praktiskt. Planen kan innehålla information om uppdrag, mål, projektplaner, resurser, nödvändig utbildning och berörda intressenters deltagande. **Praxis: God cyberhygien** Nivå 3 inriktar sig på skydd av kontrollerade oklassificerade uppgifter (CUI) och omfattar samtliga säkerhetskrav som anges i NIST SP 800-171 samt ytterligare praxis från andra standarder och referenser för att minimera hot.	**Processer: Granskade** Nivå 4 kräver att en organisation granskar och mäter metoder för att utvärdera deras effektivitet. Förutom att mäta effektiviteten kan organisationer på denna nivå vid behov vidta korrigerande åtgärder och regelbundet informera ledningen på högre nivå om status eller uppkomna frågor. **Praxis: Proaktiva** Nivå 4 är inriktad på skyddet av kontrollerade oklassificerade uppgifter (CUI) och omfattar en undergrupp av de skärpta säkerhetskraven. Dessa metoder stärker en organisations förmåga att upptäcka, reagera på och anpassa sig till ändrade taktiker, tekniker och förfaranden.	**Processer: Optimering** Nivå 5 kräver att en organisation standardiserar och optimerar genomförandet av processen i hela organisationen. **Praxis: Avancerade/proaktiva** Nivå 5 inriktar sig på skyddet av kontrollerade oklassificerade uppgifter (CUI) Övriga förfaranden säkerställer att cybersäkerhetsförmågan blir mer avancerad och grundligt genomförd.
Samhällsmodell för cybersäkerhetsmognad (CCSMM)	**Säkerhetsmedvetenhet** Det viktigaste motivet för åtgärder på denna nivå är att göra individer och organisationer medvetna om hot, problem och frågor relaterade till cybersäkerhet	**Processutveckling** Nivå utformad för att hjälpa samhällen att etablera och förbättra de säkerhetsprocesser som krävs för att effektivt åtgärda cybersäkerhetsfrågor.	**Möjliggörande av informationsutbyte** Utformad för att förbättra mekanismerna för informationsutbyte inom samhället för att göra det möjligt att effektivt korrelera information som till synes saknar samband.	**Taktikutveckling** Elementen på denna nivå är utformade för att utveckla bättre och mer proaktiva metoder för att upptäcka och hantera attacker. På denna nivå bör de flesta förebyggande metoder finnas på plats.	**Full operativ säkerhetskapacitet** Denna nivå representerar de element som bör vara på plats för att en organisation ska kunna anses vara fullt operativt redo att gripa sig an alla typer av cyberhot.
Modell för internrevisionskapacitet (IA-CM) för den offentliga sektorn	**Inledande** Ingen hållbar, repeterbar kapacitet – beroende av individuella insatser	**Infrastruktur** Hållbara och repeterbara metoder och förfaranden	**Integrerad** Förvaltning och yrkespraktik tillämpas enhetligt	**Hanterad** Integrerar information från hela organisationen för att förbättra styrning och riskhantering	**Optimering** Lärdomar hämtas inifrån och utifrån organisationen för kontinuerlig förbättring

Tabell 7: Jämförelse av attribut och dimensioner

	Mognadsmodell för nationell cybersäkerhetskapacitet (CMM)	**Mognadsmodell för cybersäkerhetskapacitet (C2M2)**	**Qatars mognadsmodell för cybersäkerhetskapacitet (Q-C2M2)**	**Certifiering av mognadsmodell för cybersäkerhet** (CMMC)	**Certifiering av mognadsmodell för cybersäkerhet** (CMMC)	**Mognadsmodell för informationssäkerhet för NIST:s cybersäkerhetsramverk (ISMM)**	**Ramen för förbättring av cybersäkerheten i** kritisk infrastruktur	**Globalt cybersäkerhetsindex (GCI)**	**Cyber Power Index (CPI)**
Nivåer	Fem dimensioner uppdelade i ett flertal faktorer, däribland flera aspekter och indikatorer(Bild 4)	Tio domäner, inklusive ett särskilt mål för ledningen och flera mål avseende tillvägagångssätt (Bild 6)	Fem domäner uppdelade i underdomäner	Sjutton domäner uppdelade i processer och en eller flera kapaciteter som sedan specificeras i förfaranden (Bild 9).	Sex huvuddimensioner	23 bedömda områden	Fem funktioner med underliggande nyckelkategorier och underkategorier (Bild).	Fem pelare med flera indikatorer	Fyra kategorier med flera indikatorer
Attribut och dimensioner	i Utforma en policy och en strategi för cybersäkerhet ii Uppmuntra en ansvarsfull cybersäkerhetskultur i samhället iii Utveckla kunskap om cybersäkerhet iv Skapa effektiva rättsliga ramar och regelverk v Riskkontroll genom standarder, organisationer och teknik	i Riskhantering ii Hantering av tillgångar, ändringar och konfigurationer iii Identitets- och åtkomsthantering iv Hantering av hot och sårbarhet v Situationsmedvetenhet vi Respons vid händelser och incidenter vii Hantering av försörjningskedjan och externa beroenden viii Personalförvaltning ix Cybersäkerhetsarkitektur x Hantering av cybersäkerhetsprogram	i Förstå (cyberstyrning, tillgångar, risker och utbildning) ii Säkra (säkra data, teknik, tillträdeskontroll, kommunikation och personal) iii Exponering (övervakning, incidentinsatser, detektering, analys och exponering) iv Svara (responsplanering, begränsning och responskommunikation) v Bibehålla (återhämtningsplanering, kontinuitetshantering, förbättring och externa beroenden)	i Tillträdeskontroll ii Tillgångsförvaltning iii Revision och ansvarsskyldighet iv Medvetenhet och utbildning v Konfigurationsledning vi Identifiering och autentisering vii Incidentinsatser viii Underhåll ix Medieskydd x Personalsäkerhet xi Fysiskt skydd xii Återhämtning xiii Riskhantering xiv Säkerhetsbedömning xv Situationsmedvetenhet xvi System- och kommunikationsskydd xvii System- och informationsintegritet	i Hot som hanterats/åtgärdats ii Mått iii Informationsutbyte iv Teknik v Fortbildning vi Test	i Tillgångsförvaltning ii Företagsmiljö iii Styrning iv Riskbedömning v Riskhanteringsstrategi vi Bedömning av överensstämmelse vii Tillträdeskontroll viii Medvetenhet och utbildning ix Datasäkerhet x Informationsskyddsprocesser och -förfaranden xi Underhåll xii Skyddande teknologi xiii Anomalier och händelser xiv Kontinuerlig säkerhetsövervakning xv Detekteringsprocesser xvi Responsplanering xvii Responskommunikation xviii Responsanalys xix Nedsatt respons xx Responsförbättringar xxi Återhämtningsplanering xxii Återhämtningsförbättringar xxiii Återhämtningskommunikation	i Identifiera ii Skydda iii Upptäcka iv Svara v Återställa	i Juridiskt ii Tekniskt iii Organisatoriskt iv Kapacitetsuppbyggnad v Samarbete	i Rättslig ram och regelverk ii Ekonomisk och social kontext iii Teknisk infrastruktur iv Branschtillämpning

BILAGA B – BIBLIOGRAFI ÖVER SKRIVBORDSUNDERSÖKNINGAR

Almuhammadi, S. and Alsaleh, M. (2017) 'Information Security Maturity Model for Nist Cyber Security Framework', in Computer Science & Information Technology (CS & IT). Sixth International Conference on Information Technology Convergence and Services, Academy & Industry Research Collaboration Center (AIRCC).

Almuhammadi, S. and Alsaleh, M. (2017) 'Information Security Maturity Model for Nist Cyber Security Framework', in Computer Science & Information Technology (CS & IT). Tillgänglig på: https://airccj.org/CSCP/vol7/csit76505.pdf

Anna, S. et al. (2016) Stocktaking, analysis and recommendations on the protection of CIIs. Tillgänglig på: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0415821:EN:HTML

Becker, J., Knackstedt, R. et al. (2009) Developing Maturity Models for IT Management – A Procedure Model and its Application. Tillgänglig på: https://link.springer.com/content/pdf/10.1007/s12599-009-0044-5.pdf.

Belgian Government (2012) Cyber Security Strategy. Tillgänglig på: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/belgian-cyber-security-strategy/@@download_version/a9d8b992ee7441769e647ea7120d7e67/file_en

Bellasio, J. et al. (2018) Developing Cybersecurity Capacity: A proof-of-concept implementation guide. RAND Corporation. Tillgänglig på: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2072/RAND_RR2072.pdf

Bourgue, R. (2012) 'Introduction to Return on Security Investment'.

Carnegie Mellon University Software Engineering Institute Pittsburgh United States (2019) "Cybersecurity Capability Maturity Model (C2M2) Version 2.0. Tillgänglig på: https://apps.dtic.mil/sti/pdfs/AD1078768.pdf

Center for Security Studies (CSS), ETH Zürich (2019) National Cybersecurity Strategies in Comparison – Challenges for Switzerland. Tillgänglig på: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-08-National%20Cybersecurity%20Strategies%20in%20Comparison.pdf

Ministerrådet (2019), Portugals officiella tidning, serie 1 – nr 108 – Ministerrådets resolution nr 92/2019. Tillgänglig på: https://cncs.gov.pt/content/files/portugal_-_ncss_2019_2023_en.pdf

Creese, S. (2016) Cybersecurity Capacity Maturity Model for Nations (CMM). University of Oxford.

CSIRT Maturity - Self-assessment Tool (inte daterad). Tillgänglig på: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey

CyberCrime@IPA project of the Council of Europe and the European Union, Global Project on Cybercrime of the Council of Europe and European Union Cybercrime Task Force (2011) Specialised cybercrime units - Good practice study. Tillgänglig på: https://rm.coe.int/2467-htcu-study-v30-9nov11/16802f6a33

Cybersecurity Incident Report and Analysis System – Visual Analysis Tool (rapport om cyberincidenter och analyssystem – verktyg för visuell analys) (inte daterad). Tillgänglig på: https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

Darra, E. (2017) Public Private Partnerships (PPP).

Darra, E. (inte daterad) 'Welcome to the NCSS Training Tool'.

Dekker, M. A. C. (2014) Technical Guideline on Incident Reporting. Tillgänglig på: https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/Article_13a_ENISA_Technical_Guideline_On_Incident_Reporting_v2_1.pdf

Dekker, M. A. C. (2014) Technical Guideline on Security Measures. Tillgänglig på: https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf

Dekker, M. A. C. (2015) Guideline on Threats and Assets. Tillgänglig på: https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets/Guideline_on_Threats_and_Assets_v_1_1.pdf

Digital Slovenia (2016) Cybersecurity Strategy. Tillgänglig på: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-slovenia

Domingo-Ferrer, J. *et al.* (2014) *Privacy and data protection by design - from policy to engineering.* Finns på: http://bookshop.europa.eu/uri?target=EUB:MEDDELANDE:TP0514111:EN:HTML

Europeiska kommissionens förordning (2012) om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden. Tillgänglig på: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX: 52012PC0238&from=SV

Europeiska byrån för nät- och informationssäkerhet (2012). NCSS: Practical Guide on Development and Execution. Heraklion: Enisa

Europeiska byrån för nät- och informationssäkerhet (2012). NCSS: Setting the course for national efforts to strengthen security in cyberspace. Heraklion: Enisa

Europeiska byrån för nät- och informationssäkerhet (2016). Guidelines for SMEs on the security of personal data processing.

Europeiska byrån för nät- och informationssäkerhet (2016) NCSS good practice guide: designing and implementing national cyber security strategies. Heraklion: Enisa

Europeiska byrån för nät- och informationssäkerhet (2017) Handbook on security of personal data processing. Tillgänglig på: http://dx.publications.europa.eu/10.2824/569768

Europeiska byrån för nät- och informationssäkerhet (2014) *ENISA CERT inventory inventory of CERT teams and activities in Europe*. Finns på http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe

Executive Office Of The President (2015) Memorandum for Heads of Executive Departments and Agencies. Tillgänglig på: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-04.pdf

Österrikes federala kansli (2013). Österrikes cybersäkerhetsstrategi. Tillgänglig på: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/austrian-cyber-security-strategy/@@download_version/1573800e2e4448b9bdaead56a590305a/file_en

Förbundsinrikesministeriet (2011), Tysklands cybersäkerhetsstrategi. Tillgänglig på: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany/@@download_version/8adc42e23e194488b2981ce41d9de93e/file_sv

Feette, L. (2016) NIS Directive and national (2015) Information security and privacy standards for SMEs: recommendations to improve the adoption of information security and privacy standards in small and medium enterprises. Tillgänglig på: http://bookshop.europa.eu/uri?target=EUB:MEDDELANDE:TP0215977:SV:HTML

Ferette, L., European Union and European Network and Information Security Agency (2015) The 2015 report on national and international cyber security exercises: survey, analysis and recommendations. Tillgänglig på: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115948:EN:HTML

Franska premiärministerns kansli (2014). Frankrikes nationella strategi för digital säkerhet. Tillgänglig på: https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf

Galan Manso, C. et al. (2015) Information security and privacy standards for SMEs: recommendations to improve the adoption of information security and privacy standards in small and medium enterprises. Tillgänglig på: http://bookshop.europa.eu/uri?target=EUB:MEDDELANDE:TP0215977:SV:HTML

Gent University et al. (2017) 'Evaluating Business Process Maturity Models', Journal of the Association for Information Systems. Tillgänglig på: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1775&context=jais

Bulgariens regering (2015), Nationell cybersäkerhetsstrategi – ett cybersäkert Bulgarien 2020.

Kroatiens regering (2015). Republiken Kroatiens nationella strategi för cybersäkerhet. Tillgänglig på: https://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf

Greklands regering (2017). Nationell cybersäkerhetsstrategi. Tillgänglig på: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-greece/view

Ungerns regering (2018). Strategi för säkra nät- och informationssystem. Tillgänglig på: https://www.kormany.hu/download/2/f9/81000/Strat%C3%A9gia%20honlapon%20k%C3%B6zz%C3%A9t%C3%A9telre-20180103_4829494_2_20190103130721.pdf#!DocumentBrowse

Irlands regering (2019). Nationell cybersäkerhetsstrategi. Tillgänglig på: https://www.dccae.gov.ie/documents/National_Cyber_Security_Strategy.pdf

Spaniens regering (2019). Nationell cybersäkerhetsstrategi. Tillgänglig på: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/the-national-security-strategy/@@download_version/5288044fda714a58b5ca6472a4fd1b28/file_sv

Institutet för internrevisorer (red.) (2009) Internrevisionskapacitetsmodell (IA-CM) för den offentliga sektorn: översikt och tillämpningsvägledning. Altamonte Springs, Fla: Institutet för internrevisorers forskningsstiftelse

Internationella teleunionen (ITU) (2018). Globalt cybersäkerhetsindex. Tillgänglig på: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Internationella teleunionen (ITU) (2018). Vägledning för att utveckla en nationell strategi för cybersäkerhet. Tillgänglig på: https://ccdcoe.org/uploads/2018/10/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

J.D., R. D. B. (2019) 'Towards a Qatar Cybersecurity Capability Maturity Model with a Legislative Framework', International Review of Law.

Lettlands regering (2014). Cybersäkerhetsstrategi för Lettland. Tillgänglig på: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss

Liveri, D. et al. (2014) An evaluation framework for national cyber security strategies. Heraklion: Enisa Tillgänglig på: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0714017:EN:HTML.

Mattioli, R. *et al.* (2014) *Methodologies for the identification of critical information infrastructure assets and services: guidelines for charting electronic data communication networks.* Finns på: http://bookshop.europa.eu/uri?target=EUB:MEDDELANDE:TP0614120:EN:HTML

Ministeriet för konkurrens och digital, marin och tjänsteekonomi (2016) Maltas cybersäkerhetsstrategi. Tillgänglig på: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-of-malta

Ekonomi- och kommunikationsministeriet (2019). Cybersäkerhetsstrategi – Estland. Tillgänglig på: https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

Republiken Litauens försvarsministerium (2018). Nationell strategi för cybersäkerhet.

Nationellt cybersäkerhetscentrum (2015). Tjeckiens nationella cybersäkerhetsstrategi. Tillgänglig på: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf

Nationella cybersäkerhetsstrategier – Interaktiv karta (inte daterad). Tillgänglig på: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map

Utvärderingsverktyg för nationella cybersäkerhetsstrategier (2018). Tillgänglig på: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool

Nationella standardiserings- och teknikinstitutet (2018). Ramverket för förbättring av den kritiska infrastrukturens cybersäkerhet, version 1.1. Gaithersburg, MD: Nationella institutet för standarder och teknik. Tillgänglig på: http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Object Management Group (2008) Business Process Maturity Model. Tillgänglig på: https://www.omg.org/spec/BPMM/1.0/PDF

OECD, Europeiska unionen och gemensamma forskningscentret – Europeiska kommissionen (2008) Handbook on Constructing Composite Indicators: Methodology and User Guide. OECD Tillgänglig på: https://www.oecd.org/sdd/42495745.pdf.

Cyperns kommissariat för elektronisk kommunikation och postförordningar (2012), cybersäkerhetsstrategi.

Europeiska unionens officiella tidning (2008) RÅDETS DIREKTIV 2008/114/EG av den 8 december 2008 om identifiering och klassificering av europeisk kritisk infrastruktur och bedömning av behovet av att förbättra skyddet av denna. Tillgänglig på: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN

Organisationen för ekonomiskt samarbete och utveckling (OECD) (2012) Cybersecurity policy making at a turning point. Tillgänglig på: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

Ouzounis, E. (2012) 'National Cyber Security Strategies - Practical Guide on Development and Execution'.

Ouzounis, E. (2012) Good Practice Guide on National Exercises.

Portesi, S. (2017) Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects

Ministerrådets ordförandeskap (2017). Den italienska handlingsplanen för cybersäkerhet. Tillgänglig på: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-strategic-framework-for-cyberspace-security

Rady Ministrów (2019) Dziennik Urzędowy Rzeczypospolitej Polskiej. Tillgänglig på: http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf

Rumäniens regering (2013). Rumäniens cybersäkerhetsstrategi. Tillgänglig på: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-romania

Sarri, A., Kyranoudi, P. and European Union Agency for Cybersecurity (2019) Good practices in innovation on cybersecurity under the NCSS: good practices in innovation on cybersecurity under the national cyber security strategies. Tillgänglig på: https://op.europa.eu/publication/manifestation_identifier/PUB_TP0119830ENN.

Säkerhetskommitténs sekretariat (2019). Finlands cybersäkerhetsstrategi 2019. Tillgänglig på: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf

Den Slovakiska regeringen (2015). Slovakiska republikens cybersäkerhetskoncept. Tillgänglig på: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-concept-of-the-slovak-republic

Smith, R. (2015), Europaparlamentets och rådets förordning (EU) 2010/41 av den 7 juli 2010.

Smith, R. (2016), Europaparlamentets och rådets förordning (EU) 2010/41 av den 7 juli 2010 i Smith, R., Core EU Legislation. London: Macmillan Education. Tillgänglig på: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX: 32016L1148&from=EN.

Stavropoulos, V. (2017) European Cyber Security Month 2017.

Sveriges regering (2017). Nationell strategi för samhällets informations- och cybersäkerhet. Tillgänglig på: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/swedish-ncss/view

Danmarks regering – Finansministeriet (2018). Dansk strategi för it- och informationssäkerhet. Tillgänglig på: https://en.digst.dk/media/17189/danish_cyber_and_information_security_strategy_pdf.pdf

Förbundsrådet (2018) Nationell strategi för skydd av Schweiz mot cyberrisker.

Luxemburgs regeringsråd (2018). Nationell strategi för cybersäkerhet. Tillgänglig på: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/strategie-nationale-en-matiere-de-cyber-securite/@@download_version/d4af182d7c6e4545ae751c17fcca9cfe/file_en

Den nederländska regeringen (2018). Nationell agenda för cybersäkerhet. Tillgänglig på: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-

security-strategies-interactive-map/strategies/national-cyber-security-strategy-1/@@download_version/82b3c1a34de449f48cef8534b513caea/file_en

Vita huset (2018). Nationell cybersäkerhetsstrategi för Amerikas förenta stater. Tillgänglig på: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Trimintzios, P., et al. (2011) Cyber Europe Report. Tillgänglig på: https://www.enisa.europa.eu/publications/ce2010report

Trimintzios, P., Gavrila, R. and European Network and Information Security Agency (2013) *National-level risk assessments: an analysis report.* Finns på: http://bookshop.europa.eu/uri?target=EUB:MEDDELANDE:TP0413112:EN:HTML

Trimintzios, P., Gavrila, R., et al. (2015) Report on cyber-crisis cooperation and management. Tillgänglig på: http://bookshop.europa.eu/uri?target=EUB:MEDDELANDE:TP0514030:SV:HTML

Trimintzios, P., Ogee, A., et al. (2015) Report on cyber crisis cooperation and management: common practices of EU-level crisis management and applicability to cyber crises. Tillgänglig på: http://bookshop.europa.eu/uri?target=EUB:MEDDELANDE:TP0115966:SV:HTML

Storbritanniens nationella cybersäkerhetsstrategi 2016-2021 (2016). Tillgänglig på: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

University of Innsbruck et al. (2009) Understanding Maturity Models.

Wamala, D. F. (2011) 'ITU National Cybersecurity Strategy Guide. Tillgänglig på: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategiGuide.pdf

White, G. (2007) 'The Community Cyber Security Maturity Model', in 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)

BILAGA C – ANDRA UNDERSÖKTA MÅL

Målen nedan studerades som en del av skrivbordsstudiersfasen och de intervjuer som genomfördes av Enisa. Följande mål ingår inte i den nationella ramen för kapacitetsbedömning men belyser trots allt ämnen som är värda att diskutera. Vart och ett av följande underkapitel kommer att ge en förklaring till varför målet avvisades.

- Utveckla sektorsspecifika strategier för cybersäkerhet.
- Bekämpning av desinformationskampanjer.
- Säkra spetsteknik (5G, AI, kvantdatorteknik etc.).
- Säkerställa datasuveränitet.
- Tillhandahålla incitament för utvecklingen av cyberförsäkringssektorn.

Utveckla sektorsspecifika strategier för cybersäkerhet

Införandet av sektorsspecifika strategier inriktade mot sektorsinterventioner och sektorsincitament presenterar utan tvekan en starkare decentraliserad kapacitet. Det gäller inte minst medlemsstater vars leverantörer av samhällsviktiga tjänster måste hantera olika ramar och bestämmelser och där många beroendeförhållanden uppstår på grund av cybersäkerhetens tvärgående karaktär. I flera medlemsstater finns det inte sällan dussintals nationella myndigheter och tillsynsorgan med kunskap om varje sektors särdrag, vilka har mandat att genomdriva särskild lagstiftning för varje sektor.

Danmark införde exempelvis sex riktade strategier för att åtgärda de mest kritiska sektorernas it- och informationssäkerhetsinsatser i syfte att utveckla en starkare decentraliserad kapacitet inom it- och informationssäkerhet. Varje "sektorsenhet" kommer bland annat att bidra till hotbedömningar på sektorsnivå, övervakning, beredskapsövningar, inrättande av säkerhetssystem, kunskapsutbyte och instruktioner. De sektorsspecifika strategierna omfattar följande sektorer:

- Energi
- Hälso- och sjukvård
- Transport
- Telekommunikation
- Finansiering
- Sjöfart

Andra medlemsstater har uttryckt intresse och överväger sektorsspecifika cybersäkerhetsstrategier för att återspegla alla lagstadgade krav. Det bör dock noteras att ett sådant mål inte nödvändigtvis passar alla medlemsstater, beroende på deras storlek, nationella politik och mognadsnivå. Den stora svårigheten att säkerställa att regelverket kan ta hänsyn till alla särdrag ledde till att Enisa inte inkluderade detta mål i regelverket.

Kampen mot desinformationskampanjer

Medlemsstaterna integrerar skyddet av grundläggande principer som mänskliga rättigheter, öppenhet och allmänhetens förtroende i sina nationella strategier för cybersäkerhet. Detta är mycket viktigt, särskilt när det gäller desinformation som sprids via traditionella nyhetsmedier eller sociala medieplattformar. Cybersäkerhet är dessutom en av de största utmaningarna vid

politiska val för närvarande. Aktiviteter som att sprida falsk information eller negativ propaganda har faktiskt observerats i olika länder inför viktiga val. Detta hot kan undergräva EU:s demokratiska process. På EU-nivå har kommissionen utarbetat en handlingsplan[32] för att intensifiera insatserna för att motverka desinformation i Europa. Planen är inriktad på fyra nyckelområden (upptäckt, samarbete, samarbete med nätplattformar och medvetenhet) och syftar till att bygga upp EU:s kapacitet och stärka samarbetet mellan medlemsstaterna.

Fyra av 19 intervjuade länder har uttryckt sin avsikt att åtgärda frågan om desinformation och propaganda i sina nationella strategier för cybersäkerhet.

Exempelvis[33] står följande att läsa i de franska nationella cybersäkerhetsstrategierna: ”Det är statens ansvar att informera medborgarna om de risker för manipulation och propagandametoder som används av skadliga aktörer på internet. Efter terroristattackerna mot Frankrike i januari 2015 inrättade regeringen till exempel en informationsplattform om riskerna med islamisk radikalisering via elektroniska kommunikationsnät: ”Stop-djihadisme.gouv.fr”. Detta tillvägagångssätt skulle kunna utvidgas för att bemöta andra fenomen, som exempelvis propaganda eller destabilisering.

I ett annat exempel[34] uppges i Polens nationella strategier för cybersäkerhet för 2019-2024 att: ”Mot manipulativ verksamhet såsom desinformationskampanjer behövs systematiska åtgärder för att öka medborgarnas medvetenhet såsom kontroll av informations äkthet och respons vid försök att förvränga den.”

Under intervjuer som genomfördes av Enisa framgick emellertid att flera medlemsstater inte tar upp frågan i sina nationella cybersäkerhetsstrategier som ett hot mot cybersäkerheten utan snarare hanterar den på en bredare samhällsnivå, till exempel genom politiska initiativ.

Säker spetsteknik (5G, AI, kvantdatorteknik etc.)

I takt med att det nuvarande cyberhotbilden fortsätter att växa kommer utvecklingen av ny teknik sannolikt att leda till en ökning av intensiteten och antalet cyberattacker och en diversifiering av de metoder, medel och mål som används av de aktörer som hanterar hoten. Under tiden har dessa nya tekniska lösningar i form av spetsteknik potential att bli byggstenarna i den europeiska digitala marknaden. För att skydda medlemsstaternas växande digitala beroende och framväxten av ny teknik bör incitament och färdiga policyer upprättas för att stödja en säker och vederhäftig utveckling och spridning av tekniken inom EU.

Under skrivbordsundersökningen av medlemsstaternas cybersäkerhetsstrategier lades följande nya teknik fram som intressant för medlemsstaterna: 5G, artificiell intelligens, kvantdatorsystem, anslutna och autonoma fordon, stordata och smartdata, blockkedjeteknik, robotteknik och sakernas internet (IoT).

I början av 2020 offentliggjorde Europeiska kommissionen ett meddelande där medlemsstaterna uppmanades att vidta åtgärder för att genomföra den samling åtgärder som rekommenderas i slutsatserna till verktygslådan för cybersäkerheten i 5G-nät[35]. Denna verktygslåda för 5G är en följd av kommissionens rekommendation (EU) 2019/534 om cybersäkerhet i 5G-nät som antogs 2019 och som efterlyste en enhetlig europeisk strategi för säkerheten i 5G-nät[36].

[32] https://ec.europa.eu/digital-single-market/sv/news/action-plan-against-disinformation
[33] https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf
[34] http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf
[35] https://ec.europa.eu/digital-single-market/sv/news/secure-5g-deployment-eu-implementing-eu-toolbox-communication-commission
[36] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019H0534

Under de intervjuer som Enisa genomfört underströks att detta ämne snarare är ett tvärgående ämne som bör behandlas i samtliga nationella cybersäkerhetsstrategier, snarare än ett specifikt mål *i sig*.

Säkerställa datasuveränitet

Å ena sidan kan cyberrymden ses som ett utomordentligt globalt gemensamt utrymme som är lättillgängligt, erbjuder en hög anslutbarhet och stora möjligheter till socioekonomisk tillväxt. Å andra sidan kännetecknas cyberrymden också av sin svaga jurisdiktion, svårigheter att tillskriva handlingar, brist på gränser och sammankopplade system som kan vara porösa och vars data kan stjälas eller till och med bli tillgänglig för främmande makt. Utöver dessa två perspektiv kännetecknas det digitala ekosystemet av en koncentration av nättjänstplattformar och infrastruktur i händerna på ett mycket litet antal intressenter. Alla ovannämnda aspekter sammantagna leder till att medlemsstaterna främjar digital suveränitet. Att uppnå digital suveränitet innebär att medborgare och företag kan blomstra fullt ut genom att använda digitala tjänster och IKT-produkter som är pålitliga utan att behöva känna oro över sina personuppgifter eller digitala tillgångar, sitt ekonomiska oberoende eller sitt politiska inflytande.

Datasuveränitet eller digital suveränitet förespråkas av medlemsstaterna på nationell nivå och på EU-nivå. Medlemsstaterna tycks inte ta upp frågan direkt i sina nationella cybersäkerhetsstrategier som ett specifikt mål, utan tar istället antingen upp den som en övergripande princip eller beskriver sin avsikt att säkerställa digital suveränitet på nationell nivå, vilket beskrivs i ad hoc-publikationer genom att fokusera på nyckelteknologi. I den franska strategiska översynen av cyberförsvaret 2018 konstateras till exempel att ”kontroll av följande tekniker är av yttersta vikt för att säkerställa digital suveränitet: kommunikationskryptering, upptäckt av cyberattacker, professionell mobilradio, molnbaserad databehandling och artificiell intelligens”[37].

På EU-nivå deltar medlemsstaterna aktivt i utformningen av den europeiska datastrategin (COM/2020/66 final) och i uppbyggnaden av EU:s certifieringsram för digitala IKT-produkter, tjänster och processer som inrättades genom EU:s cybersäkerhetsakt (2019/881) för att säkerställa strategisk digital självständighet på europeisk nivå.

Intervjufasen med medlemsstaterna visade att frågan om digital suveränitet ofta betraktas som en bredare fråga än enbart en fråga begränsad till cybersäkerhet. Medlemsstaterna tar därför inte upp ämnet i sina nationella cybersäkerhetsstrategier, och de få som ändå gör det tar inte upp frågan som ett specifikt mål i sig.

Tillhandahålla incitament för utvecklingen av cyberförsäkringssektorn.

Den nuvarande situationen inom cyberförsäkringssektorn visar att den globala marknaden otvivelaktigt har vuxit. Det är dock fortfarande ett tidigt skede, då uppgifter måste samlas in och många prejudikat måste fastställas först (t.ex. tyst täckning, systemiska cyberrisker etc.). Dessutom uppskattas de sammanlagda förlusterna från cyberattacker runt om i världen vara flera storleksordningar högre än den nuvarande täckningskapaciteten för cyberförsäkringssektorn (IMF Working Paper – Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment WP/18/143 (Arbetsdokument från IMF – Cyberrisk för finanssektorn: En ram för kvantitativ bedömning). Utvecklingen av cyberförsäkringssektorn kan dock utan tvekan ge fördelar och lägga grunden för fördelaktiga mekanismer. It-försäkringsmekanismer kan exempelvis bidra till att:

- Öka medvetenheten om företags cybersäkerhetsrisker.

[37] http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf

- Utvärdera exponeringen för cyberrisker på ett kvantitativt sätt.
- Förbättra hanteringen av cybersäkerhetsrisker.
- Ge stöd till organisationer som drabbats av it-attacker.
- Täcka skador (materiella och icke-materiella) som orsakats av en cyberattack.

Vissa medlemsstater har börjat arbeta med denna fråga. Exempel:

- Estland har antagit en "vänta och se-strategi" i sin nationella cybersäkerhetsstrategi: ”För att minska it-riskerna i den privata sektorn i allmänhet kommer efterfrågan och utbudet av it-försäkringstjänster i Estland att analyseras och på grundval av detta kommer man att enas om samarbetsprinciper för närstående parter, inklusive informationsutbyte, utarbetande av riskbedömningar osv. Idag är leverantörer av cyberförsäkringstjänster få på den estniska marknaden och det är nödvändigt att först kartlägga vem som erbjuder vad. Försäkringsskyddets komplexitet betraktas ofta som ett hinder för utvecklingen av it-försäkringsmarknaden."
- Luxemburg stödjer särskilt utvecklingen av cyberförsäkringssektorn i sin nationella cybersäkerhetsstrategi: ”Mål 1: Att skapa nya produkter och tjänster. För att samla risker och uppmuntra offer för digitala cyberincidenter att söka hjälp från experter för att hantera incidenten och återställa ett system som påverkas av en skadlig handling, kommer försäkringsbolagen att uppmuntras att skapa särskilda produkter för it-försäkringsområdet .”

Återkopplingen från de intervjuade personerna var relativt varierande i denna fråga: vissa medlemsstater uppgav att it-försäkringsfrågan nyligen har blivit ett diskussionsämne, medan andra menade att även om ämnet lovar gott så är sektorn ännu inte tillräckligt mogen. Ett stort antal intervjuade förklarade dock att ämnet inte behandlas som en del av den nationella cybersäkerhetsstrategin, antingen för att det ansågs vara alltför specifikt eller för att det inte ansågs ligga inom ramen för den nationella cybersäkerhetsstrategin.

TP-02-21-253-SV-N

Om Europeiska unionens cybersäkerhetsbyrå, Enisa

Europeiska unionens cybersäkerhetsbyrå (Enisa) är ett EU-organ med uppgift att uppnå en hög gemensam nivå av cybersäkerhet i hela Europa. Europeiska unionens cybersäkerhetsbyrå, som grundades 2004 och stärktes genom EU:s cybersäkerhetsakt, bidrar till EU:s cyberpolitik och förbättrar tillförlitligheten hos produkter, tjänster och processer inom IKT genom program för cybersäkerhetscertifiering. Dessutom samarbetar byrån med medlemsstater och andra EU-organ, och hjälper Europa att förbereda sig inför morgondagens cyberutmaningar. Genom kunskapsspridning, kapacitetsuppbyggnad och åtgärder för att öka medvetenheten arbetar byrån tillsammans med sina huvudintressenter för att stärka tillförlitligheten i den uppkopplade ekonomin, motståndskraften i unionens infrastruktur och, mer generellt, för att upprätthålla den digitala säkerheten i Europa och för dess medborgare. För mer information se www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-495-4
DOI: 10.2824/943770