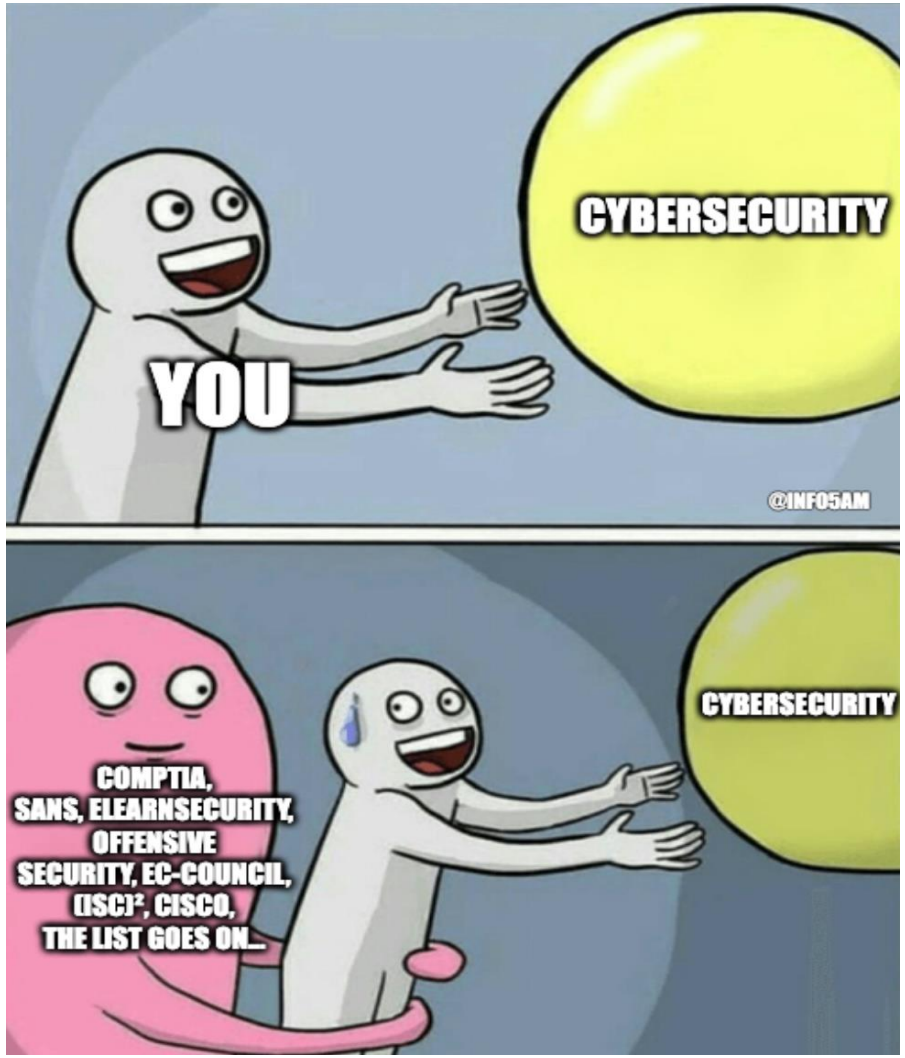
"Policies and regulations in cybersecurity"

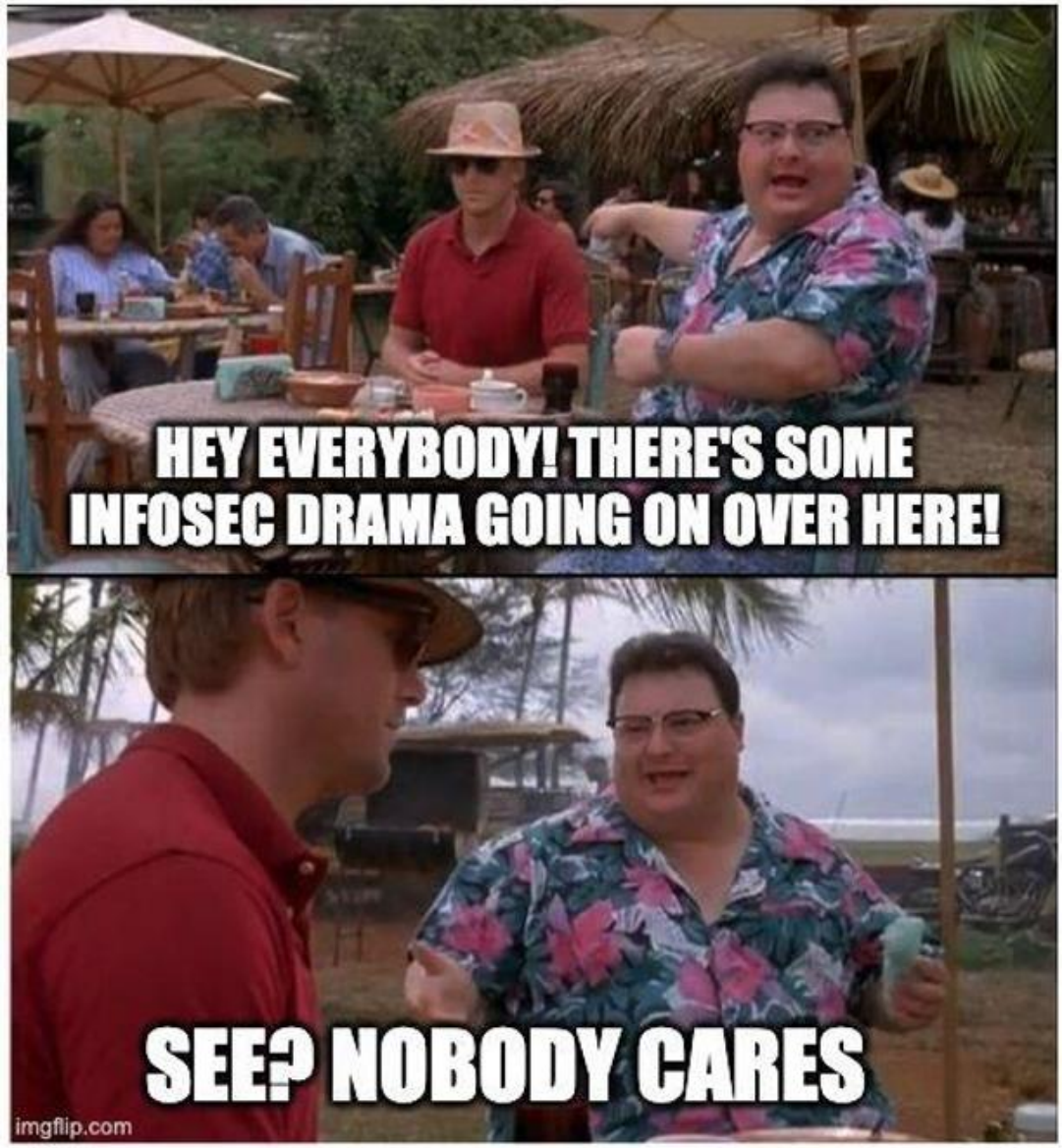
Politici și Reglementări în domeniul Securității Informației

Name: Elena Cristian, Vlad Belloiu
Business Generator S.R.L.
www.businessgenerator.ro
Email: office@businessgenerator.ro
Phone: +40720328424


CYBERSECURITY
YOU
@INFOSAM
CYBERSECURITY
COMPTIA,
SANS, ELEARNSECURITY,
OFFENSIVE
SECURITY, EC-COUNCIL,
(ISC)², CISCO,
THE LIST GOES ON...

AGENDA

- Context;
- Core-business analysis;
- Mapping the standards & regulations in Cybersecurity;
- Transition to the NIS 2 Directive.


HEY EVERYBODY! THERE'S SOME INFOSEC DRAMA GOING ON OVER HERE!
SEE? NOBODY CARES
imgflip.com

…*"nobody cares"* till it's too late

Updated September 2022 cyber news:

4.7 billion global internet users, 21 billion devices connected to the internet and a cyberattack happening every 40 seconds, 35.6 Million Records Breached and 88 publicly disclosed security incidents (big companies)

Recent cyber attacks & data breaches in 2022:

TikTok - Cyber Attack, NATO - Data Leak, Samsung - Exposed Personal Information, Uber - Systems Compromised, SpaceX Starlink - Hacked, Cisco - Cyber Attack, French Hospital - Cyber Attack, etc.

Common cybersecurity incidents:

data leaks, ransomware, phishing, insider threats, malwares, 0-day exploits etc.

Dilemmas in Cybersecurity and INFOSEC

- Challenges with regulations / frameworks
  - too many OR
  - none

- The defense complexity
  - the daily-increasing number of choices and options. It is not that we don't have good defense systems available, rather we have so many that we just couldn’t buy.
  - what data do we have to protect?

Our DATA

- data is the lifeblood of a business. Not only is there a high volume of information that an enterprise stores, but it is also of high value.

- bad actors find this an attractive opportunity and will be seeking ways to evolve their attack techniques in order to breach an organisations' systems.

- To combat these expanding attack surfaces, security teams need to think beyond the standard tools to do the job.

BUSINESS GENERATOR

Assess first.
Buy after.

- Organization's mission:
  - clarify the scope of the business;
  - what type of data to protect*(national/NATO/EU classified, critical infrastructure data, business related, personal);
  - asses the most suitable information security solution;

E.g. A National Agency which deals with classified information

- Compliance first with the national legislation and regulations;
- On top of that – implement a security/cybersecurity standard;

E.g. A company having business in healthcare or payment industry

- Compliant with business & personal related regulations (HIPAA / PCI DSS, GDPR).

Assess first.
Buy after.

Organization's budget

Key factor in choosing the best defense technology.

E.g.

Low-medium budget:

Use free cyber defense guidance (for instance: CIS Security Controls, NIST 800-53);

Implement manually;

Medium-large budget:

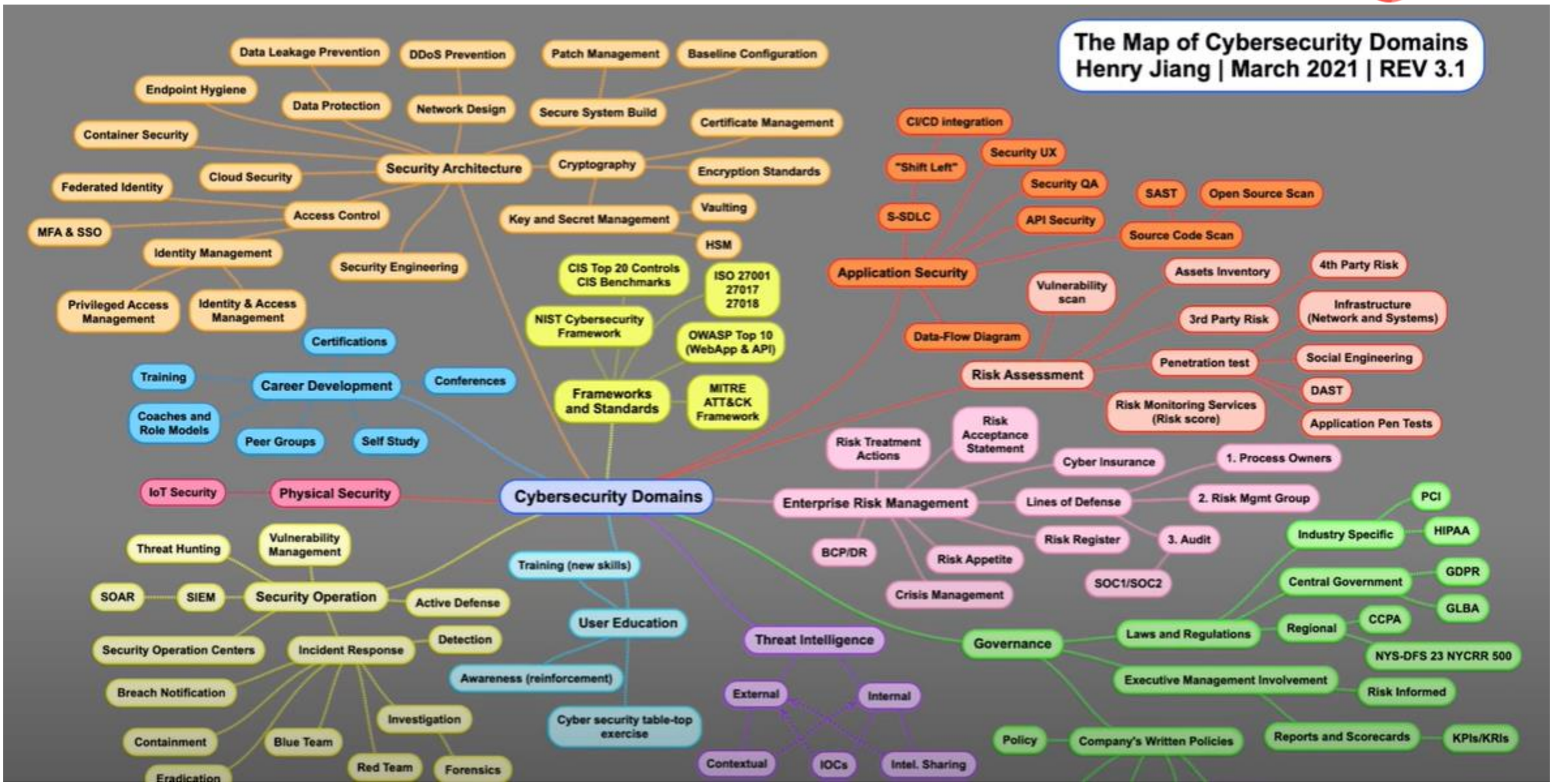
Use benchmarks;

Automatically verify the compliance of your policy with the desired frameworks & standards;

Information Security Frameworks

BUSINESS GENERATOR

- ISO 27000
- CIS Controls
- NIST Cybersecurity
- COBIT
- MITRE ATT&CK
- PCI DSS
- …


The Map of Cybersecurity Domains
Henry Jiang | March 2021 | REV 3.1
Cybersecurity Domains
Security Architecture
Data Leakage Prevention
DDoS Prevention
Patch Management
Baseline Configuration
Endpoint Hygiene
Data Protection
Network Design
Secure System Build
Certificate Management
Container Security
Cloud Security
Cryptography
Encryption Standards
Federated Identity
Access Control
Key and Secret Management
Vaulting
MFA & SSO
HSM
Identity Management
Security Engineering
Privileged Access Management
Identity & Access Management
Certifications
Career Development
Training
Conferences
Coaches and Role Models
Peer Groups
Self Study
Physical Security
IoT Security
Frameworks and Standards
CIS Top 20 Controls
CIS Benchmarks
ISO 27001
27017
27018
NIST Cybersecurity Framework
OWASP Top 10 (WebApp & API)
MITRE ATT&CK Framework
Application Security
CI/CD integration
Security UX
"Shift Left"
Security QA
S-SDLC
API Security
SAST
Open Source Scan
Source Code Scan
Vulnerability scan
Data-Flow Diagram
Risk Assessment
Assets Inventory
4th Party Risk
3rd Party Risk
Infrastructure (Network and Systems)
Penetration test
Social Engineering
DAST
Risk Monitoring Services (Risk score)
Application Pen Tests
Enterprise Risk Management
Risk Treatment Actions
Risk Acceptance Statement
Cyber Insurance
1. Process Owners
Lines of Defense
2. Risk Mgmt Group
Risk Register
3. Audit
BCP/DR
Risk Appetite
SOC1/SOC2
Crisis Management
Governance
Laws and Regulations
Industry Specific
PCI
HIPAA
Central Government
GDPR
GLBA
Regional
CCPA
NYS-DFS 23 NYCRR 500
Executive Management Involvement
Risk Informed
Reports and Scorecards
KPIs/KRIs
Policy
Company's Written Policies
Security Operation
Threat Hunting
Vulnerability Management
SOAR
SIEM
Active Defense
Security Operation Centers
Incident Response
Detection
Breach Notification
Investigation
Containment
Blue Team
Red Team
Forensics
Eradication
Training (new skills)
User Education
Awareness (reinforcement)
Cyber security table-top exercise
Threat Intelligence
External
Internal
Contextual
IOCs
Intel. Sharing

- Is a concept in security known as attack surface. Basically the more things you have exposed the more potential avenues there are into that device or in that technology.
- CIS benchmarks are consensus based best practices provided by volunteer community. Benchmarks are important because when folks download an application or install an O.S by default EVERYTHING is ON. Ports are open, application services are running.
- Benchmarks allow you to make sure that you have locked down those ports that are unnecessary and those applications that are unneeded that could provide an open vulnerability for an attacker to come in and take over a system.
- One of the things that makes benchmarks so important is that if you look at most any of the regulatory frameworks (whether it be PCI, HIPPA Sox, FedRAMP), they all insist that you are audited to show that you are in compliance with certain configuration checklists.
- Ways of become compliant with the Benchmarks: download the pdf manual and manually implement the configuration settings or becoming a security suite member (of a bechmarking service provider) and acces all the automated tools (remediation kits) that will help you to automatically implement he configurations.
- CIS provide the knowledge, the guidance and the tools to secure those systems.

CIS Controls:

- provide a prioritized path to improve an enterprise's cybersecurity program and to keep up with the ever-changing cyber ecosystem.
- the challenge with cybersecurity is the complexity, the number of choices and the number of options. Is not that we don't have good deffence, we have so many that we just couldn't buy.
- are based of understanding the attacker life cycle and then modeling deffence actions in order to better defend yourself against a cyber attack. Every organization whether it is small, medium or large enterprise should use the controls.
- hired to build a security program for an institution.
- prioritise set of actions to protect organizations against the best known attack vectors. Easy to implement and maintain and help you become more secure - that's the ultimate goal.
- translate the science into a relative number of rules that are positive constructive.

Mapping the standards & regulations

BUSINESS GENERATOR

E.g.

Mapping of the relationships between CIS Critical Security Controls and ISO 27001.

CIS Control	CIS Sub-Control	Title	Description	Relationship	ISO 27001 Objective Number	ISO 27001 Control Objective
1		**Inventory and Control of Hardware Assets** ***Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.***				
1	1,1	Utilize an Active Discovery Tool	Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.	small subset	A.8.1.1	Inventory of assets
1	1,2	Use a Passive Asset Discovery Tool	Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory.	small subset	A.8.1.1	Inventory of assets
1	1,3	Use DHCP Logging to Update Asset Inventory	Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory.	small subset	A.8.1.1	Inventory of assets
1	1,4	Maintain Detailed Asset Inventory	Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.	large subset	A.8.1.1	Inventory of assets
1	1,5	Maintain Asset Inventory Information	Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.	small subset	A.8.1.1	Inventory of assets
1	1,6	Address Unauthorized Assets	Ensure that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner.	small subset	A.11.2.5	Removal of assets
1	1,7	Deploy Port Level Access Control	Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.	small subset	A.13.1.1	Network Controls
				large subset	A.9.1.2	Access to networks and network services
1	1,8	Utilize Client Certificates to Authenticate Hardware Assets	Use client certificates to authenticate hardware assets connecting to the organization's trusted network.	small subset	A.9.3.1	Use of secret authentication information
1	1,8	Utilize Client Certificates to Authenticate Hardware Assets	Use client certificates to authenticate hardware assets connecting to the organization's trusted network.	small subset	A.13.1.1	Network Controls

The Network and Information Security (NIS) Directive

adopted in all 28 EU Member States, marks a major step in cybersecurity.
Is **the first cybersecurity law - 362/2018** which will have important, positive effects on the Operators of Essential Services.

Cover two type of companies:

operators in:
Energy sector;
Transportation sector;
Healthcare sector;
Distributors of drinking water.

digital service providers:
Cloud service providers;
Online search companies;
Online marketplaces.

What are the news in NIS 2 Directive

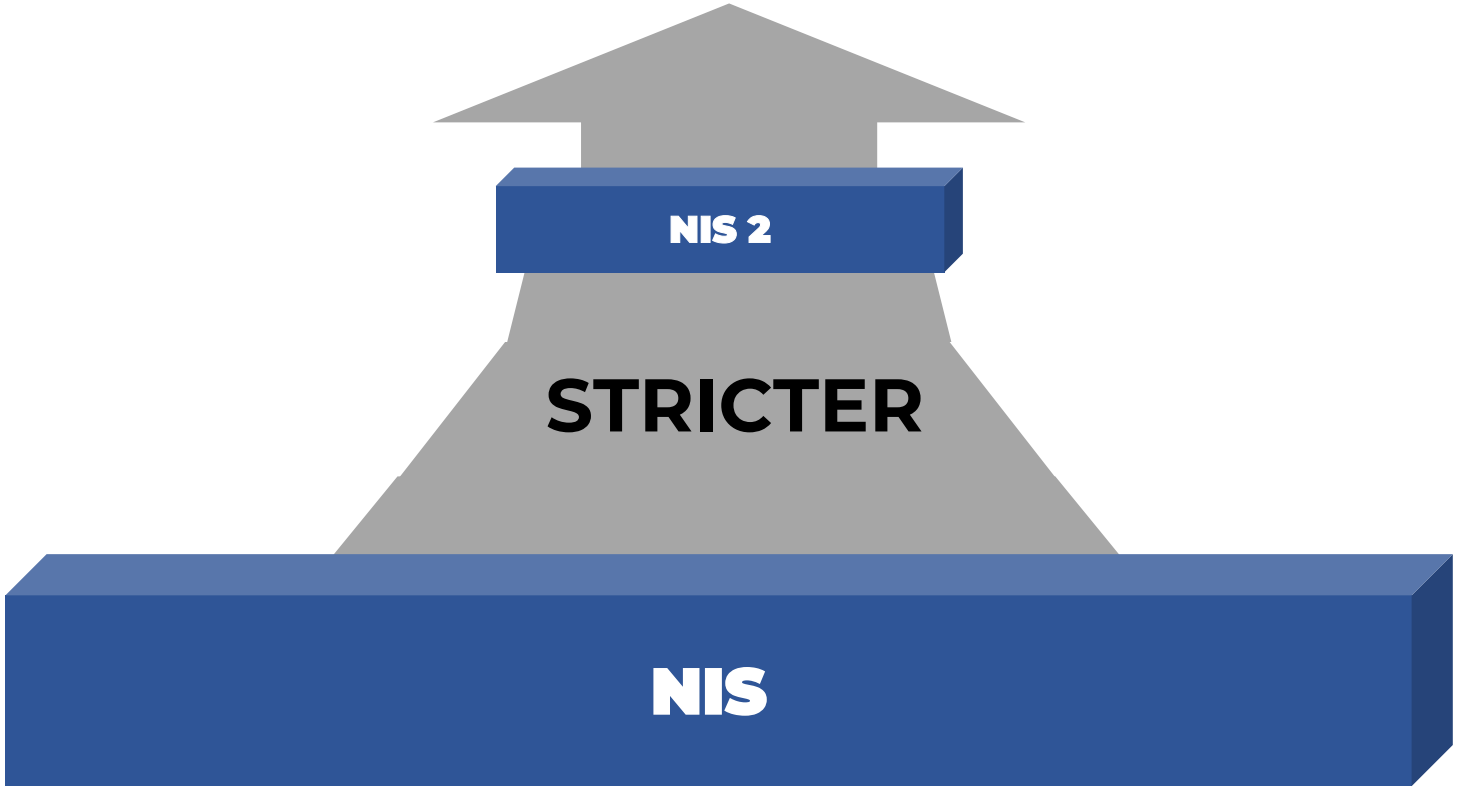
The proposal introduces more stringent supervisory measures for national authorities, stricter enforcement requirements and aims at harmonising sanctions regimes across Member States.

The proposal strengthens security requirements for the companies, by imposing a risk management approach providing a minimum list of basic security elements that have to be applied.

The proposal introduces more precise provisions on the process for incident reporting, content of the reports and timelines.

The proposal also eliminates the distinction between operators of essential services and digital service providers. Entities would be classified based on their importance, and divided respectively in essential and important categories with the consequence of being subjected to different supervisory regimes.

Transition to NIS 2



IMPROVEMENT POINTS

- ✓ Awareness
- ✓ Human Resource
- ✓ Buget

CONCLUSION
The main takeaway

- ✓ Any standard is better than nothing
- ✓ Start with what you have implemented already
- ✓ Map it in the right way
- ✓ Make the transition

BG is authorized by Romanian National Authority to perform security audit: (https://businessgenerator.ro/auditor-securitate-cibernetica/);

Authorized courses by the Romanian National Authority:

- GDPR/DPO (https://businessgenerator.ro/cursuri-acreditate/curs-responsabil-protectia-datelor-caracter-personal/);
- Information Security Manager (https://businessgenerator.ro/cursuri-acreditate/curs-manager-securitatea-informatiei/);

Specialized courses:

- Computer forensic; Malware analysis; NIS directive implementation;

Network and Information Security

https://businessgenerator.ro/cursuri-acreditate/curs-responsabil-nis-foundation/
https://businessgenerator.ro/cursuri-acreditate/curs-responsabil-nis-network-and-information-security-practitioner/

Multiple R&D areas: (https://businessgenerator.ro/domenii-cercetare/)

BUSINESS GENERATOR

THANK YOU!