Informationsmöte om certifiering av cybersäkerhet i it-produkter och it-tjänster

15 november 2024

NATIONELLT CYBERSÄKERHETSCENTER

FMV

SWEDAC

Agenda

Inledning av NCSC, Swedac, FMV

EU:s cybersäkerhetslagstiftning

EU-ramverk för certifiering av cybersäkerhet

- IT-produkter (EUCC)
- Ackreditering av Swedac
- Molntjänster (EUCS)
- Utlokaliserade säkerhetstjänster

Nato och NIAPC-listan

Avrundning, Frågor

EU:s arbete med cybersäkerhet

EU:s arbete och policyer kring cybersäkerhet

- KOM-meddelanden (tex. EU-kommissionens cybersäkerhetsstrategi från 2020)
- Rådslutsatser om cybersäkerhet (senaste från 21 maj 2024)

EU-rättsakter om cybersäkerhet

- EU-rättsakter (Rådet/EP- + KOM-akter)
- Sätter sektorsvisa cybersäkerhetskrav
- Certifiering presumtion för kravuppfyllelse
- KOM-riktlinjer

Cybersäkerhetsakten (CSA)

- Enisas mandat
- Certifieringsramverk

- ENISA = Europeiska unionens byrå för cybersäkerhet (www.enisa.eu)
- Ramverket = CSA + certifieringsordningar enligt CSA + ENISA-riktlinjer/vägledning

FMV

Table 1: Overview of EU Legislations in the Digital Sector

Applicable law	Published in the Official Journal of the European Union.
In negotiation	Proposal by the European Commission entered the legislative process.
Planed initiative	Mentioned by the European Commission as potential legislative initiative.

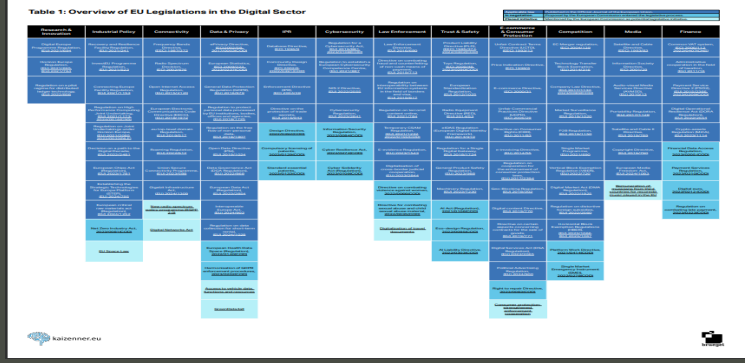
Research & Innovation	Industrial Policy	Connectivity	Data & Privacy	IPR	Cybersecurity	Law Enforcement	Trust & Safety	E-commerce & Consumer Protection	Competition	Media	Finance
Digital Europe Programme Regulation, (EU) 2021/694	Recovery and Resilience Facility Regulation, (EU) 2021/241	Frequency Bands Directive, (EECL) 1987/372	ePrivacy Directive, (EU) 2009/136, 2017/0003(COD)	Database Directive, (EC) 1996/9	Regulation for a Cybersecurity Act, (EU) 2019/881, 2023/0108(COD)	Law Enforcement Directive, (EU) 2016/680	Product Liability Directive (PLD), (EEC) 1985/374, 2022/0302(COD)	Unfair Contract Terms Directive (UCTD), (EC) 1993/13	EC Merger regulation, (EC) 2004/139	Satellite and Cable Directive, (EC) 1993/83	Common VAT system, (EC) 2006/112, 2022/407(CNS)
Horizon Europe Regulation, (EU) 2021/695, (EU) 2021/764	InvestEU Programme Regulation, (EU) 2021/523	Radio Spectrum Decision, (EC) 2002/676	European Statistics, (EC) 2009/223, 2023/0032(COD)	Community Design Directive, (EC) 2002/6, 2022/0392(COD)	Regulation to establish a European Cybersecurity Competence Centre, (EU) 2021/887	Directive on combating fraud and counterfeiting of non-cash means of payment, (EU) 2019/713	Toys Regulation, (EC) 2009/48, 2023/0290(COD)	Price Indication Directive, (EC) 1998/6	Technology Transfer Block Exemption, (EU) 2014/316	Information Society Directive, (EC) 2001/29	Administrative cooperation in the field of taxation, (EU) 2011/16
Regulation on a pilot regime for distributed ledger technology, (EU) 2022/858	Connecting Europe Facility Regulation, (EU) 2021/1153	Open Internet Access Regulation, (EU) 2015/2120	General Data Protection Regulation (GDPR), (EU) 2016/679	Enforcement Directive (IPR), (EC) 2004/48	NIS 2 Directive, (EU) 2022/2555	Regulation on interoperability between EU information systems in the field of borders and visa, (EU) 2019/817	European Standardization Regulation, (EU) 2012/1025	E-commerce Directive, (EC) 2000/31	Company Law Directive, (EU) 2017/1132, 2023/0089(COD)	Audio-visual Media Services Directive (AVMSD), (EU) 2010/13	Payment Service Directive 2 (PSD2), (EU) 2015/2366, 2023/0209(COD)
	Regulation on High Performance Computing Joint Undertaking, (EU) 2021/1173, 2023/0160(NLE)	European Electronic Communications Code Directive (EECC), (EU) 2018/1972	Regulation to protect personal data processed by EU institutions, bodies, offices and agencies, (EU) 2018/1725	Directive on the protection of trade secrets, (EU) 2016/943	Cybersecurity Regulation, (EU) 2019/881	Regulation on terrorist content online, (EU) 2021/784	Radio Equipment Directive (RED), (EU) 2014/53	Unfair Commercial Practices Directive (UCPD), (EC) 2005/29	Market Surveillance Regulation, (EU) 2019/1020	Portability Regulation, (EU) 2017/1128	Digital Operational Resilience Act (DORA Regulation), (EU) 2022/2554
	Regulation on Joint Undertakings under Horizon Europe, (EU) 2021/2085, 2023/0199(NLE)	.eu top-level domain Regulation, (EU) 2019/517	Regulation on the free flow of non-personal data, (EU) 2018/1807	Design Directive, 2022/0392(COD)	Information Security Regulation, 2022/0084(COD)	Temporary CSAM Regulation, (EU) 2021/1232, 2020/0259(COD)	eIDAS Regulation (European Digital Identity Framework), (EU) 2014/910	Directive on Consumer Rights (CRD), (EU) 2011/83	P2B Regulation, (EU) 2019/1150	Satellite and Cable II Directive, (EU) 2019/789	Crypto-assets Regulation (MiCA), (EU) 2022/1114
	Decision on a path to the Digital Decade, (EU) 2022/2481	Roaming Regulation, (EU) 2022/612	Open Data Directive (PSI), (EU) 2019/1024	Compulsory licensing of patents, 2023/0129(COD)	Cyber Resilience Act, 2022/0272(COD)	E-evidence Regulation, (EU) 2023/1543	Regulation for a Single Digital Gateway, (EU) 2018/1724	e-invoicing Directive, (EU) 2014/55	Single Market Programme, (EU) 2021/690	Copyright Directive, (EU) 2019/790	Financial Data Access Regulation, 2023/0205(COD)
	European Chips Act (Regulation), (EU) 2023/1781	Union Secure Connectivity Programme, (EU) 2023/588	Data Governance Act (DGA Regulation), (EU) 2022/868	Standard essential patents, 2023/0133(COD)	Cyber Solidarity Act (Regulation), 2023/0109(COD)	Digitalisation of cross-border judicial cooperation, (EU) 2023/2844	General Product Safety Regulation, (EU) 2023/988	Regulation on cooperation for the enforcement of consumer protection laws, (EU) 2017/2394	Vertical Block Exemption Regulation (VBER), (EU) 2022/720	European Media Freedom Act, (EU) 2024/1083	Payment Services Regulation, 2023/0210(COD)
	Establishing the Strategic Technologies for Europe Platform (STEP), (EU) 2024/795	Gigabit Infrastructure Act, (EU) 2024/1309	European Data Act (Regulation), (EU) 2023/2854			Directive on combating violence against women, 2022/0066(COD)	Machinery Regulation, (EU) 2023/1230	Geo-Blocking Regulation, (EU) 2018/302	Digital Market Act (DMA Regulation), (EU) 2022/1925	Preservation of medicines from third countries for recognised public interest in the EU	Digital euro, 2023/0212(COD)
	European critical raw materials act (Regulation), (EU) 2024/1252	New radio spectrum policy programme (RSPP 2.0)	Interoperable Europe Act, (EU) 2024/903			Directive for combating sexual abuse and child sexual abuse material, 2024/0035(COD)	AI Act (Regulation), 2021/0106(COD)	Digital content Directive, (EU) 2019/770	Regulation on distortive foreign subsidies, (EU) 2022/2560		Regulation on combating late payment, 2023/0323(COD)
	Net Zero Industry Act, 2023/0081(COD)	Digital Networks Act	Regulation on data collection for short-term rental, (EU) 2024/1028			Digitalization of travel documents	Eco-design Regulation, 2022/0095(COD)	Directive on certain aspects concerning contracts for the sale of goods, (EU) 2019/771	Horizontal Block Exemption Regulations (HBER), (EU) 2022/1066, (EU) 2022/1067		
	EU Space Law		European Health Data Space (Regulation), 2022/0140(COD)				AI Liability Directive, 2022/0303(COD)	Digital Services Act (DSA Regulation), (EU) 2022/2065	Platform Work Directive, 2021/0414(COD)		
			Harmonisation of GDPR enforcement procedures, 2023/0202(COD)					Political Advertising Regulation, (EU) 2024/900	Single Market Emergency Instrument (SMEI), 2022/0278(COD)		
			Access to vehicle data, functions and resources					Right to repair Directive, 2023/0083(COD)			
			GreenData4all					Consumer protection: strengthened enforcement cooperation			

kaizenner.eu

bruegel

FMV

EU-rättsakter med cybersäkerhetskrav och kopplingar till certifiering



Cybersecurity

- Regulation for a Cybersecurity Act (CSA), (EU) 2019/881
- NIS2 Directive, (EU) 2022/2555
- Cyber Resilience Act (CRA) (Regulation) 2022/0272(COD)
- Cyber Solidarity Act (CSoA) (Regulation) 2023/0109(COD)

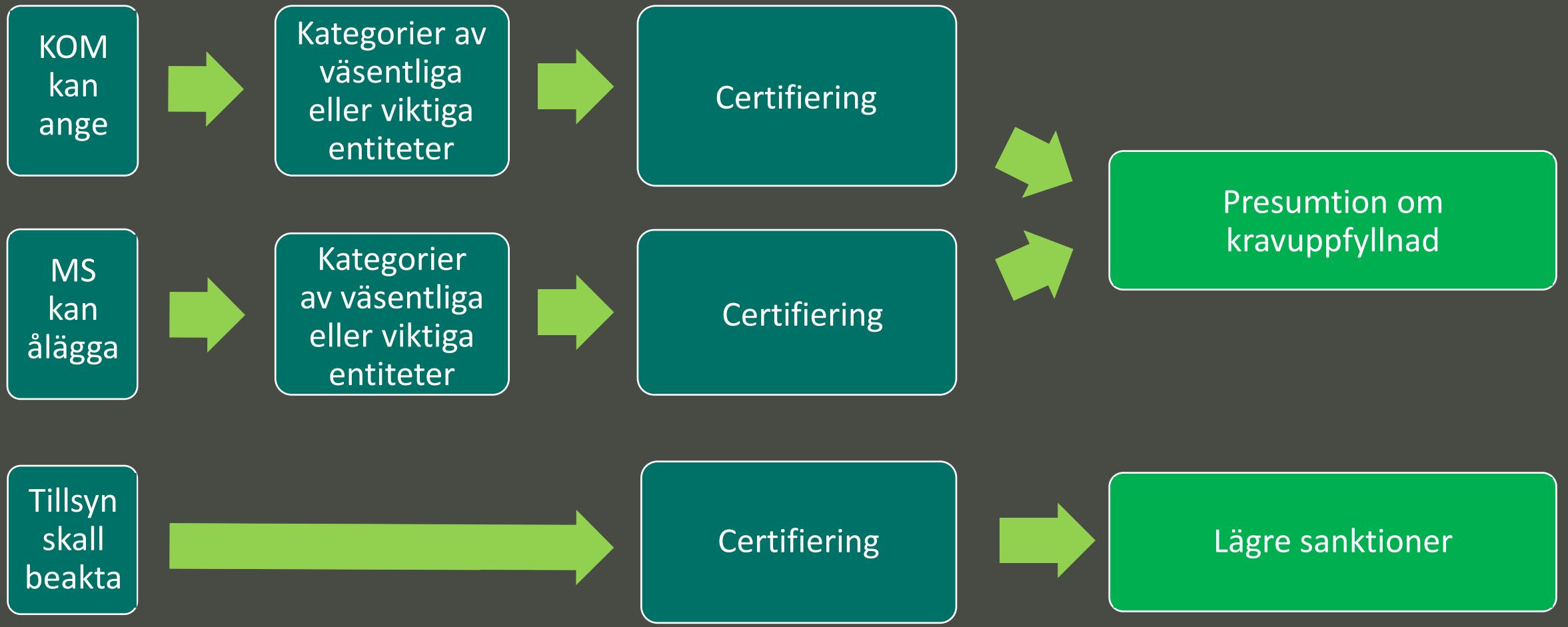
Trust & Safety

- EU Identity Framwork (eIDAS2/EDIF) (Regulation) (EU) 2014/910
- AI Act (Regulation) (EU) 2024/1689

NIS2-direktivet: de största förändringarna

- Fler omfattas (59 viktiga samhällsfunktioner)
- Ensad kravställning
- Ensad incidentrapportering
- Kraftigare sanktioner
- Skarpare krav, bl.a. rörande cybersäkerhet
- Hela organisationen
- Stärkt internationellt samarbete
- Paketlösning med CER-direktivet

NIS2-direktivet och certifiering



Produktkrav och kontroller enligt Cyberresiliensakten (CRA)

Väsentliga cybersäkerhetskrav

Bilaga I

Del 1: Cybersäkerhetskrav hos produkter

- *Säker standardkonfiguration*
- *Automatiska säkerhetsuppdateringar*
- *Skydd mot obehörig åtkomst (IAM)*
- *Uppgiftsminimering*
- *Resiliens- och begränsningsåtgärder bl.a. mot DoS-attacker*
- *Begränsa attackytor*
- *Säker databorttagning*

Lämplig nivå baserat på riskerna

Del 2: Krav på sårbarhetshantering

- *Programvaruförteckning*
- *Åtgärda och avhjälpa*
- *Offentligt redovisa information; samordnad delgivning*
- *Säkerhetsuppdatering separat från funktionsuppdatering*
- *Provningar och granskning av säkerheten*
- *Kostnadsfria uppdateringar*

Obligatoriska krav

Hur kritisk produkten är

	90% av produkterna	*10% av produkterna*	
Produkter med digitala element	**Viktiga: Klass I**	**Viktiga: Klass II**	**Kritiska**
	Bilaga III	***Bilaga III***	***Bilaga IV***
Alla produkter som inte ingår i övriga kategorier	*Identitets-hanteringssystem, webläsare, lösenords-hanterare, PKI, VPN, OS, router, mikroprocessor, system för nätverks-förvaltning, SIEM m.fl.*	*Hypervisor, brandväggar, IDS/IPS, manipulationssäkra mikroprocessorer och mikrokontroller*	*Hårdvaruenheter med säkerhets-boxar, smarta mätarportar, smartkort*
Intern kontroll, Självbedömning (modul A)			

Överensstämmelse: EU-typkontroll (modul B) + Intern tillverkningskontroll (modul C)

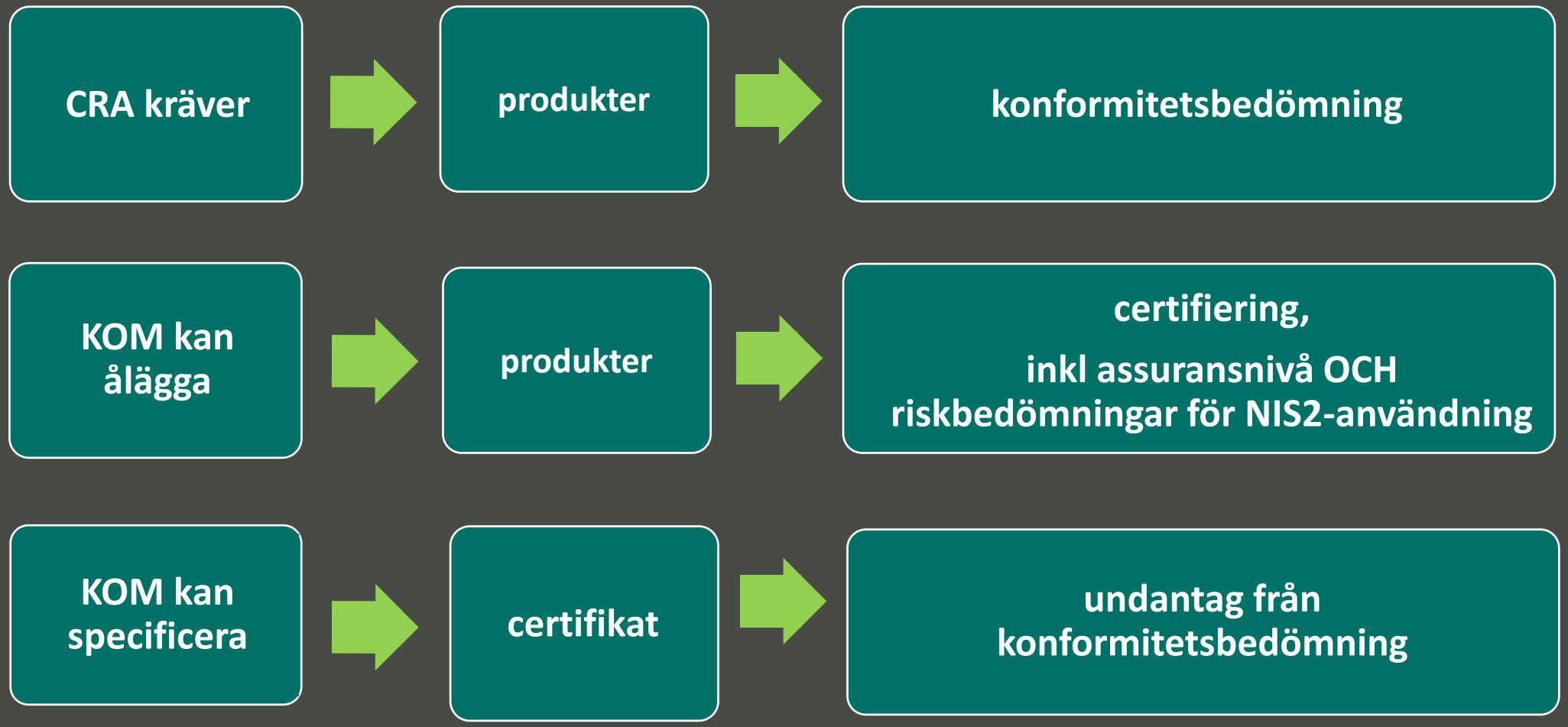
Överensstämmelse: Fullständig kvalitetssäkring (modul H)

Europeisk ordning för cybersäkerhetscertifiering (minst assuransnivå betydande)

Kontrollkravens strikthet

FMV

Cyberresiliensakten (CRA) och certifiering



Vad är en certifieringsordning?

En certifieringsordning är en uppsättning regler, tekniska krav, standarder och förfaranden för tillämpning vid certifiering eller bedömning av överensstämmelse.

Axplock av vad en certifieringsordning ska innehålla
(Artikel 54 i cybersäkerhetsakten)

- Föremålet/tillämpningsområdet
- Användning av standarder/specifikationer
- Assuransnivåer
- Evalueringsmetoder och evalueringskriterier
- Konsekvenser vid bristande regeluppfyllnad
- Sårbarhetshantering

Assurans och evaluering – art. 52 CSA

Assuransnivåer *Förtroendegrund för att en produkt/tjänst/ process uppfyller säkerhetskraven*	**Evalueringsnivåer** *Stringens och djup i utvärderingen/ evalueringen*	**Komponenter** *Utvärderingsaktiviteter*
HÖG	Minimera risken för avancerade cyberattacker som genomförs av **aktörer med omfattande kunskaper och resurser**.	- en granskning för att allmänt **kända sårbarheter** inte föreligger - testning för att produkter, tjänster eller processer genomför **nödvändiga säkerhetsfunktioner** med den **senaste tekniken** - en bedömning av **motståndskraften** mot kunniga angripare genom **penetrationstestning**
BETYDANDE	Minimera kända cyberrisker, och risken för incidenter och cyberattacker som genomförs av **aktörer med begränsade kunskaper och resurser**	- en granskning för att visa att **allmänt kända sårbarheter** inte föreligger - testning för att visa att produkter, tjänster och processer på ett korrekt sätt genomför **nödvändiga säkerhetsfunktioner**
GRUNDLÄGGANDE	Minimera kända grundläggande risker för **incidenter och cyberattacker**	- granskning av den **tekniska dokumentationen**

FMV

Cybersäkerhetsaktens certifieringsordningar

Beslutade	• EUCC (it-produkter/Common Criteria)
Beställda	• EUCS (molntjänster) • EU5G (5G-nätverk) • eIDAS2/EUDI Wallet (digitala identitetsplånboken)
Planerade	• MSS (utlokaliserade säkerhetstjänster) • AI (artificiell intelligens)

Nationellt genomförande av certifieringsramverket

Nationellt

- Lag (2021:553) med kompletterande bestämmelser till EU:s cybersäkerhetsakt
- Förordning (2021:555) med kompletterande bestämmelser till EU:s cybersäkerhetsakt
- FMV:s Myndighets-instruktion & Regleringsbrev
- Annan nationell lagstiftning t.ex. Förvaltningslag/ OSL

Myndighetsutövning & uppgifter som nationell myndighet för cybersäkerhetscertifiering – FMV

Beslut, tillstånd och myndighetsutövning

- Beslut om bemyndigande
  - *För särskilda och ytterligare krav*
- Beslut om förhandsgodkännande (certifikat)
  - *För assuransnivå HÖG*

- Notifiering till EU av ackrediterade och bemyndigade organ i Sverige
- Tillsyn (aktörer, certifikat)
  - *Föreläggande, vite och sanktioner*

Övriga uppgifter

- Nationell representant i Europeiska gruppen för cybersäkerhetscertifiering (ECCG)

- Delta i utveckling av certifieringsordningar
  - *Inkl. representant i kommittéförfarande i EU*

- Samverkan nationellt och internationellt
  - *Swedac, MSB , NCSC*
- Omvärldsbevakning

Myndighetsutövning & uppgifter som nationell myndighet för cybersäkerhetscertifiering – FMV

Beslut, tillstånd och myndighetsutövning

- Beslut om bemyndigande
  - *För särskilda och ytterligare krav*
- Beslut om förhandsgodkännande (certifikat)
  - *För assuransnivå HÖG*

- Notifiering till EU av ackrediterade och bemyndigade organ i Sverige
- Tillsyn (aktörer, certifikat)
  - *Föreläggande, vite och sanktioner*

Övriga uppgifter

- Nationell representant i Europeiska gruppen för cybersäkerhetscertifiering (ECCG)

- Delta i utveckling av certifieringsordningar
  - *Inkl. representant i kommittéförfarande i EU*

- Samverkan nationellt och internationellt
  - *Swedac, MSB , NCSC*
- Omvärldsbevakning

Europeiska certifieringsordningen för Common Criteria (EUCC)

Bakgrund

- Europeiska ordningen för Common Criteria
- Publicerad under (EU) 2024/482
- Common Criteria – etablerad standard (ISO/IEC 15408)
- EU-samverkan – SOG-IS
- Global samverkan – CCRA

Tredjepartsevaluering och standarder

- Endast assuransnivåerna betydande och hög
- Tredjepartsevaluering
- Standarders roll

Certifieringsorgan
- ISO/IEC 17065
- ISO/IEC 15408 1-5 – Common Criteria

Evalueringsföretag
- ISO/IEC 17025
- ISO/IEC 15408 1-5 – Common Criteria
- ISO/IEC 18045 – Common Evaluation Methodology

Omfattning och tillämpningsområden

- Del av produkt
- Säkerhetsfunktionalitet

Betydande – exempel
- Skrivare
- Databaser
- Nätverkskomponenter

Hög – exempel
- Smal omfattning
- Smarta kort
- Datadioder

Samspel med CRA

Problem
- Skillnad i omfattning
  - Hel produkt kontra del av produkt
  - SBOM
- GAP-Analys

Lösningar
- Skyddsprofil
  - Generell
  - Specificerad

SWEDAC

SWEDAC ACKREDITERING

Swedacs uppdrag

- Sveriges ackrediteringsorgan och expertmyndighet för teknisk kontroll.
- Föreskrivande myndighet och tillsynsmyndighet för reglerad mätteknik och ädelmetall.
- Samordnar marknadskontroll i Sverige.
- Internationellt samarbete för utveckling och förstärkt kvalitetsinfrastruktur.

SWEDAC

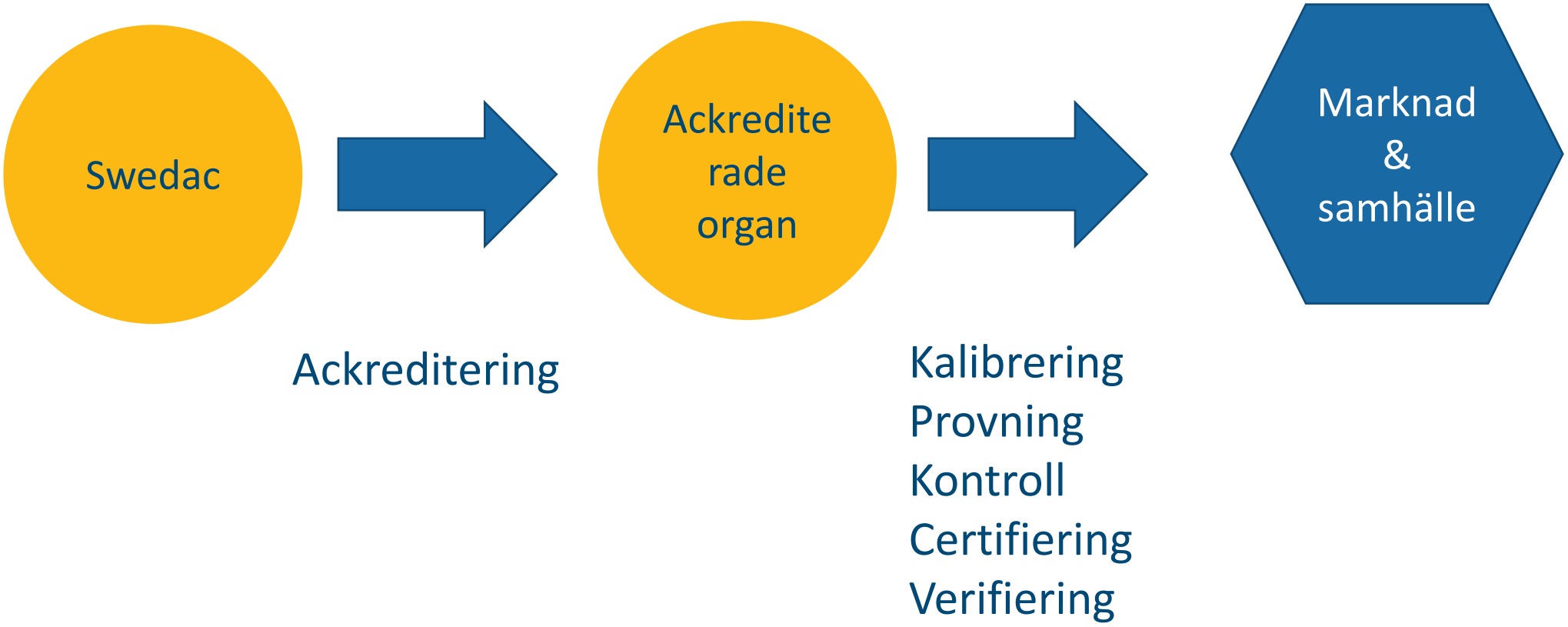
Omfattar:
Bedömning av kompetens och ledningssystem för att säkerställa att alla krav uppfylls

Baseras på:
→ Opartiska aktörer
→ Svensk samt europeisk lagstiftning
→ Nationell och internationell nivå

Ackreditering

Bidrar till:
→ Stärkt konsumentskydd
→ Stärkt konkurrenskraft
→ Ökad hållbarhet
→ Ökad kvalitet och säkerhet

SWEDAC


Swedac
Ackrediterad organ
Marknad & samhälle
Ackreditering
Kalibrering
Provning
Kontroll
Certifiering
Verifiering

SWEDAC

Ett öppet system

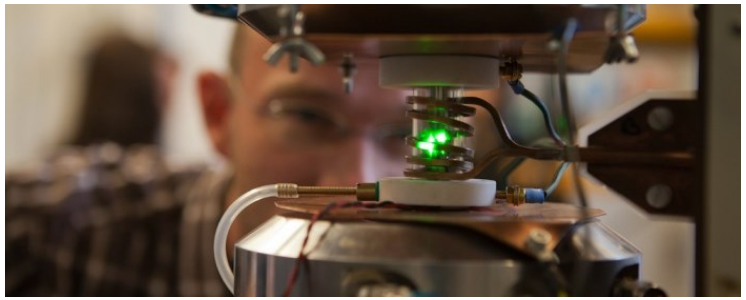
- Ackreditering är ett verktyg för samhället att säkerställa opartiskhet och kompetens hos marknadens aktörer.
- Ackrediterade organ är fria att verka inom de områden som de ackrediterats för.
- Tillämpas både nationellt och internationellt samt på frivilliga och tvingande områden.

Ackreditering inom EUCC

Laboratorium

ISO/IEC 17025

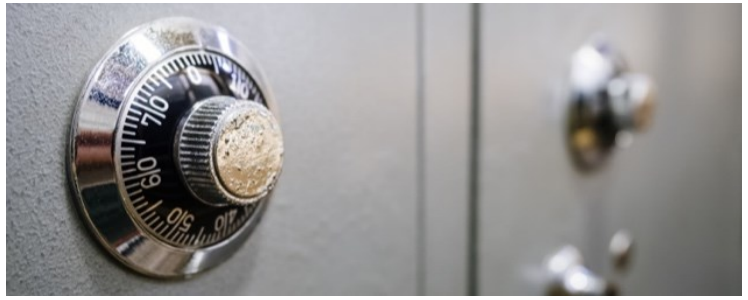
→ Provning



Certifieringsorgan

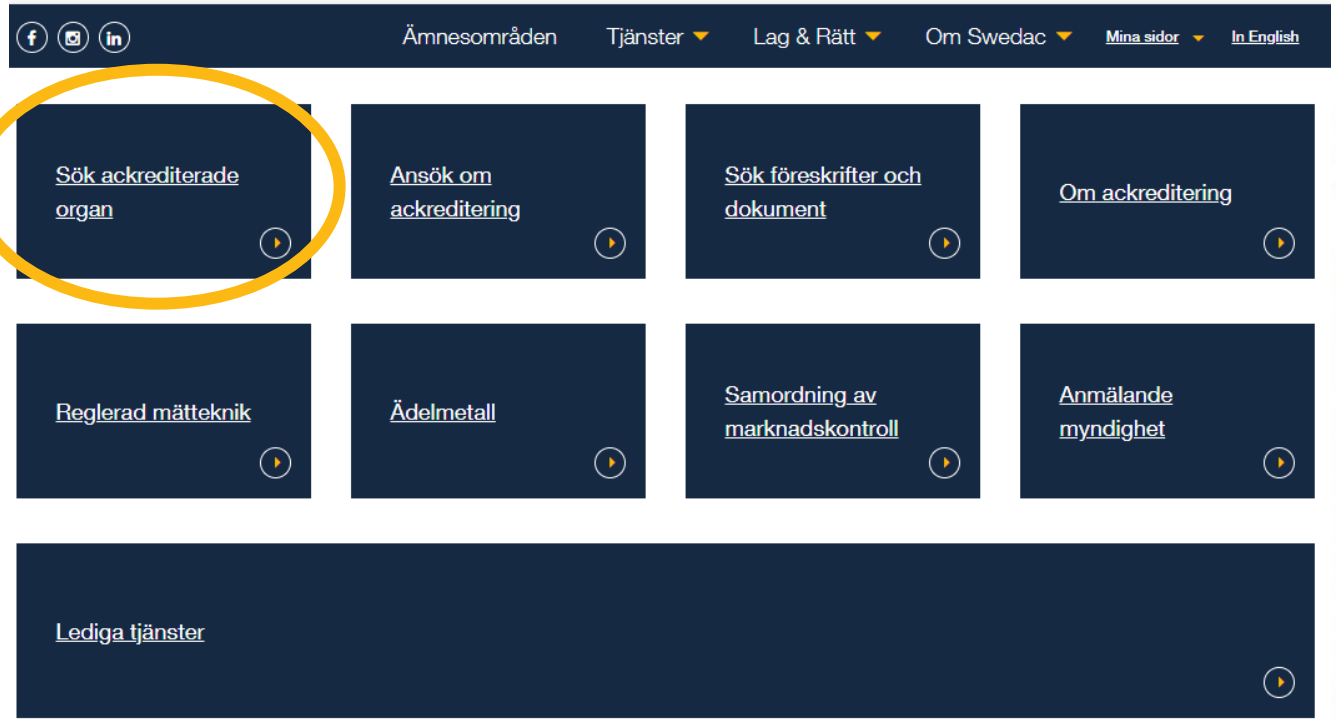
ISO/IEC 17065

→ Produkt/Process/Tjänst



Ytterligare information

www.swedac.se



Europeiska certifieringsordningen för molntjänster (EUCS)

Europeisk certifieringsordning för molntjänster (EUCS)

Syfte

- Stärka nivån på cybersäkerhet
- Förmåga att fatta informerade upphandlingsbeslut

Definition

- ”Molntjänst” – Ett generiskt begrepp
- En digital tjänst med särskilda egenskaper
- Definition enligt EUCS

Olika typer

- Horisontell ordning
- Heltäckande och kan användas av alla typer av molntjänster (IaaS, PaaS, SaaS)

Assuransnivåer och tillämpningsområden

Grundläggande

- Basnivå av krav
- Skydd mot generiska hot

Betydande

- Avancerade krav
- Skydd mot sofistikerade attacker

Hög

- Strikta krav
- Skydd mot avancerade och riktade attacker samt hybridhot och statsaktörer
- Kritisk infrastruktur och känslig data

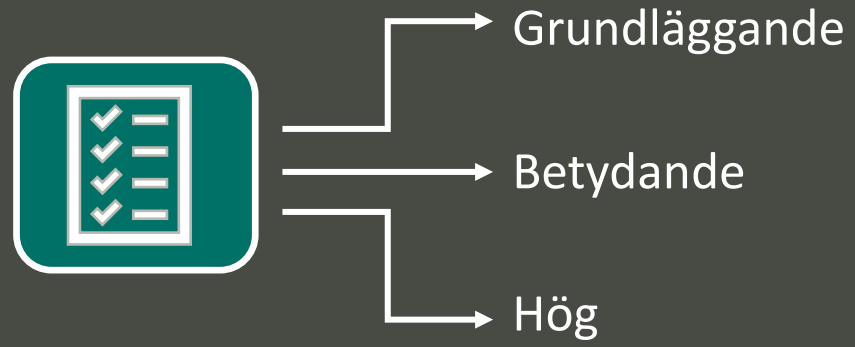
- *Icke-känslig verksamhet*
- *Exempelvis ”webb-hosting” utan känslig information*

- *Affärskritiska data och system*

- *Verksamhetskritiska data och system*

Teknisk specifikation - TS18026

- Cybersäkerhetskrav för molntjänster fördelat på tre nivåer.
- Framtagen av CEN/CENELEC.
- Publikt tillgänglig.



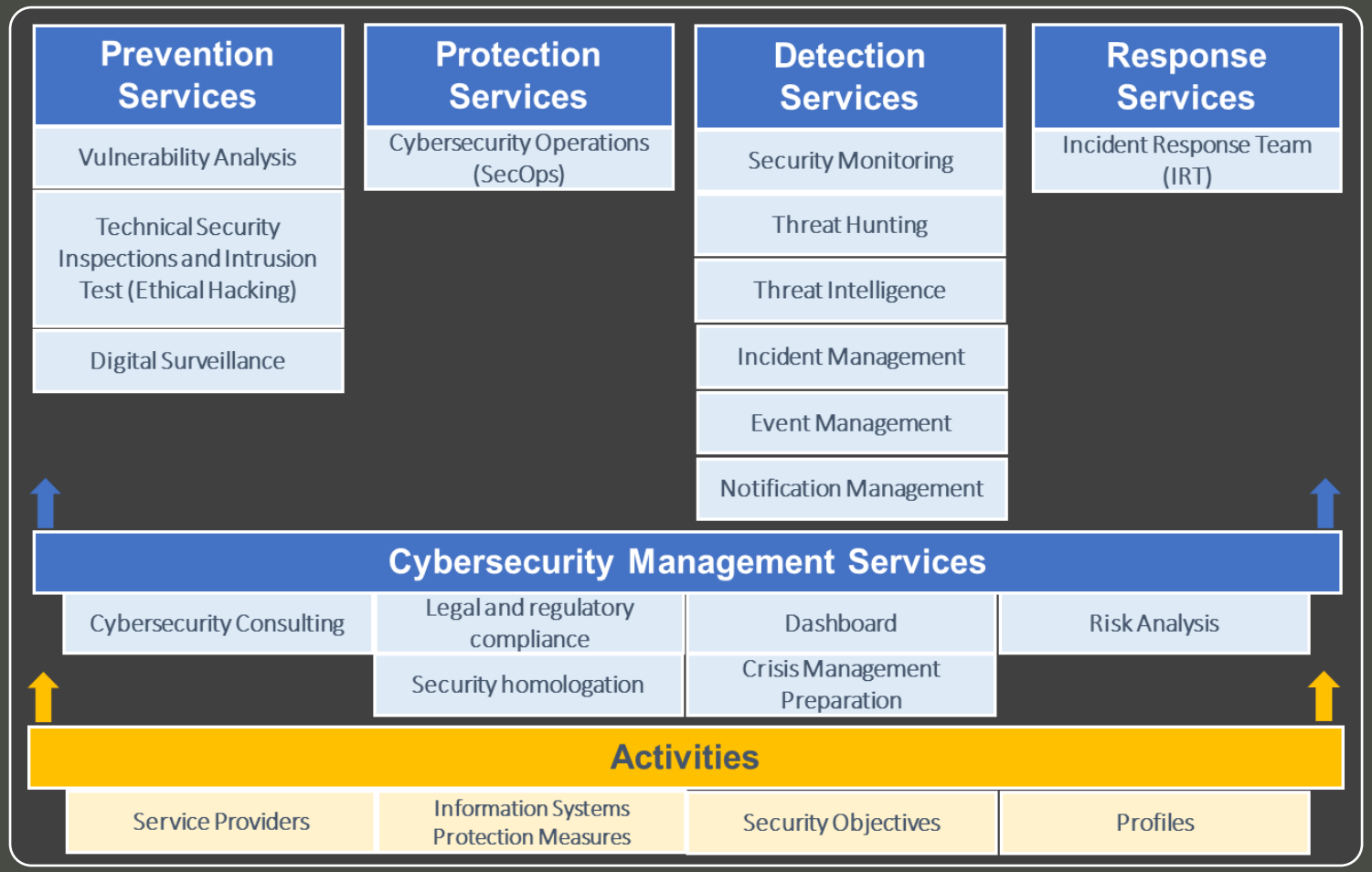
Digital suveränitet

- Finns krav på digital suveränitet i relation till EUCS?
- Kommissionen är inte i mål med diskussionen.

Managed Security Services

”Utlokaliserade säkerhetstjänster”

Tjänster



- Tjänster delas upp i fem kategorier
- Aktiviteter som är generellt för alla tjänster

Koppling till andra EU-regelverk

- Cybersäkerhetsakten
- NIS2
- Cybersolidaritetsakten
- DORA

Mål med utlokaliserade säkerhetstjänster

Öka tillit

Kravefterlevnad

Förbättra incidenthantering

Status

Ingen beställning på certifieringsordning än

Enisa arbetar på en lämplighetsstudie

CSEC och Nato NIAPC

Agenda

- CSEC — Sveriges certifieringsorgan för IT-säkerhet
- Nato, Common Criteria, och NIAPC-listan
- Vad är NIAPC
- Anmälan

CSEC: Sveriges certifieringsorgan för it-säkerhet

- Nationellt certifieringsorgan för IT-säkerhet
- Tar fram och utvecklar regler för granskning av IT-säkerhet i produkter och system
- Common Criteria
- Internationell samverkan inom **CCRA** (globalt) och SOG-IS MRA (Europa)
- Påverkas av **EUCC**

NATO Information Assurance Product Catalogue (NIAPC)

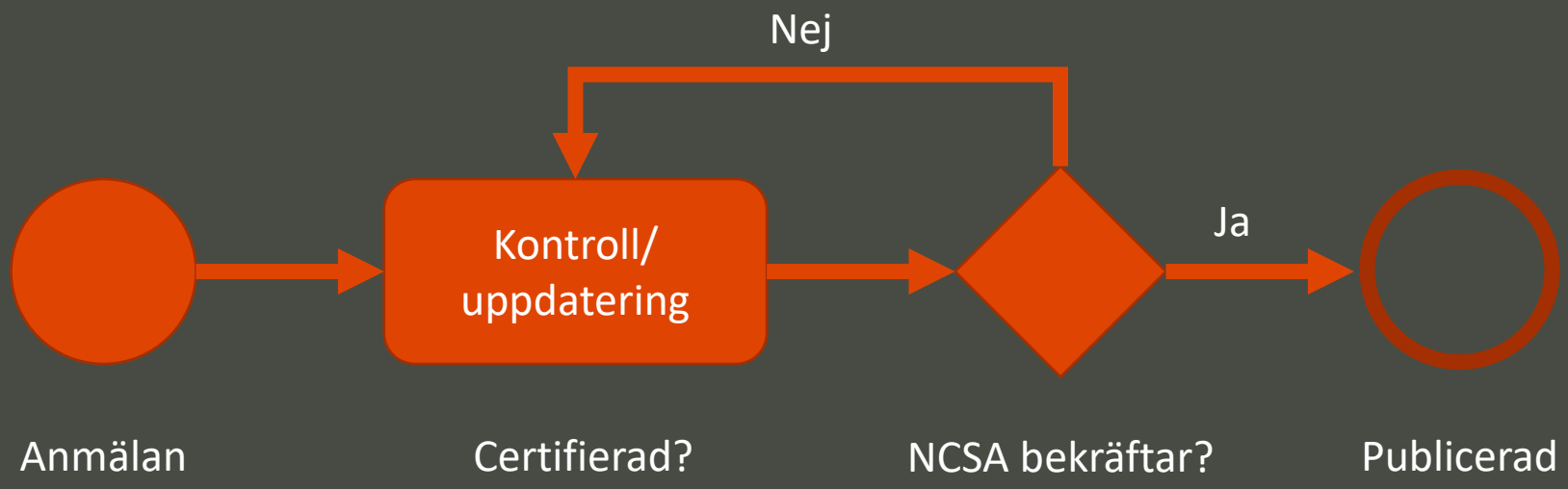
- **Syfte**
  - Nato ser CC som ett kostnadseffektivt sätt att säkerställa god säkerhetsnivå på produkter
  - NIAPC är en kvalificerad lista med certifierade it-säkerhetsprodukter av och för Natoländer
- **NIAPC**
    - Inledande öppning för försäljning av it-säkerhetsprodukter till Nato-länder
    - Bekräftat certifierade produkter från tillverkare i Nato-länder
    - För svenskt vidkommande innebär det Common Criteria
    - En bekräftad (certifierad) produkt är dock **inte** därmed godkänd för användning/inköp i respektive försvarsorganisation
- **Innebörd**
  - **NIAPC öppnar för försäljning av certifierade it-produkter till Nato-länder**
  - **Common Criteria är en gemensam nämnare för Nato och EUCC**

NIAPC, CCRA och EUCC

- Natos regelverk pekar idag specifikt på CC-certifiering inom ramen för CCRA-samarbetet (en multilateral överenskommelse om ömsesidigt certifikatserkännande)
- EUCC påverkar genom att certifieringsverksamhet huvudsakligen övergår från statliga organ (som CSEC) till privata organ. Ikraftträdandet innebär att svensk statlig certifieringsverksamhet inom CCRA avslutas och privat certifieringsverksamhet inom EUCC tar vid
- Övergångsdatum:
  - **27 februari 2025 är** sista datum för att ansöka om CCRA-certifiering genom CSEC
- Troligen kommer EUCC-certifikat accepteras av Nato

NIAPC — Anmälan

- Processen hanteras genom Nato med kontroller utförda av NCSA
- NCSA för Sverige:
  - CSEC för säkerhetshöjande it-produkter
  - FM-MUST för kryptografiska produkter och TEMPEST
- Anmälningsformulär: https://www.ia.nato.int/NIAPC (välj Vendor Information)



Sammanfattning CSEC och NIAPC

- EUCC påverkar CSEC – certifieringsverksamhet övergår huvudsakligen till privata organ
- Common Criteria är relevant även för Nato
- NIAPC öppnar för försäljning av säkerhetshöjande IT-produkter inom Nato
- 27 februari 2025 deadline för certifiering inom CCRA och SOG-IS genom CSEC

Ytterligare information

- FMV:s hemsida EU-certifiering
- Certifiering på Enisas hemsida
- Hemsida för certifiering (Enisa)
- CSEC:s hemsida
- Swedacs hemsida
- NCSC:s hemsida