itrust consulting

Move securely within the cyberworld

New Trends in InfoSec, Cybersecurity and Supply Chain Attacks

Cloud Cybersecurity Fortress of Open Resources and Tools for Resilience (CyFORT)

itrust consulting s.à r.l.
55, rue Gabriel Lippmann
L-6947 Niederanven

Tel: +352 26 176 212 6
Fax: +352 26 710 978
Web: www.itrust.lu

Dr Carlo Harpes
itrust consulting

itrust consulting

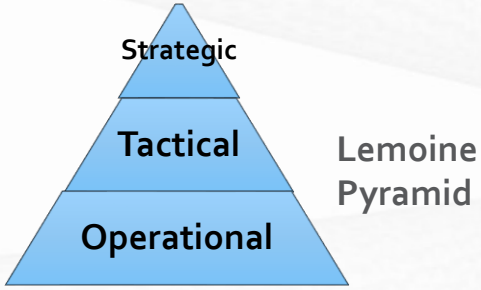
- **itrust**: acronym of
  'Information: Techniques and Research for Ubiquitous Security and Trust'
- An SME from Luxembourg specializing in Information Security Systems
  - CISOaaS, DPOaaS, Internal Audits (Technical, Compliance, hacking)
- High-turnover from co-funded R&D over past years (28%, 10%, 13%, 17%…)
- Start-up of the year 2008
- Current staff: ~18 persons
- Turnover ~1,5 M€ since 2013
- Customer:
  - Public sector
  - Energy sector
  - SME and industries

itrust consulting

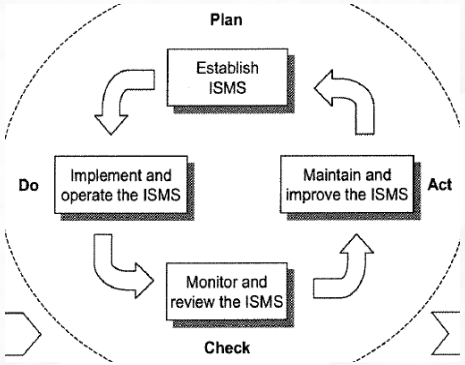
- **Norms related to the management of Information Security**

Terminology	ISO 27000				
Requirements	ISMS Requirements IS **27001:2013**	Certification Requirements IS 27006		TISAX RESULT AVAILABLE	Règle technique d'exigences et de mesures pour certification des PSDC
Guidance (for all domains)	Code of Practice IS 27002:2022	Implementation Guidance IS 27003:2017	Management Measurements IS 27004:2016	Risk Management IS 27005:2018	
Domain-specific guides	Telecom. IS 27011:2016	Health IS 27799:2016	Process control systems – Energy TR 27019:2017	TISAX RESULT AVAILABLE	
Toolbox of techniques	Storage security 27040	Incident Management TR 27035-x	Intrusion Detection IS 17039	IT Network Security IS 17033-x	

- Common structure for all management system (ISO 9000, 14000…)
- But RISK driven!



Lemoine Pyramid



InfoSec: ISO 27002:2022 (NEW!)

- **Old themes**
  - 5 Information security policies
  - 6 Organization of information security
  - 7 Human resource security
  - 8 Asset management
  - 9 Access control
  - 10 Cryptography
  - 11 Physical and environmental security
  - 12 Operations security
  - 13 Communications security
  - 14 System acquisition, development and maintenance
  - 15 Supplier relationships
  - 16 Information security incident management
  - 17 Info.Sec. aspects of business continuity mgt
  - 18 Compliance

- **New**
  - 5 Organizational controls (37)
  - 6 People controls (8)
  - 7 Physical controls (14)
  - 8 Technological controls (44)
  - **Total of 93 controls/safeguards**

- **To be done:**
  - **Adapt**
    - Policies,
    - Risk treatment
    - Audit

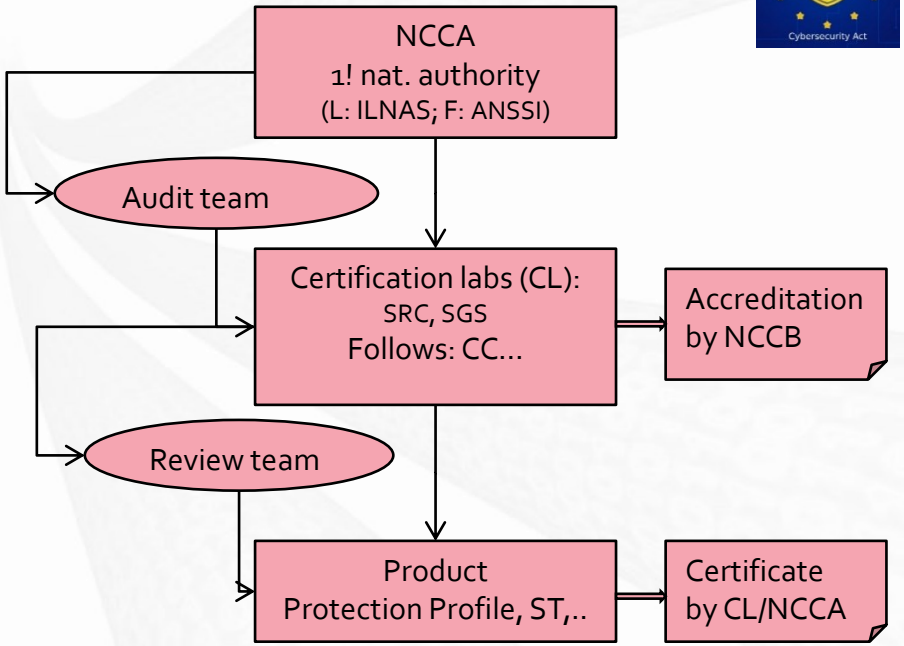
- **Legal context**
  - **2016: GDPR,** focused on data privacy for both individuals and legal entities.
    - obligation to proof compliance to principles, for incident reporting,
    - high penalties by CNPD possible.
  - **2016: eIDAS,** establishing guidelines for electronic identification and transactions.
  - **2017: NIS Directive,** proposing measures aimed at ensuring a high common level of security of the European Union **networks and information systems**.
    (NIS 2.0 in work, to expand the scope, add supply chain security…)
    - Obligation to report incidents and risks, to implements measure on request by ILR/CSSF
  - **2020:** a new **European cybersecurity strategy** setting **certification as a priority**
  - **Next: DORA (Digital Operational Resilience Act)** creates a regulatory framework on digital operational resilience whereby all firms need to make sure they can withstand, respond to and recover from all types of ICT-related disruptions and threats.
    - Exists as Project; similar penalties than for GDPR.

- **Cybersecurity act (CSA)**
  - **REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on**
    - ENISA (the European Union Agency for Cybersecurity) and
    - on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)

- **Article 1 Subject matter and scope**
  1. **ENISA**
  2. **a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services and ICT processes** in the Union, as well as for the purpose of avoiding the fragmentation of the internal market with regard to cybersecurity certification schemes in the Union.

- **Cybersecurity act (CSA)**
  - certification schemes in the Union.

Level	What is tested?	Objective	Minimum assesstment
High	Compliance and robustness	Preserving sovereignty, protecting the citizen and industry from criminal organizations	Pentesting State-of-the-Art attacks
Substantial	Compliance and robustness	Prevent scalable attacks on medium/high cost devices	Absence of public vulnerabilities Compliance testing
Basic	Compliance	Prevent massive attacks on low-cost devices	Technical documentation review Self-assessment



- **Trend:**
  - New ISO 15408... to be published v.soon
  - Focus here: Product certification

More compliance/certification needed to access EU markets

Supply chain attacks

- **Definition**
  - a (cyber-)attack that seeks to damage an organization by targeting less secure elements in the supply chain.
  - Cybercriminals typically tamper with the manufacturing or distribution of a product by installing malware or hardware-based spying components
- **Growth**
  - Symantec's 2019 Internet Security Threat Report states that supply chain attacks increased by 78 percent in 2018…
  - Supply chain cyberattacks jumped 51% in 2021 (Source: TechRepublic)
  - See Enisa monthly reports (not public, but green)

enisa

OSINT REPORT

Covering: 1 June – 7 June 2022 | TLP GREEN | Publication: June 7, 2022

Annual statistics:

DOMAIN	
FAR	59
GLOBAL	66
MID	47
NEAR	266

CATEGORY	
APT	45
Cyber-attack	191
Cybercrime	138
Cybersecurity	38
Cyberwarfare	14
Espionage	31
Geopolitics	61
Hacktivism	16
Poor security measures	7
Possible cyber-attack	14

SECTOR	
All Sectors	41
Arts sector	1
Construction industry	7
Critical Infrastructure	6
Education/Academic	15
Energy sector	21
Facility services	7
Finance sector / Banking	44
Food industry	11
General public	52
Healthcare/Medical	45
Industrial	19
Insurance	1
ISP	4
Legal	4
Mail/ Shipping services	4
Maritime sector	5
Media sector/ Entertainment industry	28
Military	14
Non-Government Organisations	7
Not enough information	3
Political organizations	5
Private sector	20
Public administration/Government	123
Religious organizations	2
Research	5
Retail/Commerce	14
Software supply chain	1
Space sector	3
Sports sector	1
Targeted individuals	23
Technological	34
Telecommunications	11
Transportation sector	17

TYPE	
Backdoor	13
Banking trojan	2
BGP hijack	2
Blackmail	1
Breach/Intrusion	75
Credential harvesting	2
Credential stuffing attack	1
Defacement	4
Domain hijacking	1
DoS/DDoS/RDoS	55
Exfiltration/ Data leakage/Breach	60
Exploitation	14
Fraud/Impersonation/Counterfeit	34
IoT botnet	6
Malware	71
Miner/Crypto	6
Misinformation/Disinformation	4
Multiple	7
Not enough information	45
Ransomware	113
RAT	6
Skimmers/Magecart	4
SMShing/Vishing	11
Social Engineering	7
Software supply chain	1
Spear phishing/Phishing	76
Spoofing	1
Spyware	8
Stealer	2
Trojan	4
Warning	35
Watering hole	2
Zero Day	6

Supply chain attacks

- **Examples**
  - **Compiler attack (2019): Corrupted Apple's XCode and Microsoft Visual Studio**
  - **Target (US retailor) (2013,$61 Mio loss, hacker entered through third-party access**
  - **STUXNET**
    - malicious computer worm entering over USB and modifying PLC to give unexpected command
    - believed to disturb the uranium enrichment programs in Iran.
  - **NotPetya (2017) targeted financial package in Ukraine via a provider**
  - **SolarWinds (2020):**
    - infiltrating the security and monitoring software ORION,
    - Victimes: Microsoft, National Nuclear Security Administration (NNSA), Department of Homeland Security, and ~30k customers worldwide
  - **Ransomware attacks combined to supply chain**
    - **on** Colonial pipeline (May 2021): Urgent US Act to ensure fuel transports, Biden warning Putin
    - thousands other companies targeted (1 July 2021)

Current solutions

- A set of Policy, Procedures, Excel tables to document compliance
  - To copy/paste, then tailor
- A risk assessment and treatment tool (TRICK service)
- A structured approach for audits and reviews
- Services:
  - Pentests…
  - Technical advice (crypto…)

New: IPCEI-CIS CyFORT

- CyFORT = Cloud Cybersecurity Fortress of Open Resources and Tools for Resilience
  - An new integrated 3-year EU project, similar to Gaia-X,
  - started with 6 people involved at itrust consulting
- Each of our Work packages creates an open-source or free-to-use tool:
  1. IDPS-ESCAPE: Tackling Supply Chain Attacks (on intrusion detection capabilities)
  2. SATRAP-DL: Enhancing threat intelligence
  3. C5-DEC: Common Criteria for Cybersecurity, Crypto, Clouds – Design Evaluation and Certification (on Requirement engineering and testing)
  4. DLT-PSaaS: Distributed Ledger Technology: Pseudonymization as a Service
  5. CS-GRAM: Cloud services – Governance, Risk management, Audit, and Monitoring
  6. PQC-MAT: Paving the way to a quantum-secure cloud-edge infrastructure
- During the project,
  1. integrate specific needs (TISAX, cloud regulation…)
  2. coach partners and interested parties (Focus on Energy and Industry) to use these tools.

Conclusion – Hints

1. **Be prepared to be attacked**
   - Not only your IT, but now also
   - your operation technology (OT).
2. **Invest in documentation/justification to demonstrate compliance (see penalties),**
3. **Follow technical vulnerabilities and patch (listen to your technical managers).**
4. **Get your (IT-OT-related) product certifiable/certified.**
5. **Prepare for more resilience in your supply chain contracts.**

itrust consulting

Move securely within the cyberworld

Move securely within the cyberworld

itrust consulting s.à r.l.
55, rue Gabriel Lippmann
L-6947 Niederanven

Tel: +352 26 176 212 6
Fax: +352 26 710 978
Web: www.itrust.lu

Carlo Harpes
harpes@itrust.lu