Directive NIS2

Jacek Stańczyk
IBM Security
jacek.Stanczyk@pl.ibm.com
Tel. +48885673425

DIRECTIVE NIS2 changes in EU regulations - IBM POV

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022

on measures for a high common level of cybersecurity across the Union,

amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972,
and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

AMENDMENTS UNDER THE DIRECTIVE

- Increase the level of cyber security
- Reduce inconsistencies in cyber resilience
- Increase the level of shared situational awareness

SCOPE - NIS2

- Support in adapting the company to the new directive
- Assessing the company's cybersecurity readiness level
- Development of security policies
- CSIRT center management, construction and equipment
- Testing and training in crisis management technological support in NIS2 areas

NIS

NIS 2

Greater capabilities

EU Member States improve their cybersecurity capabilities.

More stringent supervision measures and enforcement are introduced.

A list of administrative sanctions, including fines for breach of the cybersecurity risk management and reporting obligations is established.

Cooperation

Increased EU-level cooperation.

Establishment of European Cyber crises liaison organisation network (EU- CyCLONe) to support coordinated management of large scale cybersecurity incidents and crises at EU level

Increased information sharing and cooperation between Member State authorities with enhanced role of the Cooperation Group.

Coordinated vulnerability disclosure for newly discovered vulnerabilities across the EU is established.

Cybersecurity risk management

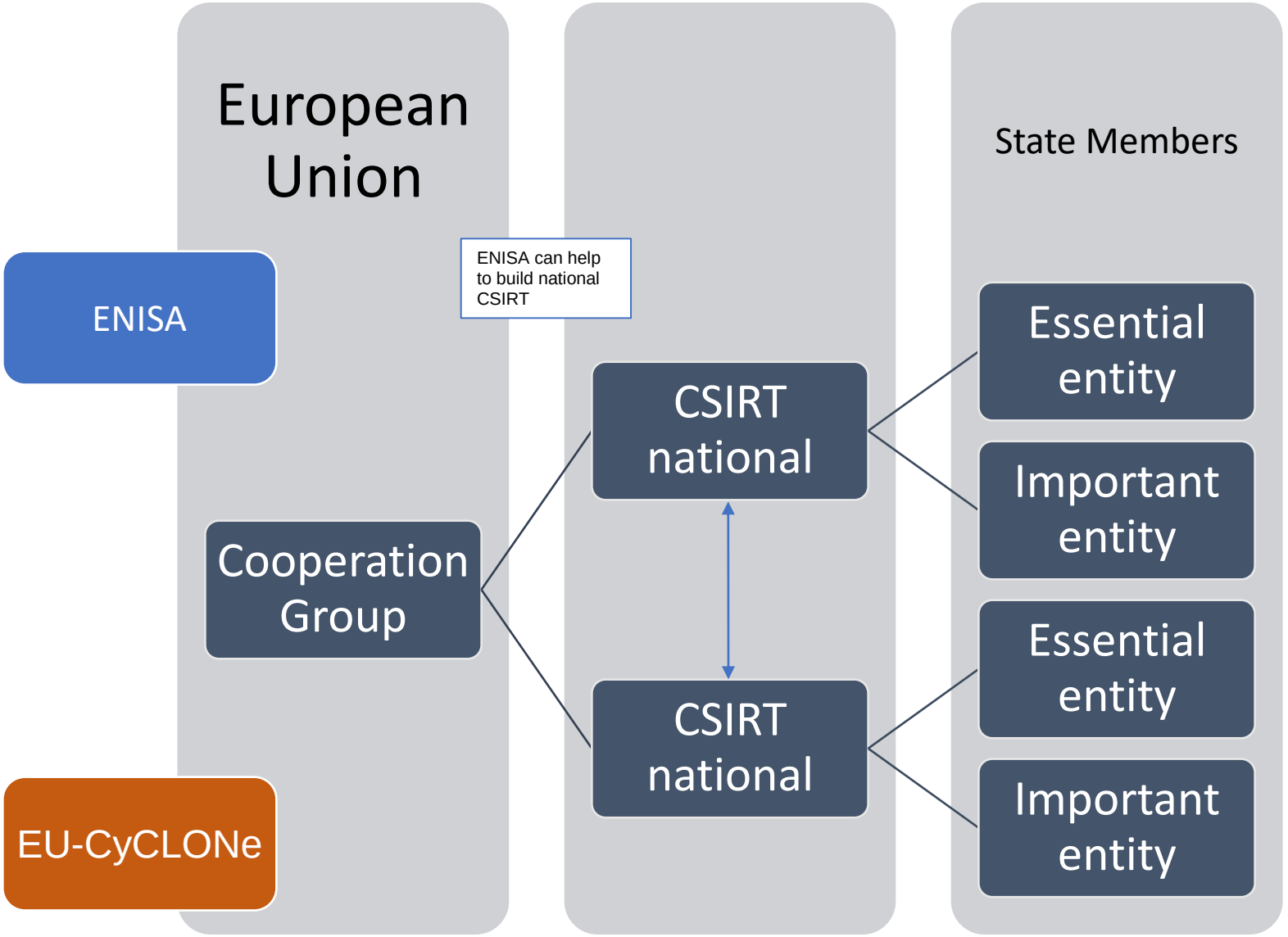
Operators of Essential Services (OES) and Digital Service Providers (DSP) have to adopt risk management practices and notify significant incidents to their national authorities.

Strengthened security requirements with a list of focused measures including incident response and crisis management, vulnerability handling and disclosure, cybersecurity testing, and the effective use of encryption.

Cybersecurity of supply chain for key information and communication technologies will be strengthened.

Accountability of the company management for compliance with cybersecurity risk-management measures.

Streamlined incident reporting obligations with more precise provisions on the reporting process, content and timeline.



Article 10

Entities under NIS1

Categories of OESs and DSPs	
OES	**DSPs**
• Energy (electricity, oil and gas) • Transport (air, rail, water and road) • Banking • Financial market infrastructures • Health • Drinking water supply and distribution • Digital infrastructure	• Online marketplaces • Online search engines • Cloud computing services

Essential entities - NIS2

- Energy
  - Electricity
  - District heating and cooling
  - Oil
  - Gas
  - Hydrogen
- Transport
  - Air
  - Rail
  - Water
  - Road

- Banking
- Financial market infrastructure
- Health
- Drinking water
- Wastewater
- Digital infrastructure
- Public administration
- Space

Important entities -NIS2

- Postal and courier
- Waste management
- Manufacture production and distribution of chemicals
- Food production and distribution
- Manufacturing
- Digital providers

- Manufacturing
  - Medical devices / diagnostic devices
  - Computer and electronics
  - Electrical equipment
  - Machinery and equipment (n.e.c.)
  - Motor vehicles, trailers
  - Other transport equipment

Penalties:

- maximum of at least
  - 10 000 000 EUR – essential entities
  - 7 000 000 EURO – important entities
- up to - of the total worldwide annual turnover
  - 2% - essential entities
  - 1.4%- important entities
- State Members can impose periodic penalty payments
- suspend a certification or authorization
- temporary ban against any **person** discharging managerial responsibilities at chief executive officer exercising managerial functions in that entity.
- **natural persons** may be held liable for breach of their duties

Article 34

Areas	**risk analysis** and information system **security policies**	**incident handling** (prevention, detection, and response to incidents)	**business continuity** and **crisis management**
supply chain security including security-related aspects concerning the for suppliers or service providers such as providers of data storage	**security in network** and **information systems** acquisition, development and maintenance, including vulnerability handling and disclosure	policies and procedures (testing and auditing) to assess the effectiveness of **cybersecurity risk management** measures	policies and procedures regarding the use of **cryptography** and, where appropriate, encryption;
basic cyber hygiene practices and **cybersecurity training**;	human resources **security, access control** policies and asset management;	the use of **multi-factor authentication** or continuous authentication solutions,	*Article 21*

IBM Offering:

Risk analysis and information system security policies

- Randori Recon (ASM)
- IBM Guardium Vulnerability assessment
- IBM Guardium Data Discover and Classification
- IBM QRadar UBA

- Business case/ output:

A fundamental challenge with data security is identifying who has access and what can they do. Enterprises need real-time activity monitoring for on-premises and cloud data sources, so mission-critical data remains protected.

- Strategy plan with security policies – Business Partner
- Milestones to grow security level - Business Partner

IBM Offering:

incident handling (prevention, detection, and response to incidents)

- IBM QRadar Suite
- IBM Security QRadar SIEM
- IBM Security QRadar SOAR
- IBM X-Force *
  - Pentest
  - Manage SOC
- IBM PL – Cyber Range mobileSOC

*- for enterpise customer

Business value/result:

"It's not the problem that matters, it's how you deal with it."

Solution Support:

- IBM SOC / SOC business partner
- IBM tactical cyber security training

IBM Offering:

business continuity and crisis management

- IBM QRadar SOAR
  - CSIRT Integration (automation, incident reporting system)
  - SOC >> CSIRT
- IBM Storage (safe guarded copies)
- IBM Cloud - backup

Business case/ output:

When it comes to cyber threats, you can't always predict when one will occur, but you can prepare. Responding to a cyber incident is a business-wide responsibility. Your entire organization should be prepared to react with speed, agility and a common purpose. Robust case management and tasks, your team can guide and execute investigation and response actions consistently, while benefiting from the streamlined automation of manual and repetitive tasks.

Solution support:

Test your organization and people's dexterity, capacity, capability and resilience against cyber hazards, threats and attacks and to effectively address any gaps and shortages.

IBM Offering:

supply chain security including security-related aspects concerning the relationships between each entity

- IBM Security Supply Chain Cyber Risk Management Services
- IBM Cloud Security - Dev/Sec/Ops

Business case/ output:

„A supply chain is only as strong as its most vulnerable entity. The Port of Los Angeles's Cyber Resilience Center will help each participating member of the supply chain to better protect themselves, and by extension each other."

Support SW supply chain

Deliver greater visibility across all supply chain activities. Gave near real-time visibility into operations, and the ability to take action earlier. Speedup onboarding process through an immutable record of new vendor details that business network participants can trust

Data protection

Data locality

Data visibility and governance

Fraud prevention

Third-party risk

IBM Offering:

security in network and information systems acquisition

- IBM CloudPak for Security
  - Qradar QNI, Forensic
  - IBM QRadar SOAR
  - OT/IoT security
  - IBM QRadar XDR
- MaaS360
- Randori (ASM)
- ReaQta (EDR)

Business case/ output:

Acquiring an information system therefore involves more than just obtaining and installing software. It involves incorporating the software into the current technological infrastructure and integrating the software into the data and procedures people use to make things happen in an organization.

Support

Phishing email and campaign detection
Insider threats
Lateral movement attack detection
Data exfiltration protection
Identify compliance gaps
Malware detection and analysis
OT-Security with AI/ML

*- for enterpise customer

IBM Offering:

policies and procedures (testing and auditing) to assess the effectiveness of **cybersecurity risk management** measures

- IBM QRadar SOAR
- IBM Open Pages (GRC)
- IBM Guardium Data Protection

Business case/ output:

Internal audits help organizations achieve corporate objectives by keeping a pulse on the consistency of internal business practices. The goal of an internal audit is to ensure organizational policies and procedures are followed and to alert the management of gaps in policy compliance

Dashboard, KPI’s,

IBM Cognos

IBM Offering:

the use of **cryptography and encryption**

- IBM Security Guardium
  - Data Encryption (GDE)
- IBM Cloud - Hyper Protect Crypto Services (Quantum Computing)
- Unified Key Orchestrator (multicloud)

Business case/ output:

Cryptography is one of the most important tools businesses use to secure the systems that hold its most important asset – data – whether it is at-rest or in-motion. Data is vital information in the form of customer PII, employee PII, intellectual property, business plans, and any other confidential information.

- Data encryption
- Cloud operations
- Future threats

IBM Offering:

basic cyber hygiene practices and **cybersecurity training**

- IBM xx – Cyber Range to create by local BP and IBM
- X-Force - Cyber Range*

Business case/ output:

Cyber Range solution creates immersive simulations to guide your team through realistic breach scenarios, helping ensure you can respond and recover from enterprise-level cyber security incidents and build a stronger security culture in your organization.

- Learn from industry best practices
- Incident response readiness
- Experience a simulated cyber incydent
- Sharpen collaboration across your organization

IBM Offering:

the use of **multi-factor authentication** or continuous authentication solutions,

- IBM Security Verify Trust (MFA)

Business case/ output:

IBM Verify supports two-step verification with accounts such as

- Amazon, Amazon Web Services,
- Bitbucket,
- Digital Ocean,
- Evernote,
- Github,
- Heroku,
- Hover,
- Intuit TurboTax,
- Joyent,
- LastPass,
- Rackspace,
- Salesforce,
- Slack,

and many more.

Solutions help you to detect fraud, authenticate users and establish identity trust across the omnichannel customer journey. Solutions uses cloud-based intelligence, AI and machine learning to holistically identify new and existing customers while improving the user experience

IBM Offering:

human resources security, **access control policies** and asset management;

- IBM IAM
- IBM Verify
- IBM Trusteer
- IBM Cognos

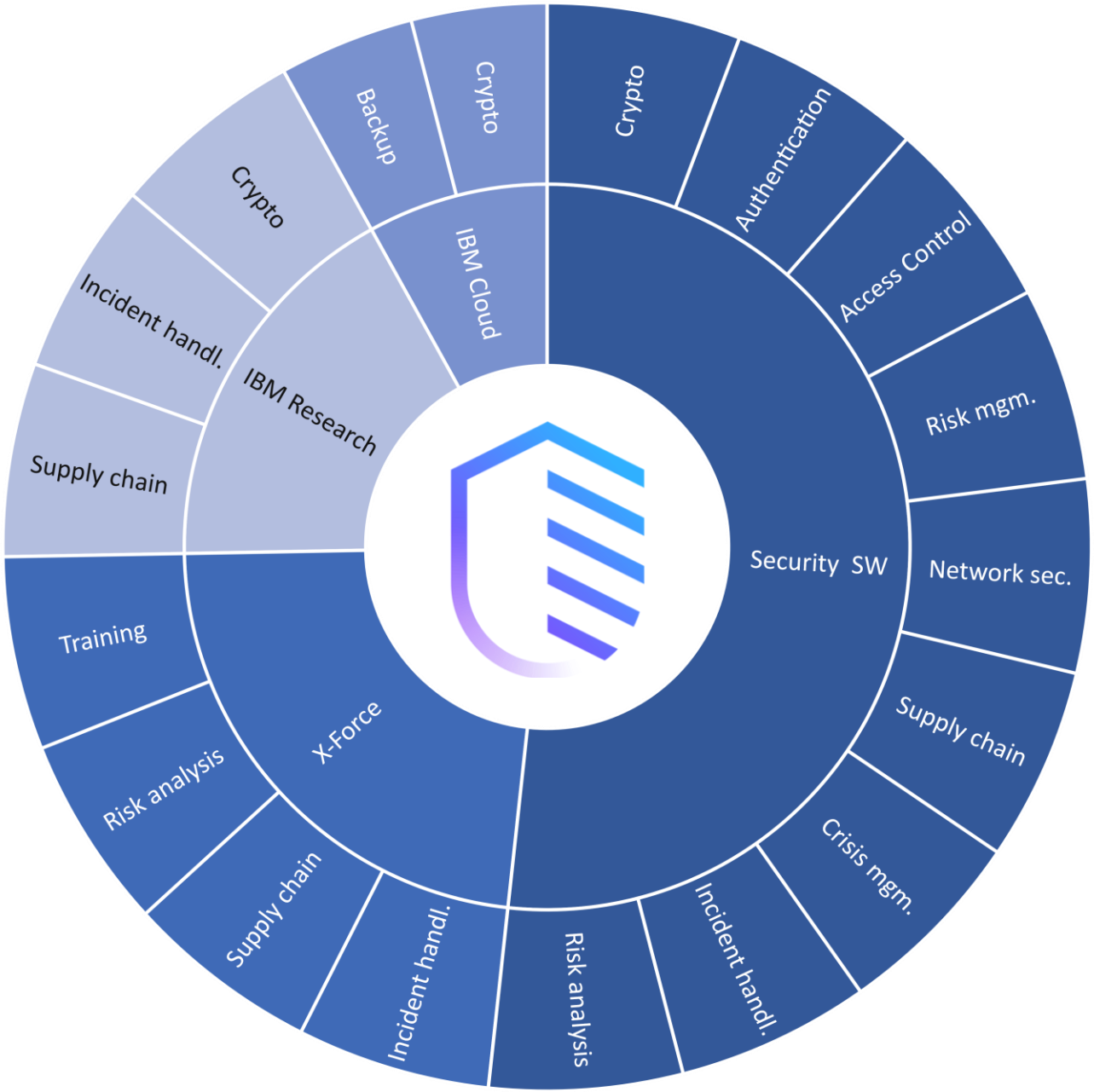
Business case/ output:

Internal audits help organizations achieve corporate objectives by keeping a pulse on the consistency of internal business practices. The goal of an internal audit is to ensure organizational policies and procedures are followed and to alert the management of gaps in policy compliance

Dashboard, KPI’s,

IBM Cognos

IBM Security – NIS2- POV



DIGITAL EUROPE PROGRAMME (DIGITAL) AN ORGANIZATION CAN GET FUNDING FOR THE FOLLOWING:

A budget of EUR 177 million for actions related to the “cyber-shield” announced in the EU Cybersecurity Strategy, including Security Operation Centres (SOC);

A budget of EUR 83 million for actions supporting the Implementation of relevant cybersecurity EU Legislation;

A budget of EUR 9 million for programme support actions, including evaluations and reviews.

Sources of financing

European Funds:

New Horizons

CEF - Connecting Europe

National:

- BGK - Infrastructure & Software
- FENG - Module digitalization
- FENIKS - Infrastructure transport –
- KPO – Pre financing
  - Increasing cybersecurity - innovative potential
  - e-commerce

Regional:

- Fundusze Europejskie dla Pomorza 2023
- Fundusze Europejskie dla Mazowsza 2027

More about founds: kalendarzdotacji.pl

Cooperation:

- IBM offer - SW / HW / Cloud
- BP offering - security status analysis (audit) / m-SOC services / implementation with analysis
- Marketing support - social media campaigns / telemarketing
- Technical support - participation of IBM engineers
- Client event - executive lunch for selected clients
- Planning and verification - monitoring of activities and progress