CRA and compliance – what to do?

Björn Sjöholm

bear@unidot.se

EU:s legislation on products with digital elements

”The Cyber Resilience Act will introduce extensive challenges to organisations that develop products with digital elements. The requirements will hit several parts of your organisation like software development, product management, testing, marketing and risk management. How can an organisation handle this challenge and where do you start?”

Björn Sjöholm

Cyber Security Entrepreneur

bear@unidot.se

Business leader, Advisor, Auditor, Trainer
Cyber Security, IT-Security, Information Security

M.Sc. Comp.Sci.
CISA, CISM, CRISC, CGEIT, CDPSE, CISSP
ISO 27001 Lead Auditor, Kantara Accredited Assessor

Linkedin: linkedin.com/in/bjornsjoholm

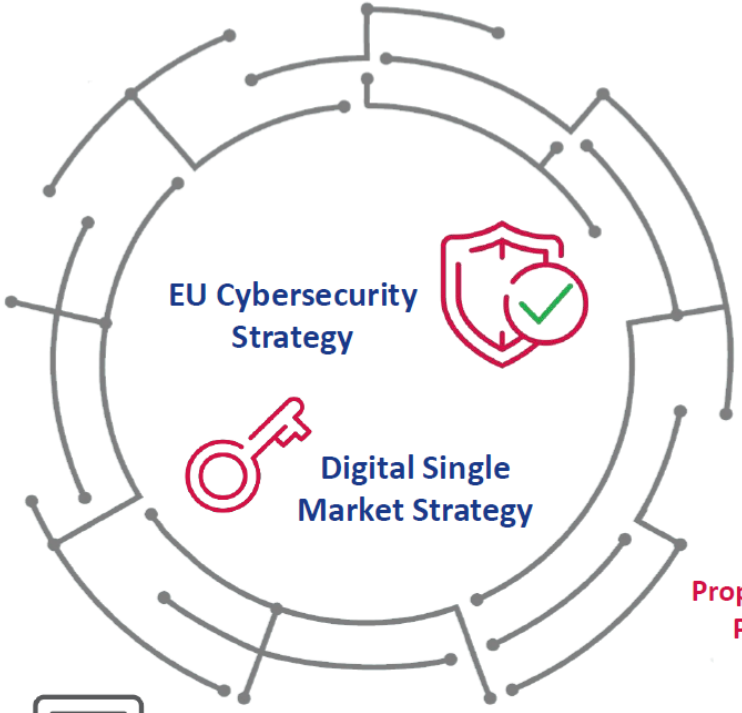
unidot

seadot
CYBERSECURITY

Agenda

- EU Cybersecurity Legislation
- What is actually compliance?
- CRA
  - Who / What is affected?
  - Penalties
  - Requirements
  - When?
- How to comply - Your compliance activities

EU Cybersecurity legislation



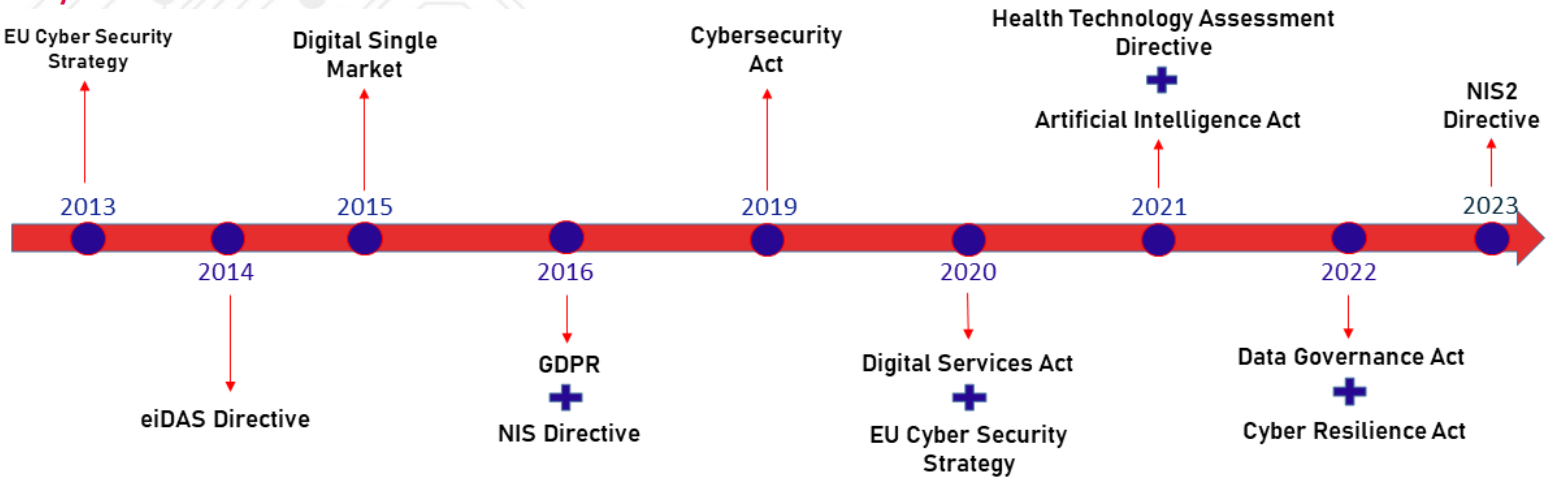
Network and Information Security Directive

eIDAS Regulation

Payment Services Directive 2

General Data Protection Regulation

Proposal for a Regulation on Privacy and Electronic Communications



What are the trends?

- General and sector specific regulations

- In GDPR, NIS, NIS2, PSD2, DORA, CER, CRA … you will find requirements on:

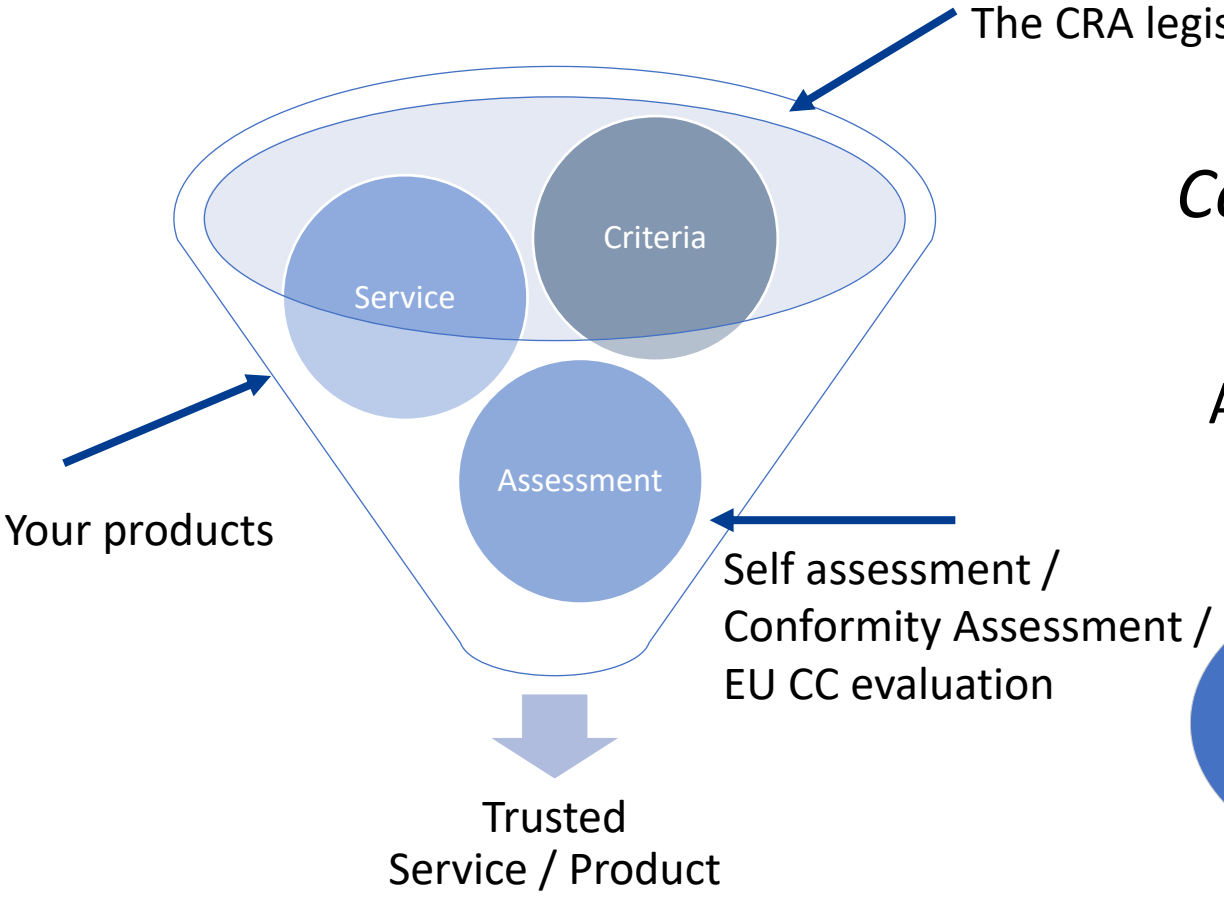
  Incident reporting

  Supply chain management & security

What is actually compliance?

… or regulatory compliance

Compliance & Trust



Compliance is handling another party's risk

Adhering to requirements or set of controls in a standard, contract or regulation

Who / What is affected?

Who / What is affected?

- Products with digital elements
- Organisations (in EU) in the complete supply chain of the product and its component
  - Organisations that import to EU resposible for supply chain of imported components
- … if the product is not covered by other specific regulation
- Security for components in the complete supply chain and lifecycle of the product:
  - Will require SBOM - Software-Bill-Of-Materials
- SaaS/cloud excluded
  - if the product does not depend on them, i.e. remote data processing solutions

CRA – Critical products

Class I

1. Identity management systems software and privileged access management software;
2. Standalone and embedded browsers;
3. Password managers;
4. Software that searches for, removes, or quarantines malicious software;
5. Products with digital elements with the function of virtual private network (VPN);
6. Network management systems;
7. Network configuration management tools;
8. Network traffic monitoring systems;
9. Management of network resources;
10. Security information and event management (SIEM) systems;
11. Update/patch management, including boot managers;
12. Application configuration management systems;
13. Remote access/sharing software;
14. Mobile device management software;
15. Physical network interfaces;
16. Operating systems not covered by class II;
17. Firewalls, intrusion detection and/or prevention systems not covered by class II;
18. Routers, modems intended for the connection to the internet, and switches, not covered by class II;
19. Microprocessors not covered by class II;
20. Microcontrollers;
21. Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) intended for the use by essential entities of the type referred to in [Annex in NIS2];
22. Industrial Automation & Control Systems (IACS) not covered by class II, such as programmable logic controllers (PLC), distributed control systems (DCS), computerised numeric controllers for machine tools (CNC) and supervisory control and data acquisition systems (SCADA);
23. Industrial Internet of Things not covered by class II.

Class II

1. Operating systems for servers, desktops, and mobile devices;
2. Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments;
3. Public key infrastructure and digital certificate issuers;
4. Firewalls, intrusion detection and/or prevention systems intended for industrial use;
5. General purpose microprocessors;
6. Microprocessors intended for integration in programmable logic controllers and secure elements;
7. Routers, modems intended for the connection to the internet, and switches, intended for industrial use;
8. Secure elements;
9. Hardware Security Modules (HSMs);
10. Secure cryptoprocessors;
11. Smartcards, smartcard readers and tokens;
12. Industrial Automation & Control Systems (IACS) intended for the use by essential entities of the type referred to in [Annex I in NIS2], such as programmable logic controllers (PLC), distributed control systems (DCS), computerised numeric controllers for machine tools (CNC) and supervisory control and data acquisition systems (SCADA);
13. Industrial Internet of Things devices intended for the use by essential entities of the type referred to in [Annex I in NIS2]
14. Robot sensing and actuator components and robot controllers;
15. Smart meters.

Supply Chain

CRA

- Responsibility for the complete supply chain of the product and its component

Sanctions

Penalties

CRA

- Non-compliance administrative fines up to (whichever is higher of):
  - 15 000 000 €,
  - 2,5 % of total worldwide annual turnover

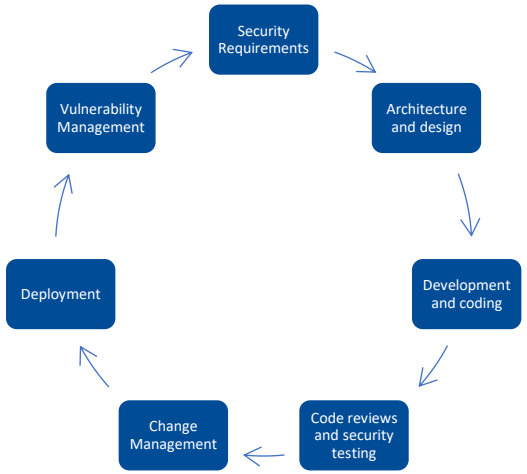
unidot

Requirements?

Requirements- CRA

- Requirements covering the whole life cycle of products
- Cybersecurity Essential Requirements
- Security updates
- Secure by default
- Vulnerability handling
- Notification of known exploited vulnerabilities
- Software Bill Of Materials (SBOM) of all components
- Planning, design, development or production, testing and maintenance of the product
- Risk management
- Secure Development Lifecycle (SDLC)
- Quality assurance

- CE marking for each individual product
- Conformity assessment
  - Internal control procedure, i.e. self assessment
  - Assessment by third-party body
  - Certification under scheme of Cyber Security Act.



When?

When?

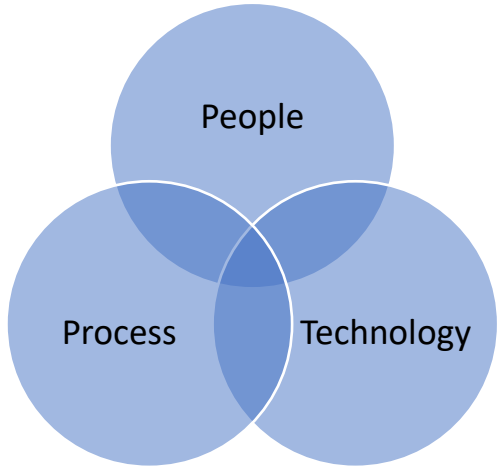
CRA

- Regulation applies 36 months from its entry into force
- Reporting obligation on exploited vulnerabilities applies after 21 months

How to comply? – Your compliance activities

CRA

Compliance management



Your Compliance Activities

Scope
- Products & Models

Maturity analysis
- How do we comply today?
- Starting point for due diligence

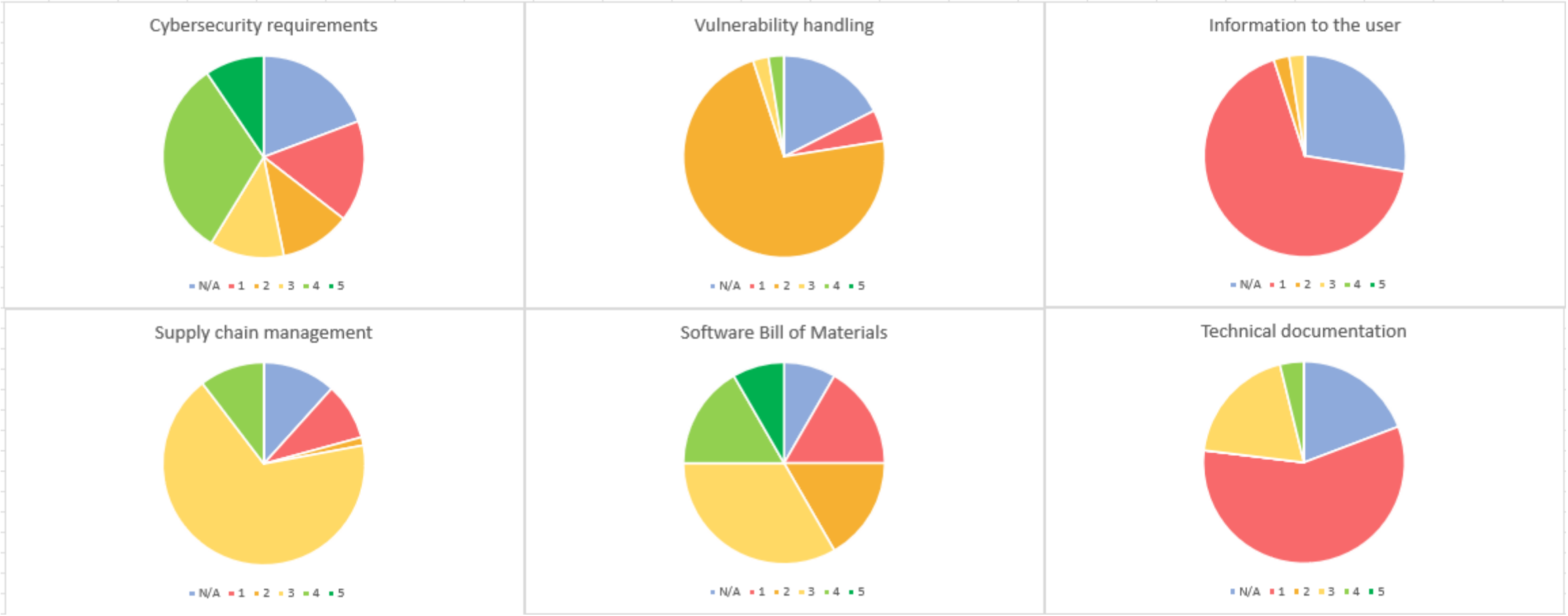
Product prioritizing
- Merge and/or phase out products

Compliance project
- Management support, Risk Management
- Vulnerability handling / Incident management, SBOM
- SDLC, Supply chain management. Technical documentation, Information to users

Maintenance
- Management system implementation and integration

unidot

Example gap/maturity assessment



Management support & Roles in the organization

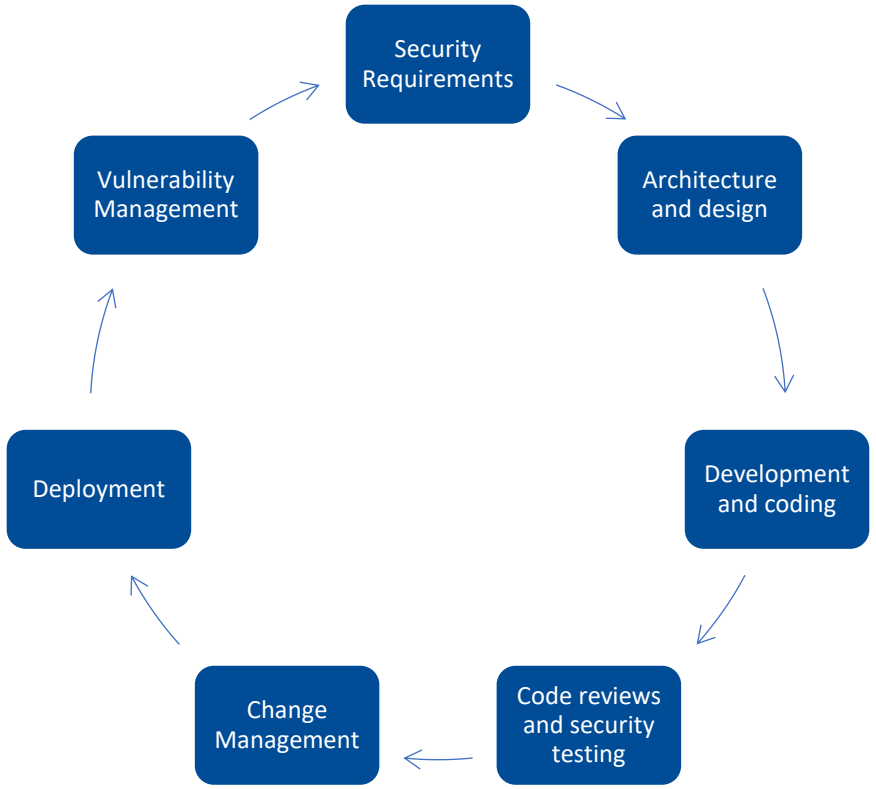
- Board and executive leadership
- CTO
- Product lead
- Product development and maintenance
- Market and Communication
- Procurement
- Internal control and Compliance

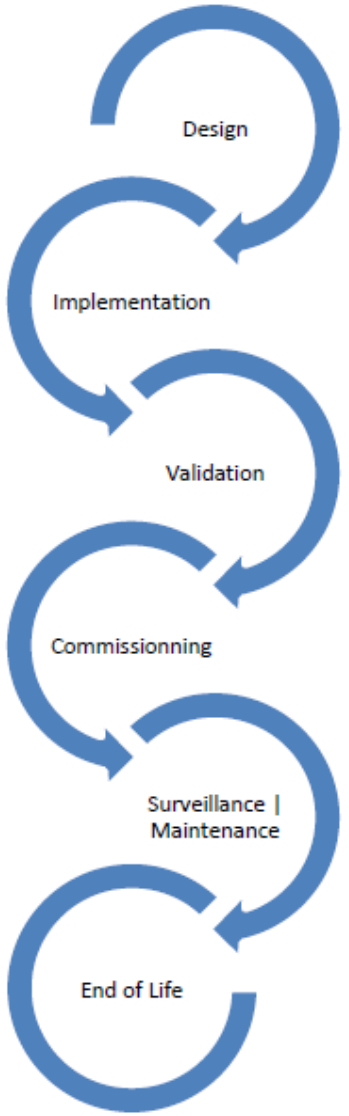
Risk Management

Risk treatment:

- Risk mitigation
- Risk transfer
- Risk acceptance
- Risk avoidance

Product Life-cycle & SDLC





Management System

- You will need a Management System for Security and Products
- You will need a Secure Software Development Lifecycle

- Integrate with existing:
  - Quality Management System (QMS) (ex. ISO 9001)
  - Information Security Management System (ISMS) (ex. ISO 27001)
  - Product Lifecycle Management System (PLM)

Questions?

CRA and compliance – what to do?

Björn Sjöholm

bear@unidot.se