Compliance Automation and Information Security - Liberal Reflections

Anne-Marie Eklund Löwinder,
Chief Information Security Officer,
The Internet Foundation In Sweden
amel@iis.se
@amelsec
https://www.iis.se
About IIS

An independent organization with two main roles:

• Responsible for the operation and administration of the top-level domains .se and .nu.

• Promote the development and use of the internet in Sweden.
Standards & Frameworks
Making our lives easier

- **NIST**
  - US-centric
  - 800-X family
  - Detailed, ready to use
  - No formal certification

- **ISO**
  - EU-centric
  - High level
  - Process oriented
  - Certifiable by independent body

- **Adoption**
  - Do not invent the wheel
  - Cost-benefit analysis
  - Multiple standards implementation
  - Scope is critical

- **Customization**
  - Understand your own enterprise
  - Pick wisely
  - Involve business
  - Make sure you understand the framework
Cost of Security
How secure do you want to be?

Enterprise wants to …
• Make profit!
• Do business
• Be agile
• Not be blocked by security

• Enterprise wants to be as secure as possible for as little cost as possible

Learn to answer the tough questions in the educated way

Security wants to …
• Spend resources
• Limit access & operations
• Have formal procedures & standards
• Have control

• Security in enterprise is always a cost, never profit

Learn to make a business case & accept the business decisions
Information is an **asset** which, like other important business assets, has **value** to an organization and consequently needs to be **suitably protected**.
Information Security Management System

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.
Information Security Management System (ISMS)

Is a systematic and structured approach to managing information so that it remains secure
CIA – The core principles of information security
Advantages if an organization is ISMS Certified (ISO/IEC 27001:2013)

- Provide a structured way of managing information security
- Provide an independent assessment
- Provide evidence and assurance
- Enhance information security governance
- Enhance the organisation’s global positioning and reputation
Compliance

• Define compliance requirements
• Procedures implemented to comply with requirements (e.g. personal data/privacy protection)
• Regular Compliance checks
Threats and vulnerabilities

• Threats come from different sources
• Threats can be identified
• Vulnerabilities exists in the system
• Threats exploit vulnerabilities
Security and compliance at velocity

- Embed compliance into the software delivery pipeline
- Automated checking of compliance criteria with analytics
- Structured review process during development
- Discovery and analysis
- Patch management and remediation
Automated tests?

1. Availability, if the system is there and alive

2. Recovery, do contingency plans exist, do they work and how quickly will it take to recover from an incident, should something bad happen

3. Perimeter defense and resilience, do we have simple hygiene factors in place and what can the system handle regarding for instance performance and throughput

4. Procedures, do we have the security procedures in place to produce and deploy code in production
Thanks! Questions?

Anne-Marie Eklund Löwinder
Chief Information Security Officer, IIS
amel@iis.se
@amelsec
https://www.iis.se