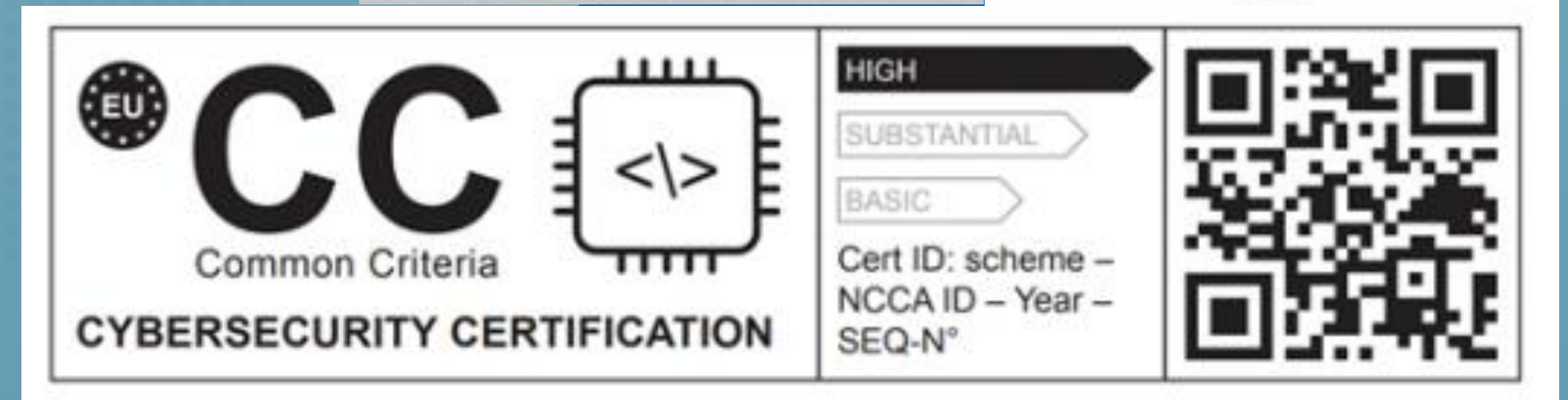


Vad man behöver tänka på
och vad som är viktigt vid
upphandling av moderna IT-
och molntjänster,

- speciellt inom offentlig
verksamhet.

Anders Jonsson, Member Enisa AHWG EUCS



Kort om mig:



Anders Jonsson

Mob: +46708655301

anders@securemailbox.com

- Senior Advisor Cyber Security & GDPR Expert
- Member ENISA AHWG EUCS & Rapportour ENISA for EUCS Guidelines
- Member in EU Alliance for Data Edge and Cloud
- Member in EDPB support group of Experts
- Har de senaste 10 åren anpassat system/tjänster till de nya kraven som vi inom EU tagit fram för att skydda invånare och viktiga tjänster i vår uppkopplade värld
- Har tidigare en lång karriär inom IT, Tech och mjukvaruutveckling internationellt.



EUROPEAN ALLIANCE
FOR INDUSTRIAL DATA,
EDGE AND CLOUD



Prostatype

Ett säkrare utlåtande om din prostatacancer

Prostatype är för dig som har diagnostiserats med prostatacancer. Med unik genanalys ger testet ett mer tillförlitligt utlåtande på hur aggressiv din prostatacancer är och ett säkrare svar på om du behöver behandling eller inte.

[GRATIS RÅDGIVNING](#) [JAG VILL VETA MER](#)

BankID Företag Privatpersoner Utvecklare Internationellt

Varning, falska SMS-utskick

Säkert, snabbt och smidigt

Med BankID får du en stabil och säker lösning som de

kry

Vi tar hand om dig om 8 minuter



4,9 Betyg App Store ★★★★★ 94% Får hjälp 4,8 Patientnöjdhet ★★★★★

miljehemSverige.se

Testa dig själv Anmäl intresse Fakta om

Vill du öppna ditt hem för ungdom?

et handlar dels om barn och ungdomar som av olika skäl inte...
dels om barn och ungdomar som flyr från krig och anländer till...
det viktigt att de får en trygg och stabil familj att bo hos oavs...

[Testa dig själv](#) [Anmäl intresse](#)

MAN BEHÖVER FÖRSTÅR HUR MODERNA MOLNTJÄNSTER FUNGERAR, "BYGGS-UPP" FÖR ATT KUNNA KRAVSTÄLLA/UPPHANDLA/AVROPA FRAMGÅNGSRIKT DEN DIGITALA UTVECKLINGEN STÅR JU INTE STILL...

Skicka säkra meddelanden

Miljö & Energi **VÄSTERVIKS KOMMUN**

Vi erbjuder heltäckande affärssystem för bolag inom bygg- och fastighetsbranschen. Vårt fastighetssystem, energiuppföljningssystem och ekonomisystem har funktioner för webb och mobil, finns som molntjänst eller egen installation, hos dig eller hos oss. På mest effektiva sätt stödjer och optimerar vi dina huvudprocesser för uthyrning & försäljning, kundservice, ekonomi, teknisk förvaltning och energiuppföljning.

Prostatype

Ett säkrare utlåtande om din prostatacancer

Prostatype är för dig som har diagnostiserats med prostatacancer. Med unik genanalys ger testet ett mer tillförlitligt utlåtande på hur aggressiv din prostatacancer är och ett säkrare svar på om du behöver behandling eller inte.

[GRATIS RÅDGIVNING](#) [JAG VILL VETA MER](#)

BankID Företag Privatpersoner Utvecklare Internationellt

Varning, falska SMS-utskick

Säkert, snabbt och smidigt

Med BankID får du en stabil och säker lösning som de aller flesta av dina kunder redan använder och litat på. Dessutom får du värdefull kunskap från 20 år som ledande experter inom digital identitet.

Säkravideomöten

Logga in med SecureMailbox

möten använder SecureMailbox som teknisk plattform där auktoriserad för att säkra och förenkla din inloggning

Powered by SecureAppbox

Miljö Energi VÄSTERVIKS KOMMUN

kry

Vi tar hand om dig om 8 minuter

- ✓ Tid på vårdcentralen inom 24 timmar
- ✓ Öppet dygnet runt i appen
- ✓ Läkare, psykologer och sjuksköterskor

[Boka möte](#)

Bästa appen någonsin. Helt fantastiskt när man har småbarn. - Limpan1986

4,9 Betyg App Store ★★★★★

94% Får hjälp

4,8 Patientnöjdhet ★★★★★

EU – "CLOUD FIRST"

"Cloud-first" innebär att all ny utveckling helst bör vara molnbaserad, och befintliga informationssystem bör omvärderas för omvandling, omskrivning eller ersättning inom ramen för de moderniseringsplaner som förutses.

2019/2020

ungdom?

et handlar dels om barn och ungdomar som av olika skäl inte kan bo tillsammans med sina föräldrar, dels om barn och ungdomar som flyr från krig och anländer till Sverige utan föräldrar. För dessa barn är det viktigt att de får en trygg och stabil familj att bo hos oavsett om det är för kortare eller längre tid.

[Testa dig själv](#) [Anmäl intresse](#)

ISSYSTEM FÖR BYGG- & FASTIGHETSBOLAG

Välkommen!

Vi erbjuder heltäckande affärssystem för bolag inom bygg- och fastighetsbranschen. Vårt fastighetssystem, energiuppföljningssystem och ekonomisystem har funktioner för webb och mobil, finns som molntjänst eller egen installation, hos dig eller hos oss. På mest effektiva sätt stödjer och optimerar vi dina huvudprocesser för uthyrning & försäljning, kundservice, ekonomi, teknisk förvaltning och energiuppföljning.

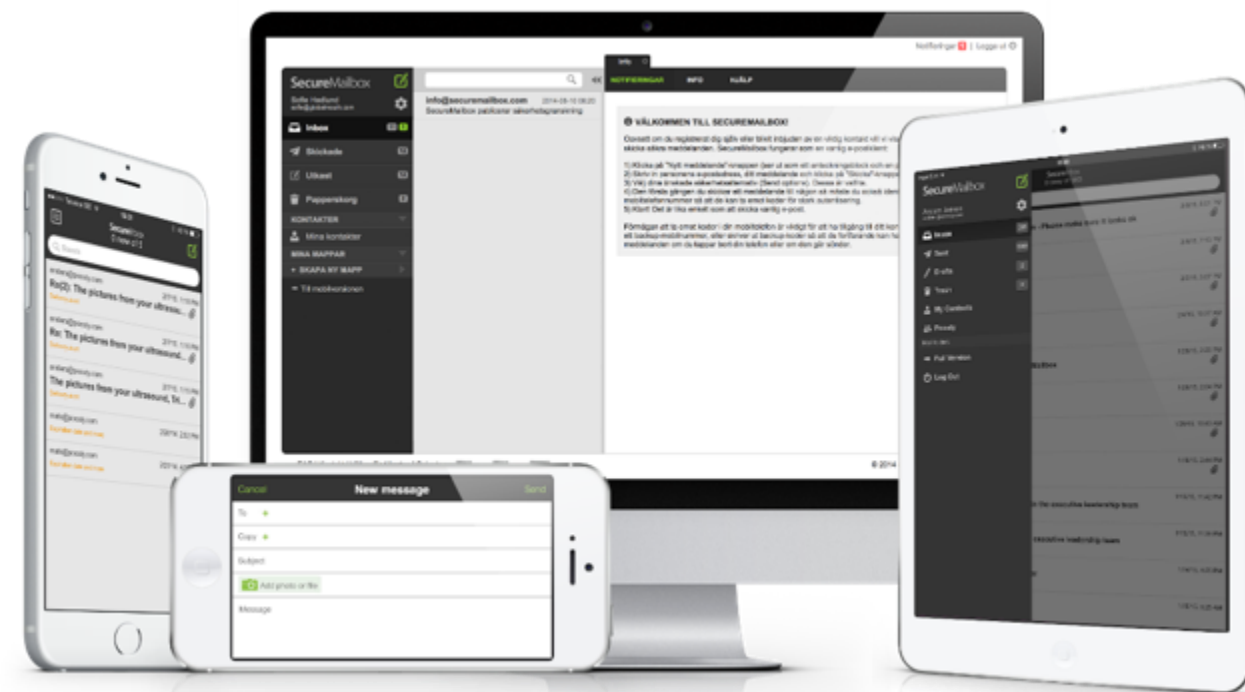
VARFÖR MAN BYGGER APPAR/TJÄNSTER PÅ "WEBBEN"!

Alla kan nå och använda webben, från valfri enhet, oavsett tid och plats..



ANVÄNDARE/KLIENT

Moderna applikationer behöver snabbt kunna användas, nyttjas, distribueras, uppdateras till sina användares olika typer av enheter, oavsett tid eller plats



UTVECKLINGEN GÅR FORT..



Google Chrome	79.9%
Safari	3.0%
Mozilla Firefox	4.8%
Microsoft Edge	10.0%

July 2023

GOOGLE CLOUD
Google SÖK!



MICROSOFT "COPILOT"!
Office 365 (CoPilot) släppt 26/9 (ChatGDP)

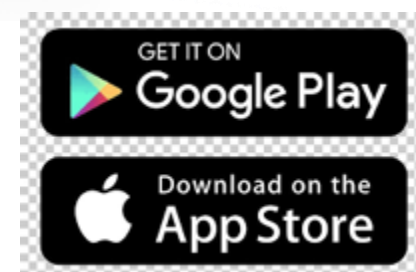
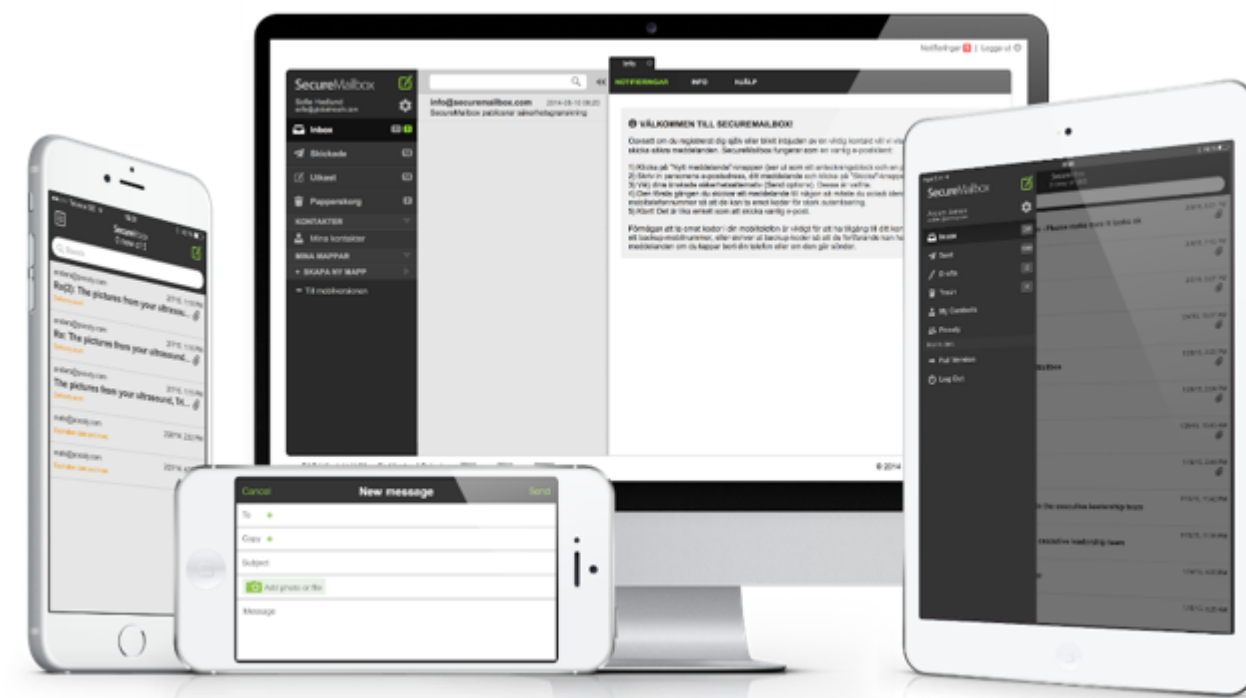
VARFÖR MAN BYGGER APPAR/TJÄNSTER PÅ "WEBBEN"!

Alla kan nå och använda webben, från valfri enhet, oavsett tid och plats..



ANVÄNDARE/KLIENT

Moderna applikationer behöver snabbt kunna användas, nyttjas, distribueras, uppdateras till sina användares olika typer av enheter, oavsett tid eller plats



ADRESSERING / BEHÖRIGHET

För att nå sina Webbtjänster genom de redan installerade webbläsarna skriver man in en DNS adress. Många tjänster kräver behörighet.

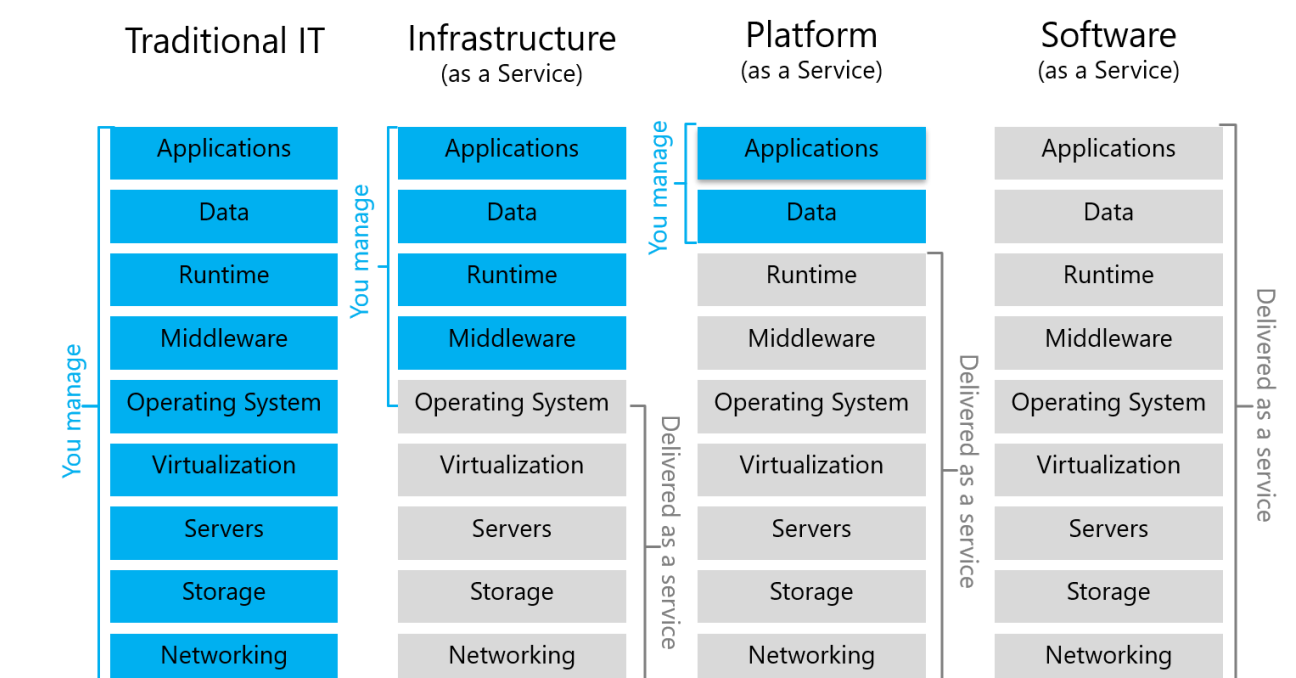
[HTTPS://Familjehemsverige.se](https://Familjehemsverige.se)

[HTTPS://connect.secureappbox.com](https://connect.secureappbox.com)



WEBBTJÄNST/SERVER

Webbtjänster byggs i "containers" genom användning av färdiga ramverk, komponenter & API tjänster. Dessa implementeras sedan i olika molninfrastrukturer där IaaS, PaaS, SaaS kombineras...



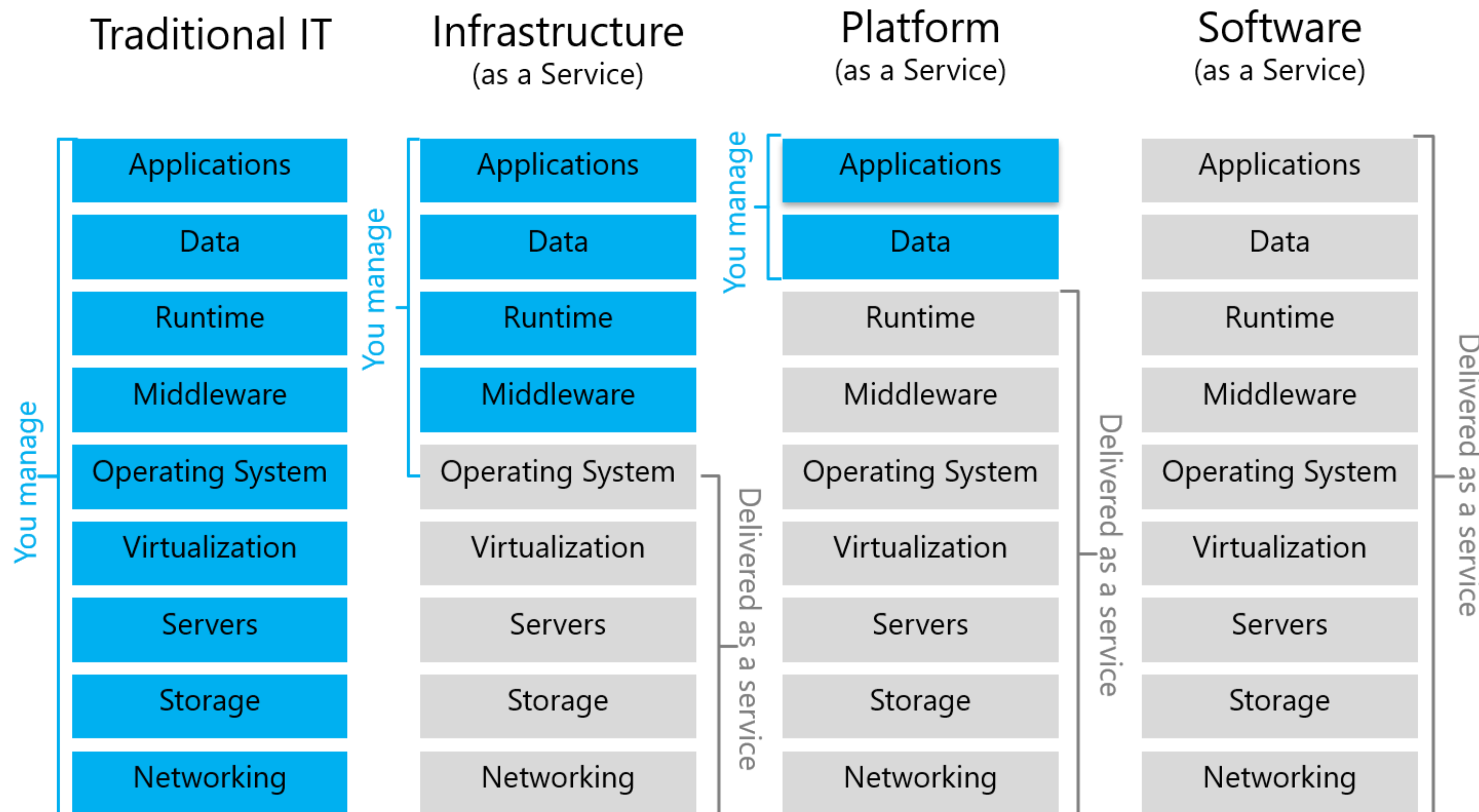
MÅNGA VÄLJER EXTERN INFRASTRUKTUR

Fokus på det man är bra på!



Redundant nät anslutning, skalbar- genomtänkt- och testad infrastruktur, hög säkerhet, klarar regulatoriska krav, hög tillgänglighet (24/7) och man betalar bara för nyttjandet

Traditionella molnmodeller



Idag: Multi/hybrid modeller

Idag handlade molnprojekt mer om att komponera funktioner, oavsett vilken "molnmodell" som användes av en viss implementering (t.ex. API, komponent, funktion, tjänst, etc.).

I moderna molnprojekt komponera man tjänster och funktioner byggda på både IaaS, PaaS och SaaS alternativ. Dessutom har mognaden kring hybrid modeller ökat så även linjerna med interna IT-miljöer suddades ut.

Trust in a Digital Society



Public services



Electronic transactions



Health



Electronic identity

Connected cities



Cybersecurity

Online privacy

Connected mobility



EU – CYBERSECURITY STRATEGY

Styrning genom förordningar och tydliga direktiv

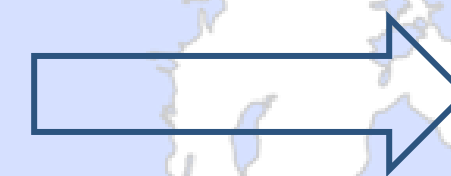
STRATEGY



2013-2019



2020-2025



2010

2013

2016

2019

2022

2024..

CER Directive

- Energy
- Transport



GDPR
NIS1



CSA
Cyber
Security
Act



NIS2
(CER)



NIS2 implemented
CSA (EUCC/EUCS/5G)
DORA (RTS/ITS)
Cyber Resilience Act
AI Act
Chips Act
Etc..

IMY – GDPR
MSB - NIS
• IVO
• PTS
• DIGG
• etc

ENISA
• EU Cybersecurity Agency
• Develop NIS
• Cybersecurity certification
framework (EUCC/EUCS/5G...)

Öka motståndskraften hos våra samhällsviktiga tjänster

Nätverks- och informationssystemen har utvecklats till ett centralt inslag i vardagslivet i och med den snabba digitala omställningen och sammankopplingen av samhället. Denna utveckling har lett till en utvidgad **cyberhotbild***, som medfört nya utmaningar som kräver anpassade, samordnade och innovativa svarsåtgärder i alla medlemsstater.

Nya uppdaterade NIS2-direktivet innehåller många nyheter:

- ny klassificering, väsentliga entiteter och viktiga entiteter samt tillämpning på flera sektorer;
- **nya krav på säkerhetsåtgärder;**
- **krav på säkerhet i leverantörskedjor;**
- utökade krav på incidentrapportering;
- införande av sanktioner;
- mm



Cybersecurity: Parliament adopts new law to strengthen EU-wide resilience | News | European Parliament

*** Cyberattacker, växer snabbt i omfattning, kostnader och i hur sofistikerade de är.**

- en av de snabbast växande formerna av brottslighet i världen

NIS2 - oktober 2024

EXTERNA CYBERHOT

1

- **Cyber attacker**
- Av andra länder/ eller anlitade av dessa
- Strategisk infrastruktur – målet data / skapa kaos

2

- **Cyber attacker**
- Kriminella attacker på er/leverantörskedjan
- "Hitta svagaste punkten" - målet är pengar



ÖKA VERKSAMHETENS
MOTSTÅNDSKRAFT

3

- **Brister i lösningar och leverans "no redundancy"**
- Dålig kontroll på andras faror/leverantörskedjan
- Brister i upphandling/underlag/implementation

4

- **Omedvetna eller medvetna misstag**
- Dåligt utvecklade tjänster/design – Brist QA
- Bristande instruktioner, kompetens eller bara otur

INTERNA HOT OCH BRISTER

Ny klassificering och tillämpning på flera sektorer;



Väsentliga entiteter (och kan även vara kritiska)

1. Energi	a) Elektricitet, b) Fjärrvärme/fjärrkyla, c) Olja, d) Gas, samt e) Vätgas
2. Transport	a) Lufttransport, b) Järnvägstransport, c) Sjöfart, samt d) Vägtransport
3. Bankverksamhet	Kreditinstitut enligt EUF 575/2013
4. Finansmarknadsinfrastruktur	Handelsplatser (värdepapperscentraler), direktiv 2014/65/EU, centrala motparter, EUF 648/2012
5. Hälso- & sjukvårdssektorn	Vårdgivare (direktiv 2011/24/EU), EU-laboratorier inom smittforskning, läkemedelsforskning (direktiv 2001/83/EG), tillverkare av farmaceutiska basprodukter och läkemedel, tillverkare av kritiska medicintekniska produkter
6. Dricksvatten	Leverantörer enligt direktiv 98/83/EG
7. Avloppsvatten	Företag som hanterar avloppsvatten mm enligt direktiv 91/271/EEG
8. Digital infrastruktur	Internetknutpunkter, DNS-tjänster, toppdomänregistrerare, molntjänst datacentraler, nättjänst innehållsleverans, betrodda tjänster (EUF 910/2014), leverantör av elektroniska kommunikationsnät/tjänster
9. Offentlig förvaltning	Offentliga förvaltningsentiteter under regeringen, regioner (och kommuner)
10. Rymden	Operatörer som tillhandahåller infrastruktur till stöd för rymdbaserade tjänster (direktiv 2018/1972)

Stor del av kommunal verksamhet omfattas

Underleverantörer omfattas

IT-infrastruktur omfattas inkl. fastighetsbolag.

Viktiga entiteter

1. Post- och budtjänster	Tillhandahållare av post- och budtjänster (direktiv 97/67/EG)
2. Avfallshantering	Företag som sköter sophämtning mm (direktiv 2008/98/EG)
3. Tillverkning, produktion och distribution av kemikalier	Företag som tillverkar, producerar och distribuerar kemtekniska ämnen och varor (EGF 1907/2006)
4. Produktion, bearbetning och distribution av livsmedel	Livsmedelsföretag (EGF 178/2002)
5. Tillverkning	a) Medicintekniska varor (EUF 2017/745 och 2017/746) b) Datorer, elektronikvaror, optik c) Elapparater d) Övriga maskiner e) Motorfordon, släpvagnar och påhängsvagnar f) Andra transportmedel
6. Digitala leverantörer	- Internetbaserade marknadsplatser - Internetbaserade sökmotorer - Plattformer för sociala nätverkstjänster

Hänvningar:

NIS2 delas i KRITISKA, VÄSENTLIGA OCH VIKTIGA

KRITISKA: Särskilt utpekade som *samhällsviktiga*, med *kritisk infrastruktur* och där en incident skulle kunna medföra *betydande störning* (se art. 2.3 och direktiv EU 2022/2557 CER)

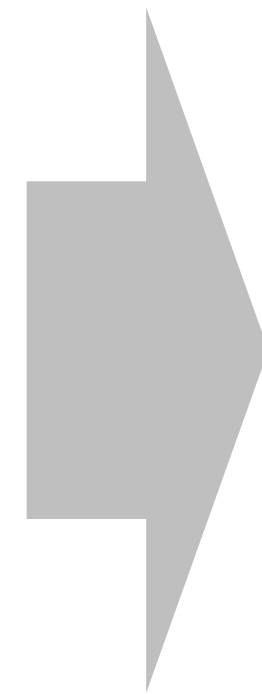
VÄSENTLIGA: Entiteter som räknas upp som "väsentliga" (se art. 3.1 och Bilaga I)

VIKTIGA: Entiteter som anges i Bilaga I eller II och som inte anses vara väsentliga enligt art. 3.1 (se art. 3.2 och Bilaga I och II)

ANSVAR ATT INFÖRA ÅTGÄRDER FÖR RISKHANTERING OCH RAPPORTERINGSKRAV FÖR CYBERSÄKERHET



ART 20: Medlemsstaterna ska säkerställa att väsentliga och viktiga entiteters ledningsorgan godkänner de riskhanteringsåtgärder för cybersäkerhet som dessa entiteter vidtar för att följa artikel 21, övervakar genomförandet av dem och kan ställas till svars för entiteternas överträdelser av den artikeln.



Det är ett tydligt krav i NIS 2-direktivet att styrelsen och VD ska ha de kunskaper och färdigheter som krävs för att bedöma cybersäkerhetsrisker, utmana säkerhetsplaner, diskutera aktiviteter, formulera åsikter och implementera lösningar som skyddar digitala processer och tillgångarna i deras organisation.

VAD BEHÖVER NI SÄKRA (ART 21.2)? VILKA ÄR MINIMI KRAVEN?

ARTIKEL 21(2): NIS2 SÄKERHETSKRAV:

- a) Aktuell riskanalys/säkerhetspolicyer för IT-systemen.
- (b) incidenthantering.
- c) Kontinuitet i verksamheten.
- d) Säkerhet i försörjningskedjan.
- e) Säkerhet i nätverk och informationssystem.
- f) Bedömning av effektiviteten av cybersäkerhets åtgärder;
- g) Grundläggande datorhygienpraxis och utbildning.
- (h) Policyer/förfaranden för användning av kryptografi.
- (i) Säkerhet för personal, policyer för åtkomstkontroll och tillgångar/förvaltning.
- (j) multifaktorautentisering, säker röst, video och text kommunikationer och fungerande nöd-system inom enheten.

Hur överensstämmer dessa krav med vad ni har idag?

Om ni upphandlar nya tjänster/IT-system, så är dessa krav minimum?

HUR SÄKRAS "EXTERN" INTERNET INFRASTRUKTUR? VILKA ÄR DERAS MINIMI KRAV?

Art 21.5. Senast den 17 oktober 2024 ska kommissionen anta en genomförande akt som fastställer de tekniska och metodologiska kraven för de åtgärder som avses i punkt 2 med avseende på:

- **Topppdomännamnregister och DNS tjänsteleverantörer,**
- **Molntjänsteleverantörer och leverantörer av datacentertjänster,**
- **Leverantörer av säkerhetstjänster, hanterade tjänster och förtroendetjänster,**
- **Online marknadsplatser, plattformar för sök, sociala nätverkstjänster.**

Kommissionen får anta en genomförande akt som fastställer de tekniska och metodologiska kraven. När kommissionen utarbetar akter skall de i möjligaste mån **följa europeiska och internationella standarder samt relevanta tekniska specifikationer.**

Art 21.5 Implementing Act – leds av ENISA i samarbete med ECASEC (the Article 40, former Article 13A Expert Group)

<https://resilience.enisa.europa.eu/article-13>

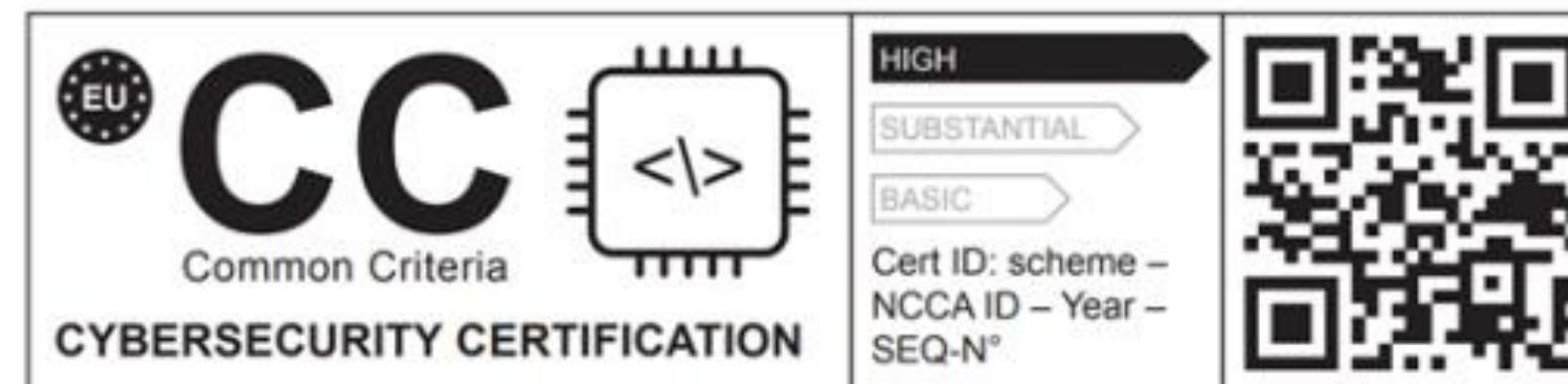
HUR KAN LEVERANTÖRER (UNDERLEV.) VISA FÖLJSAMHET TILL MINIMIKRAVEN I ART 21.2?

Art 24. Användning av cybersäkerhetscertifiering för IT-produkter, molntjänster och IT-processer

För att visa att vissa krav enligt artikel 21 är uppfyllda får medlemsstaterna ålägga väsentliga och viktiga entiteter att använda särskilda IT-produkter, molntjänster och IT-processer, som har utvecklats av den väsentliga eller viktiga entiteten eller **upphandlats från tredje part, som är certifierade enligt europeiska ordningar för cybersäkerhetscertifiering.**



- **EUCC - Certifiering av produkter**
- **EUCS - Certifiering av molntjänster/Appar**



Har era befintliga leverantörer planer på att certifiera sina tjänster?

Framöver så kommer ni kunna kravställa på att leverantörers produkter och tjänster är certifierade.

EUCS - certifiering av moln och applikationstjänster

- Alla säkerhetskrav skall vara uppfyllda utifrån en framtagna kravkatalog av "säkerhetskontroller"
- Kravkatalogen hanterar bla frågeställningarna i Art 21.2, i tre nivåer av motståndskraft: Grundläggande, Betydande (NIS2) och Hög.
- Kontroll av följsamhet är: Grundläggande - "self assessment", CAB* på betydande och myndighet (ICC-FMV) på högsta nivåerna.
- EUCS lägger grund för fler certifieringar 5G, IOT mm

*CAB – Conformity Accreditation Body



Basic, Substantial, High Cloud Service Scheme

4. RISK MANAGEMENT

PROVIDE A GLOBAL INFORMATION SECURITY POLICY, DERIVED INTO POLICIES AND PROCEDURES REGARDING SECURITY REQUIREMENTS AND TO SUPPORT BUSINESS REQUIREMENTS.

Term	Definition
risk	effect of uncertainty on objectives Note 1 to entry: An effect is a deviation from the expected — positive and/or negative. Note 2 to entry: Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, group, and process). Note 3 to entry: Risk is often characterized by reference to potential events and consequences, or a combination of these. Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence. Note 5 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood. (SOURCE: From ISO Guide 73.3.1.1)
risk owner	person or entity with the accountability and authority to manage a risk (SOURCE: From ISO Guide 73.3.3.1.3)
risk management	coordinated activities to direct and control an organization's risk (SOURCE: From ISO Guide 73.2.1)
risk assessment	overall process of risk identification, risk analysis and risk evaluation (SOURCE: From ISO Guide 73.3.4.1)
risk identification	process of finding, gathering and describing risks Note 1 to entry: Risk identification involves the identification of risk sources, events, their impacts and their potential consequences. Note 2 to entry: Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholder's needs. (SOURCE: From ISO Guide 73.3.4.1)
risk analysis	process to comprehend the nature of risk and to determine the level of risk Note 1 to entry: Risk analysis provides the basis for risk evaluation and decisions about risk treatment. Note 2 to entry: Risk analysis includes risk estimation. (SOURCE: From ISO Guide 73.3.4.1)
risk evaluation	process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable

Term	Definition
risk treatment	process to modify risk (5.1) Note 1 to entry: Risk treatment can involve: <ul style="list-style-type: none">• avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;• taking or increasing risk in order to pursue an opportunity;• retaining the risk (acceptance);• changing the likelihood;• changing the consequences;• sharing the risk with another party or parties (including contracts and risk financing); and• retaining the risk by informed decision. Note 2 to entry: Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction". Note 3 to entry: Risk treatment can create new risks or modify existing risks. (SOURCE: From ISO Guide 73.3.6.1)
residual risk	risk remaining after risk treatment Note 1 to entry: Residual risk can contain unmitigated risk. Note 2 to entry: Residual risk can also be known as "retained risk". (SOURCE: From ENX Guide 73.3.6.1.4)

4.1 RM-01 RISK MANAGEMENT POLICY

4.1.1 Objective
Risk management policies and procedures are documented and communicated to stakeholders.

4.1.2 Requirements

Basic	Substantial
The CSP shall document policies and procedures in accordance with ISP-02 for the following aspects: <ul style="list-style-type: none">• Identification of risks associated with the loss of confidentiality, integrity, availability and authenticity of information within the scope of the ISMS and assigning risk ratings;• Analysis of the probability and impact of occurrence and determination of the level of risk;• Evaluation of the risk analysis based on defined criteria for risk acceptance and prioritization of remedial actions;• Handling of risks through measures, including approval of authorization and acceptance of residual risks by risk owners; and• Documentation of the activities implemented to enable consistent, repeatable and comparable results. RM-01.15	The CSP shall document policies and procedures in accordance with ISP-02 and using a documented risk analysis method that guarantees reproducibility and comparability, for the following aspects: <ul style="list-style-type: none">• Identification of risks associated with the loss of confidentiality, integrity, availability and authenticity of information within the scope of the ISMS and assigning risk ratings;• Analysis of the probability and impact of occurrence and determination of the level of risk;• Evaluation of the risk analysis based on defined criteria for risk acceptance and prioritization of remedial actions. RM-01.15

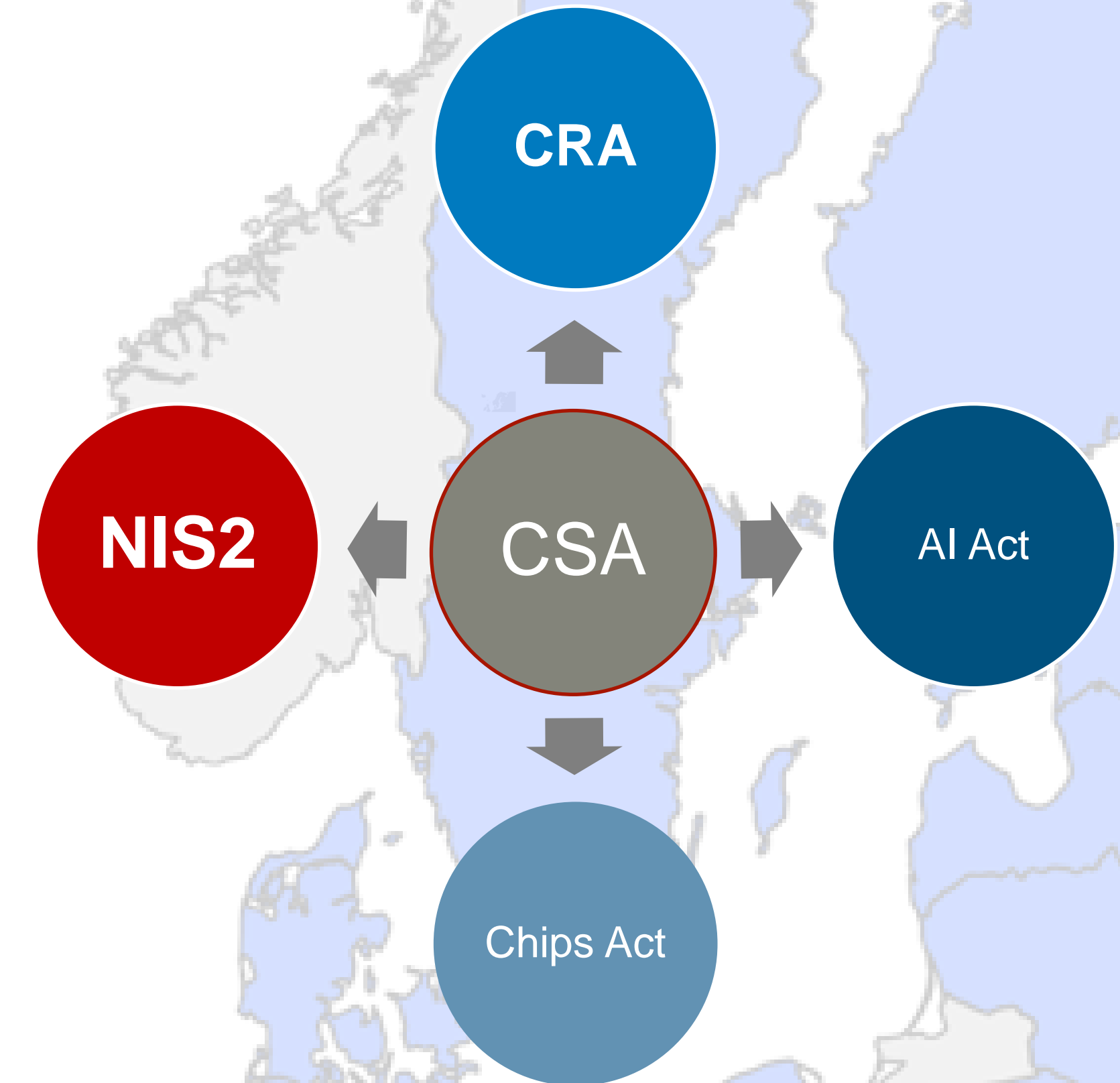
Ansvarar för CSA i Sverige:

Tillsynsmyndigheten ICC

- Etablerades genom beslut av FMV GD juni 2021. Ansvar för uppgifter som följer av EU:s cybersäkerhetsakt samt lag och förordning med kompletterande bestämmelser till EU:s cybersäkerhetsakt.
- I uppgiften ingår
 - **Omvärldsbevakning** av frågor som rör cybersäkerhet och cybersäkerhetscertifiering av IKT-produkter, -tjänster och -processer,
 - **Samverkan** med nationella och internationella aktörer på området och
 - **Tillsynsansvar** över efterlevnaden av det europeiska ramverket för cybersäkerhetscertifiering (EUCC, EUCS...)



Cybersecurity Certification
referenced in the different EU Laws



Den snabba digitaliseringen ger stora möjligheter, men utsätter också samhällen för nya typer av hot.



Cyberattacken mot Kaseya i juli 2021 är ett olyckligt och välkänt exempel på attacker i leveranskedjan.

SÄKERHET 2022-12-02 10:32

Softronic's kunder utslagna efter attack

På grund av vad som beskrivs som en säkerhetsrelaterad incident så har många av konsultbolaget Softronic's kunder drabbats hårt under morgonen. Just nu finns ingen prognos för när problemen väntas vara lösta.

NIS2 - Krav på säkerhet i leveranskedjan

Enligt NIS2-direktivet ska berörda verksamheter "entiteter" hantera säkerhetsaspekter i relationen mellan entiteten och dess direkta leverantörer och tjänsteleverantörer (samt deras ev underlev).

Detta gäller såväl i förhållande till eventuella sårbarheter hos varje direkt leverantör och tjänsteleverantör som den generella kvalitén av produkter och hur leverantören och tjänsteleverantören tillämpar cybersäkerhetskrav.

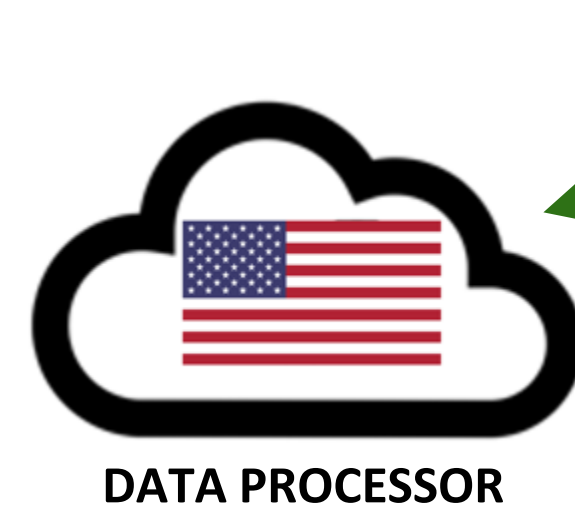
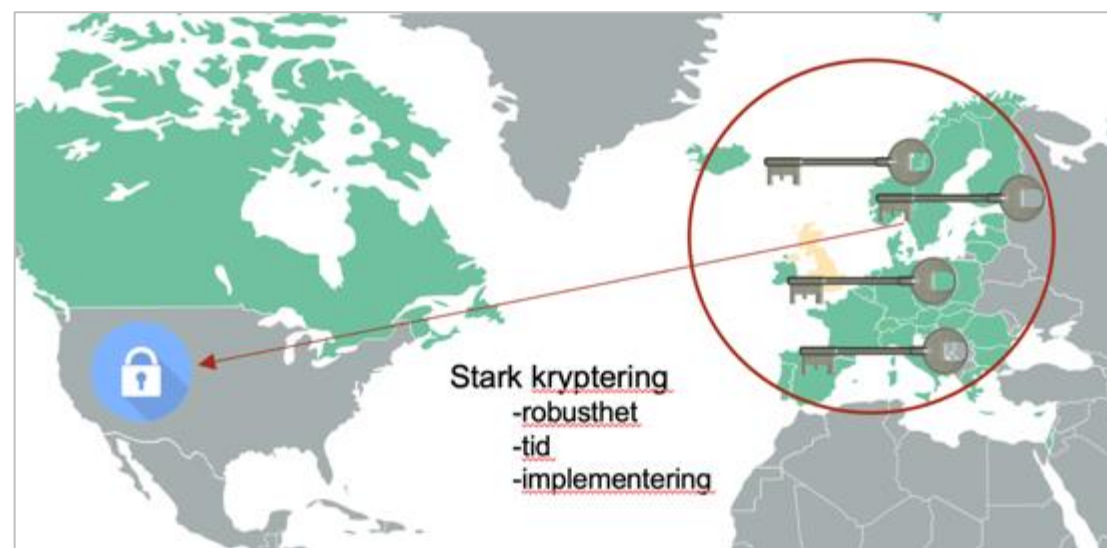
"offentliga förvaltningsentiteter" – har således inte bara ansvar för säkerheten i sin egen verksamhet, utan även de leverantörer de väljer att använda sig av.

Det nya kravet får betydelse för bedömningen av leverantörer i samband med IT-upphandlingar inom offentlig sektor. Kravet tillämpas vid sidan av de krav på säkerhet som uppställs i GDPR om tjänsteleverantören behandlar personuppgifter för myndighetens räkning.

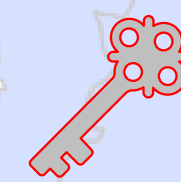
2021 - SCHREMS 2

- Registeransvarig, (processor/sub-processor) artikel 28 – artikel 82
- PUB-avtalet säkerställer försörjningskedjan
- Schrems 2 - EDPB-rekommendationer juni -21!

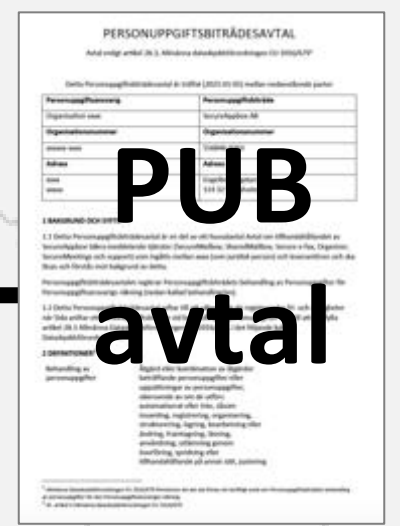
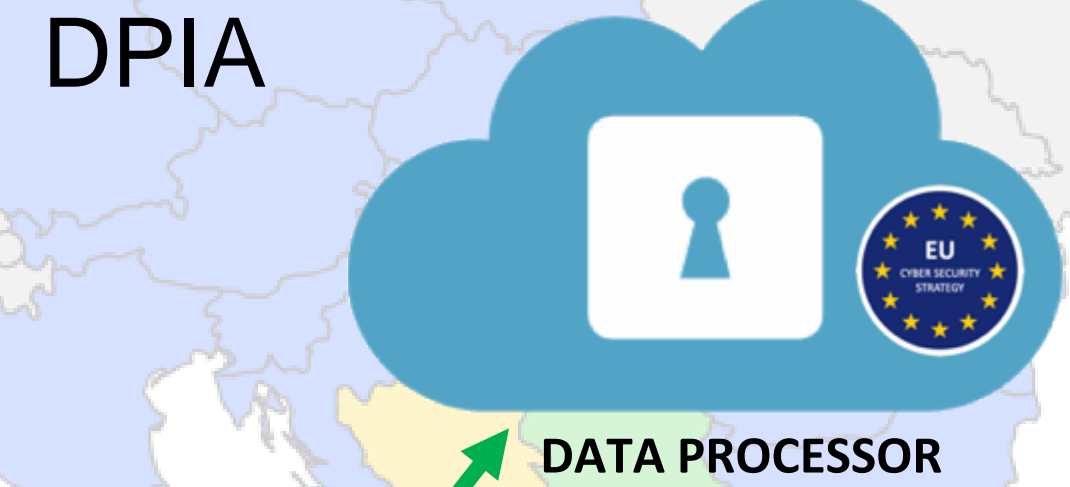
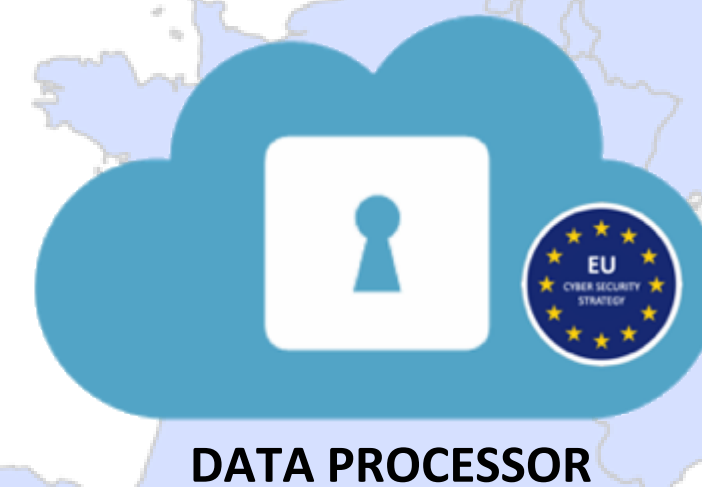
GDPR:
PERSONUPPGIFTSBITRÄDE
"DATA PROCESSOR"



TIA!



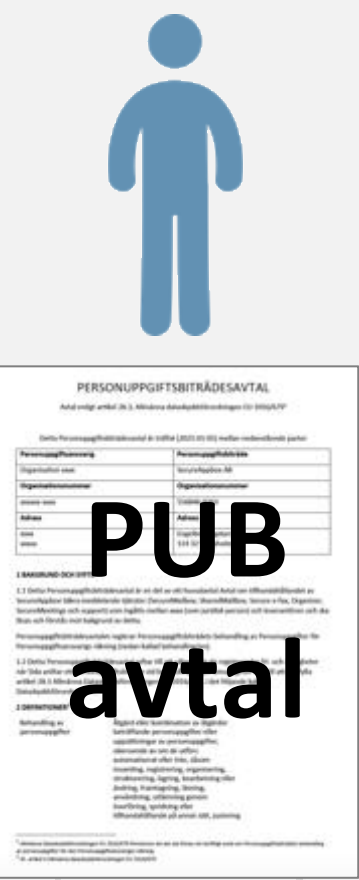
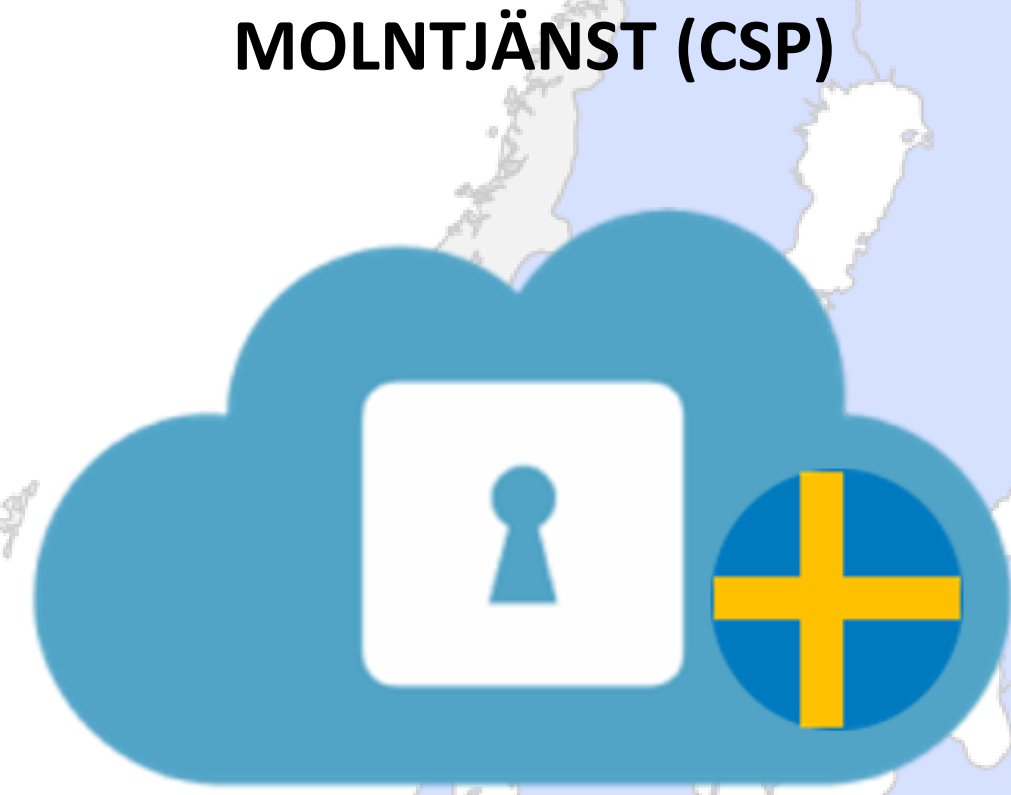
EU - Key Management Service/KMS (BYOK)
"Zero Knowledge"



PUB
avtal

GDPR - DELA ANSVAR MED DINA TJÄNSTELEVERANTÖRER

- Registeransvarig, (processor/sub-processor) artikel 28 – artikel 82
- PUB-avtalet säkerställer försörjningskedjan
- Privacy Shield (2) gäller igen, sedan 10 Juli 2023



IMY: Privacy Shield (2)

Mer information Relaterade länkar

- Pressmeddelande, beslut samt frågor och svar (EU-kommissionen)
- Lista över organisationer som omfattas av EU-US Data Privacy Framework (U.S. Department of Commerce)
- Frågor och svar om överföringar till USA efter EU-kommissionens beslut om adekvat skyddsnivå (Europeiska dataskyddsstyrelsen, EDPB)

Adekvat skyddsnivå vid överföring till tredjeland



12 oktober 2023

“The European Union General Court ruled against interim measures to pause the implementation of the EU-U.S. Data Privacy Framework. The court said to EU-member Philippe Latombe - **cannot prove the individual or collective harm the agreement raises.**”

DATA PROCESSOR



↓ TIA

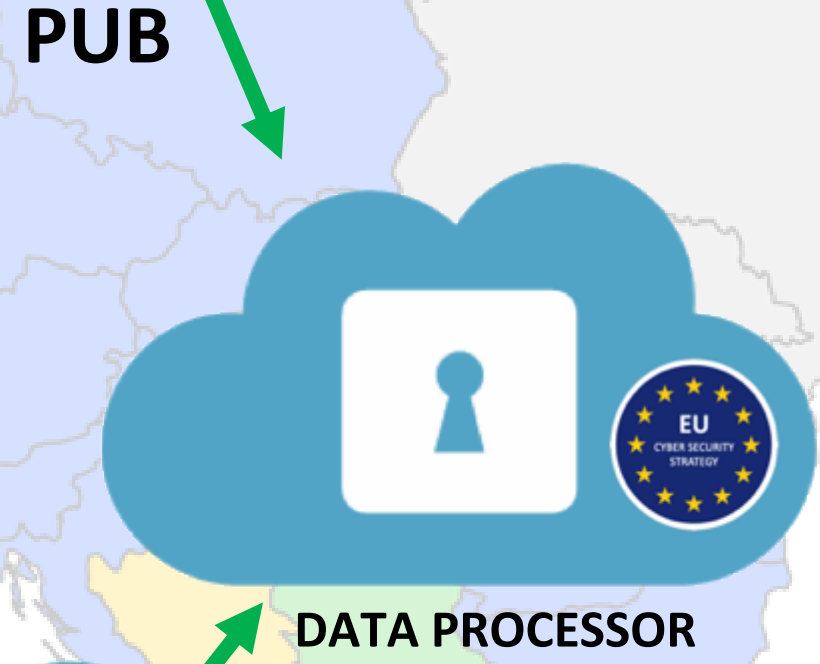
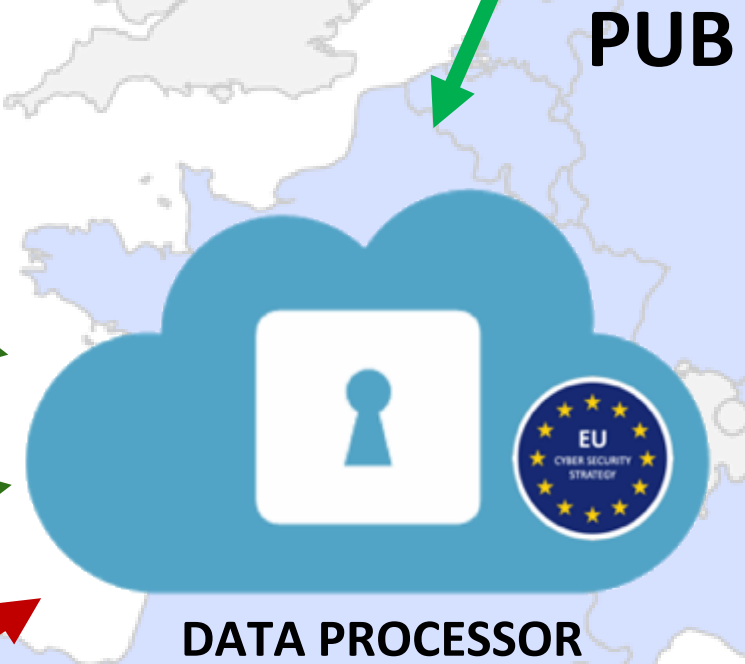


Privacy Shield 2

TIA!

TIA!

EU - Key Management Service/KMS (BYOK) "Zero Knowledge"



NIS2- SÄKERSTÄLL SÄKERHETEN I FÖRSÖRJNINGSKEDJAN (CSOC)!



- Kravställer säkerheten i leveranskedjan-CSOC!
- Certifiering: ISO 270XX, EUCS, EUCC, EU Cloud Code of Conduct
- SLA/QoS, Säker utv. Pen-tester, Redundans, kryptering HSM/KMS
- **Laglig etablering inom EU krävs.**

*EUCS - CSOC

Complementary Subservice Organization Controls

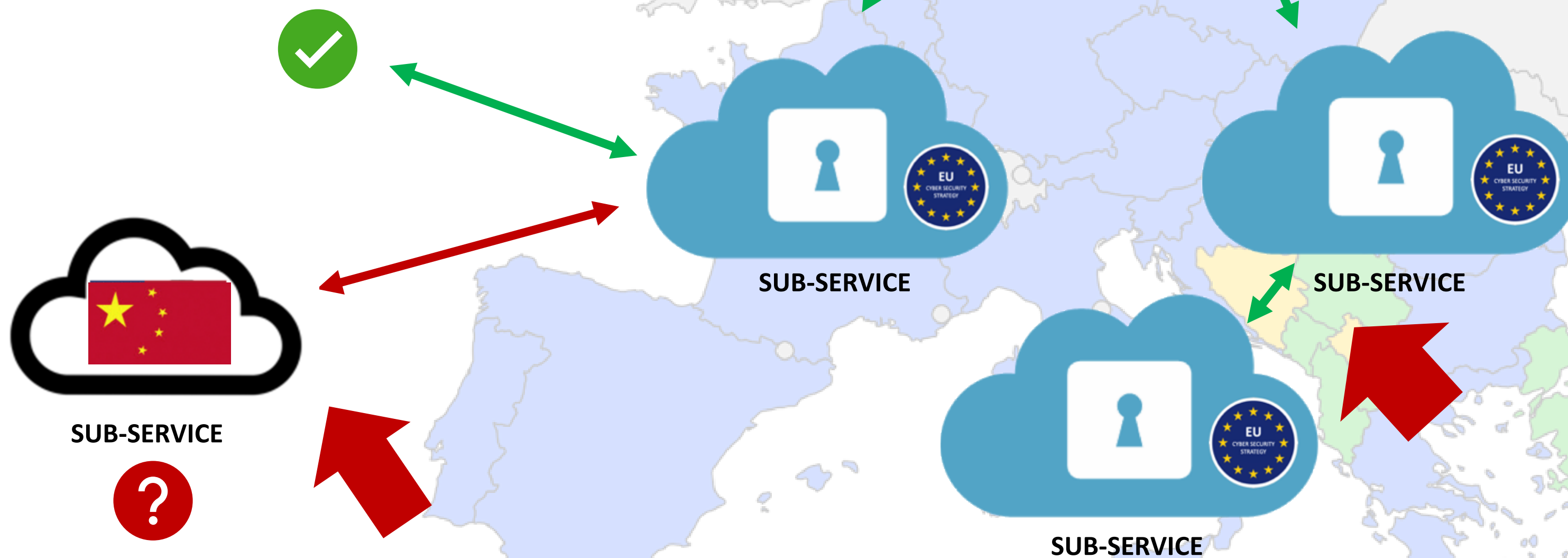
CABs will evaluate whether the controls related to the CSOCs are suitably designed, implemented and, for levels CS-Substantial/CS-High, operating effectively. Controls like access controls, authentication protocols, data encryption..

NIS2, Art 26

3. Om en enhet som avses inte är etablerad i unionen, men erbjuder tjänster inom unionen, ska den utse en representant i unionen. Ombudet ska vara etablerat i en av de medlemsstater där tjänsterna erbjuds. En sådan enhet ska anses falla under jurisdiktionen i den medlemsstat där företrädaren är etablerad.

I avsaknad av en företrädare i får varje medlemsstat där enheten tillhandahåller tjänster vidta rättsliga åtgärder mot enheten för överträdelse av detta direktiv.

Internationella företag måste vara etablerade inom EU



SUMMERING

Vad man behöver tänka på och vad som är viktigt vid upphandling av moderna IT- och molntjänster,
- speciellt inom offentlig verksamhet.

Vad gäller de som INTE omfattas av NIS2?
- Bra säkerhetsrutiner och motståndskraft är bra för alla verksamheter.



Alla behöver förstå riskerna och ledningen har ett tydligt ansvar

- **NIS2 sätter Cybersäkerhet på agendan.** Högsta ledningen i varje organisation behöver förstå vilken motståndskraft man har och vilken cyberrisk man tar.
- Alla behöver få till ett ”nuläge” - en **riskanalys utifrån NIS2** utökade omfattning och kartlägga verksamhetens risker i olika leverantörs och försörjningskedjor.
- **Analys och plan avseende kontinuitet** i verksamheten. Vad händer om kritiska system/tjänster går ner, internt/externt!
- EU kom med förtydligande 13 oktober kring NIS2 – ”en allrisk ansats”...

Kräver resurser...

Alla bör vara medvetna om att implementering av denna typ av praxis och kontroller kan kräva ytterligare ekonomiska och mänskliga resurser.

Det krävs högre nivå av testning, dokumentation av säkerhetsfunktioner från leverantörer, system integratörer och externa tjänsteleverantörer/ molntjänster. Vilket ökar deras/era kostnader och ev priset på produkter eller tjänster.

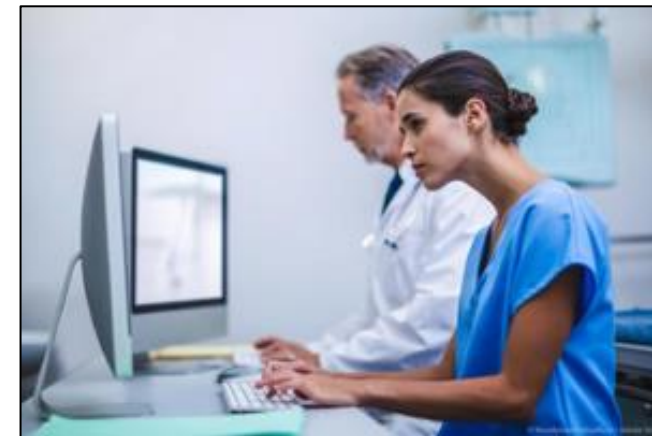
När man beslutar om detta, bör man beakta både kostnaderna för att implementera dessa kontroller och riskerna med att inte implementera dem.



Verksamhetssäkra

Fokus på fysiska risker som kan störa
möjligheten att utföra sitt samhällsuppdrag

- Motståndskraft mot fysiska attacker
- Naturkatastrofer, brand, översvämning..
- Inbrott, Terrorist attacker
- Pandemier
- Energiförsörjning/Transport



Informationssäkra

Fokus på IT-risker som kan störa
möjligheten att utföra sitt samhällsuppdrag

- IT-säkra, kvalitetssäkra och skydda
- Informations klassning
- Hantering av personuppgifter-DPIA/TIA*
- Tillgänglighet/molntjänster
- Driftsäkerhet

* Nytt avtal EU och USA 10/7-23 – Privacy Shield 2



Cybersäkra

Fokus på de cyber risker som kan störa
möjligheten att utföra sitt samhällsuppdrag

- Motståndskraft mot Cyber attacker
- Integrera/Separera/Kryptera
- Leveranskedjesäkerhet
- Externa beroenden
- IOT/Molntjänster

Pandemi!

2010

2016

2022

Bryssel den 13.9.2023: Därför bör de riskhanteringsåtgärder för cybersäkerhet som entiteten vidtar skydda inte bara entitetens nätverks- och informationssystem utan också dessa systems fysiska miljö mot sådana händelser som sabotage, stöld, brand, översvämning, telekommunikations- eller elavbrott eller obehörig fysisk åtkomst som kan undergräva tillgängligheten, riktigheten, integriteten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem.

Var står vi idag?

Starta arbetet för att ta reda på om och hur er verksamheten träffas av det nya uppdaterade NIS2 regelverket. Man behöver en grov handlingsplan, göra en GAP-analys och besluta vilka som ansvarar för vad.

Utbildning

Genomför en kort cyberutbildning av personer i ledningen kring Cyberrisker och NIS2.

Info Ledningen (delmål)

Presentera delrapport för ledningen med underlag på vilka risker verksamheten bedömer finnas och vilka konsekvenserna kan bli. Behöver vara överskådligt.

Infomöte

Genomför en informationsträff kring vad NIS2 är och förklara skillnaderna med tidigare direktiv. Bjud in de som ni tror omfattas.

Kvalificera

Kvalificera mer i detalj vilka nyckelområden som omfattas och vilka som behöver involveras

Identifiera och Analysera

Statusrapport / verksamhetsområde innehållande minst följande:

- Identifiering av viktiga leverantörskedjor och beroenden
- **Gå igenom era befintliga leverantörs avtal***
- Uppdatera er riskanalys – gör ett "allrisk" antagande

lev möten

Genomför möten med viktiga/kritiska underleverantörer för att veta hur de tänker kring NIS2

Sammanställ

Sammanställ en rapport med följande:

- En gemensam/sammanslagen analys
- Identifierat kritiska beroenden/lev.
- Förslag på prioriterad åtgärder

Mars/April - 2024...

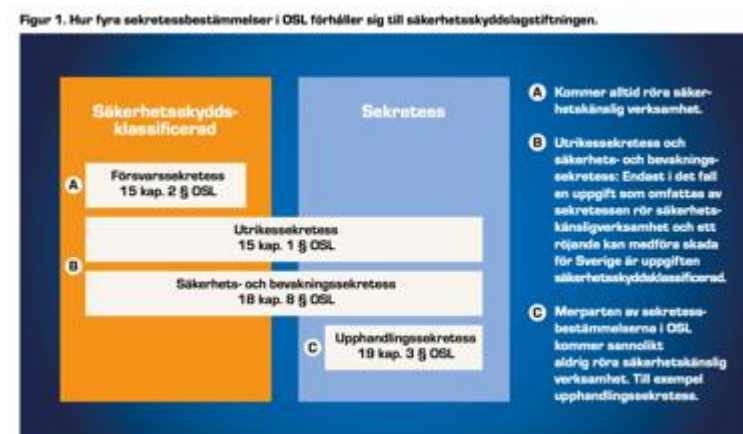
Gör en ny konsekvensanalys utifrån publicerade villkor och den riskanalys man gjort. Presentera dessa för ledningen som kan besluta om vad som behöver justeras/ändras.

Maj - 2024...

Åtgärda de saker som beslutas och förankra de risker man har kvar med ledningen och **lägga upp rutiner för Incidenthanteringen i enlighet kraven**

*Glöm inte era SCADA/OT processer

Nationella sekretess/säkerhetskrav: OSL 10.2 underlättar ut kontraktering NIS2 och Säkerhetsskyddslagen bygger på samma grundprinciper



Februari/Mars 2024

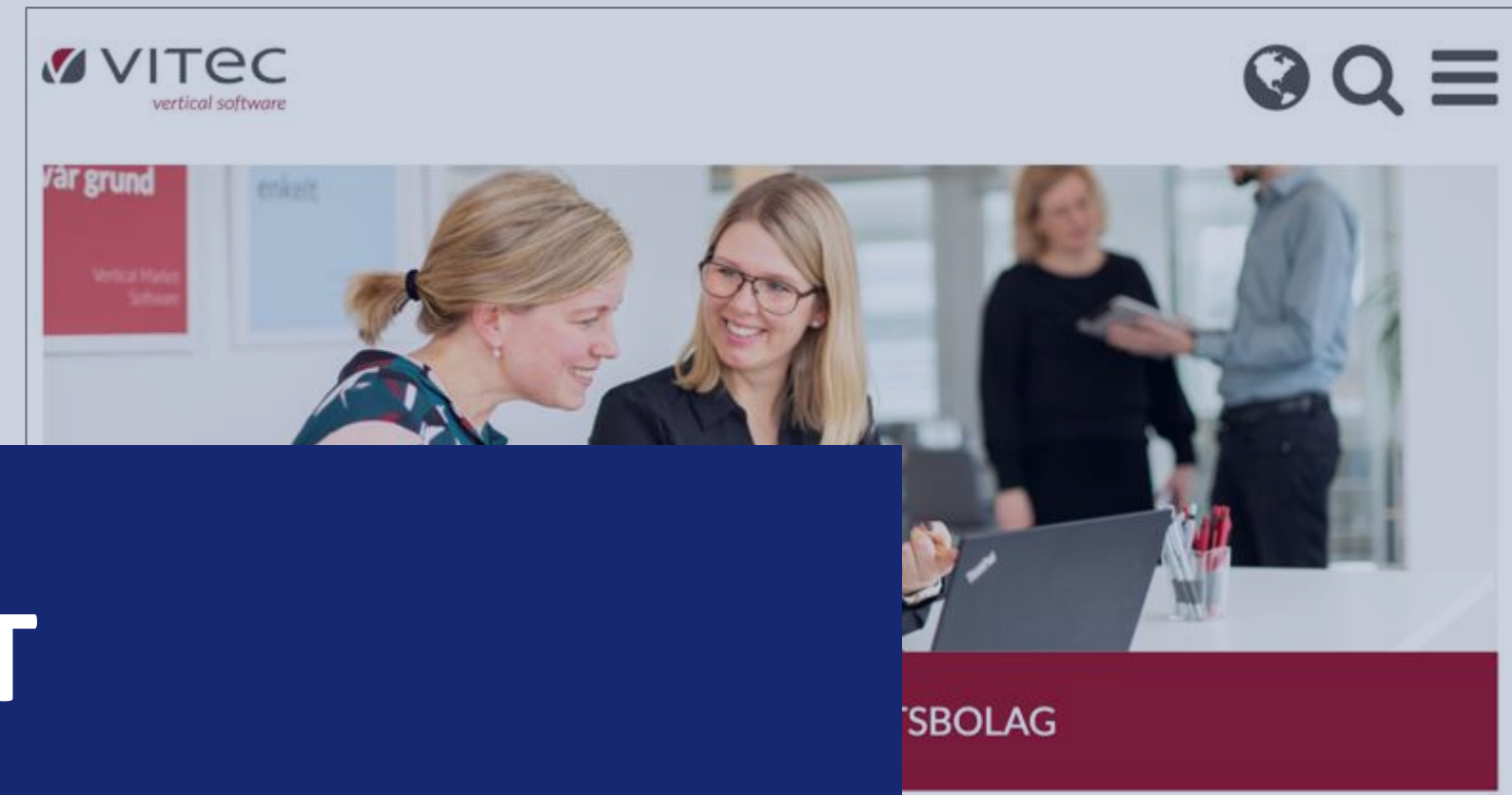
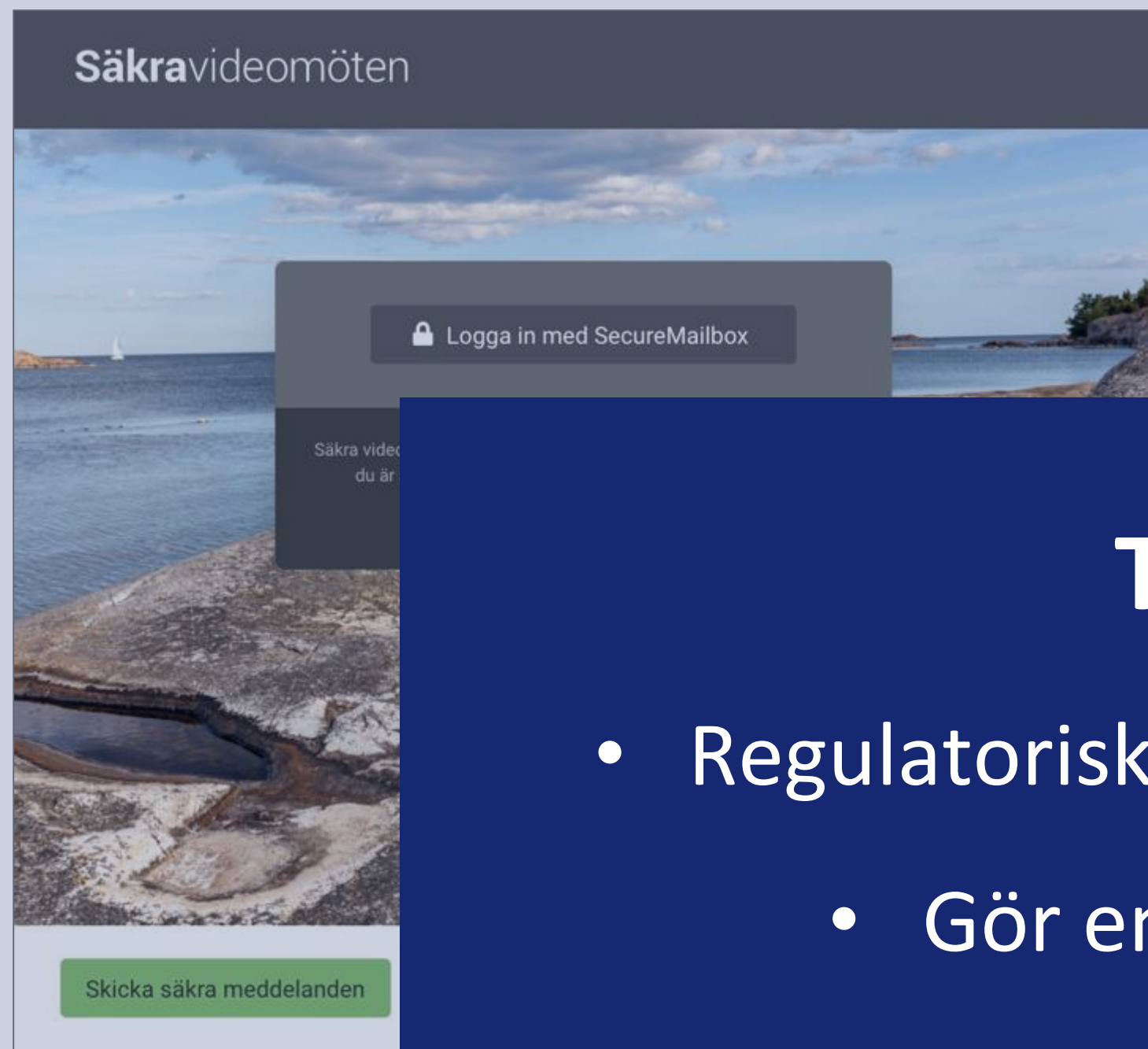
PTS/MSB presenterar detaljer hur NIS2 implementeras i svensk lag, vilka som berörs och när.

Oktober 2024

NIS2 träder i kraft över hela EU med krav på hög motståndskraft mot cyberattacker och rapporteringskrav

Intern

Extern



TRYGG DIGITALISERING I MOLNET

- Regulatorisk följsamhet, inte bara krav, utan stöd! – PUA, CSOC mm
 - Gör en övergripande handlingsplan för era risker (NIS2)
- Er säkerhet bygger på bra samarbete med era underleverantörer

”Säkerhet handlar om nära samarbete och långsiktighet, inte lägsta pris!”



plastic surgeons around the world with an expanding range of innovative implant solutions for improved patient outcomes.

FamiljehemSverige är en nationell tjänst för dig som vill göra en insats för ett barn eller ungdom.

FRÅGOR...

Tack och lycka till...



Anders Jonsson