Íslenskir staðlar

CRA lögin og staðlar

Erindi Guðmundar Valssonar

á Haustfundi FUT 2025

Íslenskir staðlar

Inngangur

•Af hverju er netöryggi orðið lykilatriði í vörum með stafræna þætti?

•Staðreynd: Kostnaður vegna netárása á heimsvísu er metinn á yfir €5,5 trilljónir á ári. [en.wikipedia.org]

•Markmið CRA: Tryggja að öll tæki og hugbúnaður sem tengjast neti séu örugg „by design“ og „by default“.

•Nýjar kröfur og staðlar fyrir öruggari stafræna framtíð

Íslenskir staðlar

CRA – Cyber resilience Act

- Lögin: Reglugerð (EU) 2024/2847 samþykkt í október 2024, í gildi frá 10. desember 2024, full framkvæmd frá 11. desember 2027.
- Hverjir falla undir CRA ?
  - Framleiðendur, innflytjendur, dreifingaraðilar og hugbúnaðarþróunaraðilar.
- Gildir um öll „products with digital elements“ – IoT, hugbúnað, vélbúnað, SaaS, o.fl.. Undantekningar: Svið með sérreglur (t.d. lækningatæki, bílar) og ókeypis opinn hugbúnaður án tekjuöflunar.
- Ábyrgð framleiðenda: Öryggi yfir allan líftíma vörunnar, hraðar öryggisuppfærslur, tilkynning um veikleika innan 24 klst.
- Viðurlög: Allt að €15 milljónir eða 2,5% af árstekjum.
- Á Íslandi fer innviðaráðuneytið – IRN - með málefni CRA

Íslenskir staðlar

Lykilkröfur

- Öryggi by design og by default
- Engar þekktar veikleikar við markaðssetningu
- Sjálfvirkar uppfærslur
- Vernd gagna: trúnaður, heilleiki, framboð

Key Definitions and Scope of Application

Product with digital elements: a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately

Remote data processing: data processing at a distance the software for which is designed and developed by the manufacturer, or under the responsibility of the manufacturer, and the absence of which would prevent the product with digital elements from performing one of its functions

Software: the part of an electronic information system which consists of computer code

Hardware: a physical electronic information system, or parts thereof capable of processing, storing or transmitting digital data

Manufacturer: a natural or legal person who develops or manufactures products with digital elements or has products with digital elements designed, developed or manufactured, and markets them under its name or trademark, whether for payment, monetisation or free of charge

Importer: a natural or legal person established in the Union who places on the market a product with digital elements that bears the name or trademark of a natural or legal person established outside the Union

Distributor: a natural or legal person in the supply chain, other than the manufacturer or the importer, that makes a product with digital elements available on the Union market without affecting its properties

Íslenskir staðlar

Kröfur til vara með „digital elements“

Article 6

Requirements for products with digital elements

Products with digital elements shall be made available on the market ***only*** where:

(1) they meet the essential requirements set out in Annex I, ***Part I, provided*** that they are properly installed, maintained, used for their intended purpose or under conditions which can reasonably be foreseen, and, where applicable, ***the necessary security updates have been installed***, and

(2) the processes put in place by the manufacturer comply with the essential requirements set out in Annex I, ***Part II.***

Íslenskir staðlar

Meginkröfur til upplýsingaöryggis

Annex I, Part I: Essential Cybersecurity Requirements
Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks,
be made available on the market without known exploitable vulnerabilities,
be made available on the market with a **secure by default** configuration,
ensure that vulnerabilities can be addressed through security updates,
ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems,
protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data,
protect the integrity of stored, transmitted or otherwise processed data,
process only data, personal or other, that are adequate, relevant and limited to what is necessary,
protect the availability of essential and basic functions, also after an incident,
have to implement **cybersecurity by design**,
provide the possibility for users to securely and easily remove on a permanent basis all data and settings.

Íslenskir staðlar

Veilumeðhöndlun - kröfur

Annex I, Part II: Vulnerability Handling Requirements
Manufacturers of products with digital elements shall identify and document vulnerabilities and components contained in products with digital elements,
address and remediate vulnerabilities without delay, including by providing security updates,
apply effective and regular tests and reviews of the security,
once a security update has been made available, share and publicly disclose information about fixed vulnerabilities,
put in place and enforce a policy on coordinated vulnerability disclosure,
take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components,
provide for mechanisms to securely distribute updates for products with digital elements,
ensure that, where security updates are available to address identified security issues, they are disseminated without delay.

Íslenskir staðlar

Flokkun á vörum eftir áhættu

Flokkur	Lýsing	Dæmi	Samræmiskröfur
Default	Almennar vörur með stafræna þætti	Snjalltæki, Bluetooth hátalarar	Sjálfsmat og CE merking
Class I (Mikilvægar)	Vörur með aukna öryggisáhættu	VPN, eldveggir, lykilorðastjórar	Þriðja aðila mat eða staðlar
Class II (Gagnrýnar)	Há áhætta, mikilvæg netöryggislausn	Stýrikerfi, PKI, HSM, IDS/IPS	Strangara mat hjá tilkynntu aðila

Cybersecurity as a Requirement "by design": Manufacturer

- **Risk assessment** for the design, development, manufacture, supply and maintenance of products
- **Digital supply chain:** third-party components must not compromise the cybersecurity of the end product
- **Documentation** obligation, declaration of conformity and consumer information
- Determination of a support period for the normal **service life of a product,** but at least five years
- **Corrective measures** in the event of missing/inadequate cybersecurity up to and including withdrawal/recall
- **Notifications to the National CSIRT and ENISA** after becoming aware of actively exploited security vulnerabilities

Cybersecurity as a Requirement "by design": Importer and Distributor

- Importers:
  - Only placing on the market of products with CRA conformity
  - Requirements comparable with manufacturer, additional information obligations (in particular contact details)
  - Withdrawal/recall in the event of non-compliance with CRA
  - In the event of cybersecurity weaknesses, information to competent market surveillance authorities in the Member States and manufacturers
- Distributors: Comparable requirements to importers with regard to conformity with CRA, additional verification of whether the manufacturer and importer have complied with the CRA requirements

Íslenskir staðlar

In scope: “products with digital elements”

✓ **Hardware products** (including components placed on the market)
(laptops, smart appliances, mobile phones, network equipment or CPUs…)

✓ **Software products** (including components placed on the market)
(operating systems, word processing, games or mobile apps, software libraries…)

…including their **remote data processing solutions**!

Íslenskir staðlar

Outside the scope

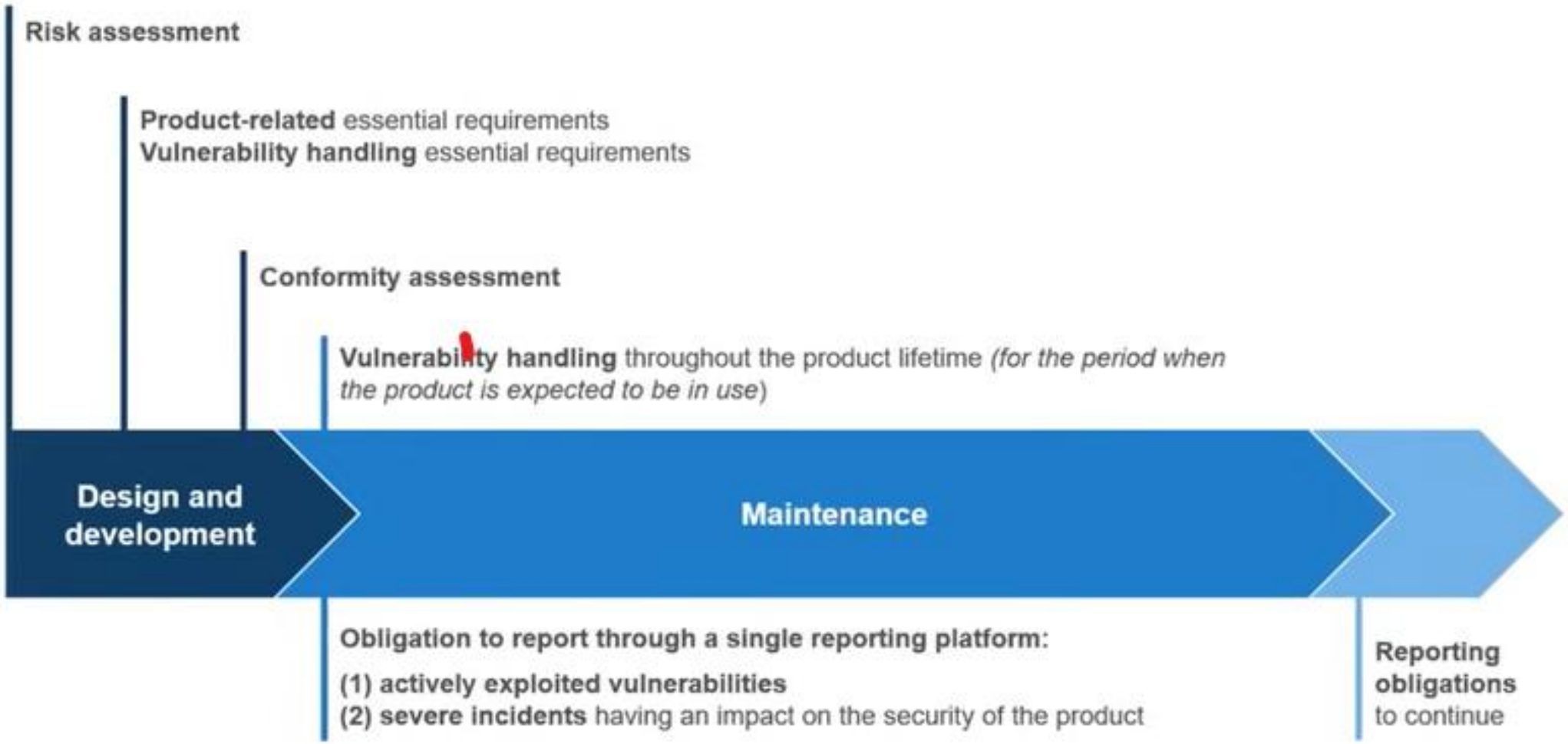
✗ **Non-commercial products**
(hobby products)

✗ **Services, in particular standalone SaaS** (covered by NIS2)
(websites, purely web-based offerings…)

✗ **Outright exclusions**
(cars, medical devices, in vitro, certified aeronautical equipment, marine equipment)

Íslenskir staðlar

Obligations of manufacturers



Íslenskir staðlar

CRA og samhæfðir staðlar

- Staðlar sem eru skrifaðir samkvæmt beiðni frá Evrópusambandinu kallast samhæfðir stalar og tilheyra NLF
- Samhæfðir staðlar eru grundvöllur fyrir CE merkingum vara
- Þá er gefin út samræmisyfirlýsing um hvaða staðlar eru uppfylttir
- Í þessu tilfelli eru vörur flokkaðar í 4 flokka

Íslenskir staðlar

Samræmisyfirlýsing – CE „merking“

Conformity assessment – product categorisation

Default category — self-assessment
(memory chips, mobile apps, smart speakers, computer games...)

Important products — application of standards/third-party assessment
(operating systems, anti-virus, routers, firewalls…)

Critical products — in the future potentially certification
(smart cards, secure elements, smart meter gateways…)

FOSS — self-assessment (unless categorized as “critical products”)
(web development frameworks, operating systems, database management systems…)

CRA implementation underway

- Development of harmonised standards
- Technical descriptions of important and critical products
  - *To be adopted by 11 December 2025*
- Terms and conditions for CSIRTs to withhold notifications
  - *To be adopted by 11 December 2025*
- Single Reporting Platform by ENISA
  - *To be operational by 11 September 2026*

CRA implementation underway

- Development of harmonised standards
- Technical descriptions of important and critical products
  - *To be adopted by 11 December 2025*
- Terms and conditions for CSIRTs to withhold notifications
  - *To be adopted by 11 December 2025*
- Single Reporting Platform by ENISA
  - *To be operational by 11 September 2026*

CRA implementation underway - continued

- Guidance to support implementation
  - *Covering at least RDPS, OSS, support period, interplay with other Union legislation, substantial modification + targeting SMEs*
- Member States to set up notifying & market surveillance authorities
- CRA Expert Group
  - First meeting on 12 February; additional fora for involvement

Standardisation

- Standardisation request for harmonised standards adopted by COM and notified to ESOs
- Building on existing international and European standards
- 2-tiered approach: horizontal and vertical standards
- Prioritising important/critical products (CRA Annex III/IV)
- First building blocks for product security ecosystem of standards

Vertical developments CEN-CLC TCs

- **CEN/TC 224 'Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment'**
  - European standard(s) on essential cybersecurity requirements for identity management systems and privileged access management software and hardware, including authentication and access control readers including biometric readers (line 16)
  - European standard(s) on essential cybersecurity requirements for Hardware Devices with Security Boxes (line 39)
- **CLC/TC 65X 'Industrial-process measurement, control and automation'**
  - Developments based on EN IEC 62443-4-2
- **CEN-CLC/JTC 13 WG 6**
  - European standard(s) on essential cybersecurity requirements for smart meter gateways within smart metering systems (line 40)
  - European standard(s) on essential cybersecurity requirements for hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments (Line 35)

Íslenskir staðlar

CRA Staðlar fyrir iðnaðarferli

- CRA byggir mikið á stöðlum m.a.
- ISO/IEC 27001 – Upplýsingaöryggi
- IEC 62443 – Iðnaðaröryggi
- ISO 9001 – Gæðastjórnun
- Mjög áhugaverður staðlaröð IEC 62443 þar sem lagt er til sameiginlegt líkan til að byggja upp traust á upplýsingaöryggi i mikilvægum iðnaðarferlum. S.s. Vatnsveitum, Rafveitum og slíkum kerfum sem keyra á nettengdum búnaði sem getur verið útsettur fyrir áhættu vegna upplýsingaöryggis.
- Skrifaðir verða evrópuviðaukar við staðla í röðinni til að víkka notkunarsvið þeirra og taka inn kröfur CRA.

FUT og CRA

- Spegilnefnd: FUT gæti stofnað spegilnefnd þar sem fylgst yrði með evrópskri staðlagerð á sviðinu.
  - Ásamt því að vera vettvangur sérfræðinga sem vilja kynna sér málefni CRA í hópi sérfræðinga sem vinna að svipuðum hagsmunum.
  - Þá gæti þýðing lykilhugtaka verið framkvæmd í slíkum hópi ef þörf væri á.
- FUT skráð sérfræðinga frá íslenskum hagaðilum til þátttöku í evrópskri staðlagerð á sviðinu
- Markhóp slíkrar spegilnefndar eru
  - Ráðuneyti
  - Sérfræðingar skipulagsheilda sem framleiða vörur með nettengda stafræna þætti sérstaklega þá sem reka krítísk kerfi s.s. Veitukerfi, iðnaðarferla ofl.
  - Ráðgjafar sem hyggjast sinna þessum markaði
- Ef þú hefur áhuga á að spegilnefnd um CRA verði til þá sendu mér skeyti á gudval@stadlar.is
- Spegilnefndir eru einingis stofnaðar ef nægur áhugi er á þátttöku í þeim.