



# Identity Day

## NIS2 Overview

Steve Mowll – Sr. Director, Solution Engineering



# Everything you need to know about the upcoming NIS2 Directive



**2016**

**The NIS Directive  
was the first  
EU cybersecurity law**

# 2022 Why NIS2 you may ask?

# Why the NIS2 Directive?



Insufficient Levels  
of understanding  
and consistency



Lack of joint crisis  
response



Little common  
understanding of  
main threats

According to the European Commission, the annual cost of cybercrime to the global economy is estimated to have reached **what?** by the end of 2020?

Source: <https://digital-strategy.ec.europa.eu/en/library/cybersecure-digital-transformation-complex-threat-environment-brochure>

**5.500.000.000.000 Euros**

**What is the UK doing?**



# The UK NIS legislation?



Government is committed to improving NIS



Scope will expand to include managed services



Broader notification requirements for Essential and Digital services



# Who does it apply to?

Essential and Important entities

# Essential & Important entities

- Companies in Highly Critical and Critical sectors
  - (With some exceptions)
  - With more than 250 employees and turnover greater than 10M €
  - Headquartered in EU or operating in one or more member state(s)

\* Companies in "other critical sectors" can be considered Essential entities

Essential	Important*
High criticality sectors	Other critical sectors
Energy	Postal and courier services
Transport	Waste management
Banking	Manufacture, production and distribution of chemicals
Financial market infrastructures	Food production, processing and distribution
Health	Manufacture of medical devices; communication and optical equipment; electrical equipment; transport equipment)
Digital infrastructure	Digital providers (online marketplaces, search engines and social networks)
Water	Research organisations
Digital infrastructure	
ICT service management (B2B)	
Public administration	
Space	

# 10X affected companies

# Supervision

- Competent authorities can subject Essential entities to:
  - **Regular and targeted audits** (based on risk assessment) by independent body or authority.  
Paid by audited entity
  - Ad hoc audits\*
  - Security **scans**
  - Requests for information, including **cybersecurity policies**
  - Requests to **access data, documents**
  - Requests for evidence of implementation (e.g results of security audits)

# Enforcement

- Competent authorities **enforcement powers** related to essential entities:
  - Issue warning
  - Binding instructions to prevent or remedy incidents
  - Order entities to
    - cease non-compliant conduct
    - Comply with article 21 measures
    - Inform legal or natural persons using their services of the existence of a threat and provide instructions to protect or remediate against the threat
    - Implement recommendations from a security audit
    - **Make violations** to the directive **public**
    - Designate a monitoring officer for a determined period of time\*
  - Request administrative fine



# The cost of Non-Compliance

# The cost of Non-Compliance



NIS2 makes  
Senior Management  
responsible & liable



Fines – up to 2% Global  
Revenue, 10€



Further measures –  
Suspend services &  
Limit CEO Managerial  
functions





# Pillars of the NIS2 Directive

Recommended risk management measures

# Recommended Cybersecurity Risk Management Measures within NIS2 (Article 21)

Policies on risk analysis and information system security

Incident handling

Business continuity and crisis management

Supply chain security

Security in network and information systems acquisition, development and maintenance

Policies and procedures to assess effectiveness of cybersecurity risk-management measures

Basic cyber hygiene practices and cybersecurity training

Policies and procedures regarding use of cryptography and encryption

HR security, access control policies and asset management

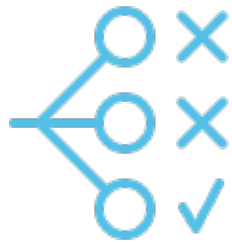
MFA, continuous authentication, and secure communications

# Recommended Cybersecurity Risk Management Measures within NIS2 (Article 21)

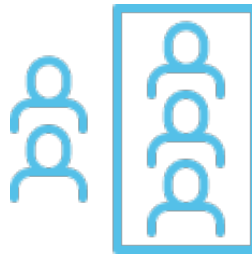


 = Identity Security related

## Art 21 – Policies on risk analysis and information system security



Zero Trust



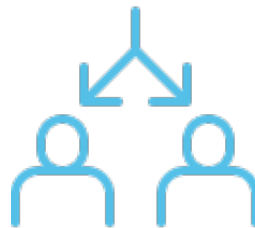
Least Privilege  
Access Model



Roles



Access  
Certifications



Separation of  
Duties



Detect Risky  
Identities

# Art 21 – Supply Chain Security

- Facts:
  - In 2022, supply chain attacks surpassed the number of malware-based attacks by 40%. Source <https://www.helpnetsecurity.com/2023/01/26/data-compromises-2022/>
  - Providing secure access for partners and contractors is the 2<sup>nd</sup> biggest identity and access challenge (41% of respondents to IDC's European Security Survey 2022)
- Examples of Supply chain attacks:
  - **Toyota:** In 2022, three separate suppliers were hacked, not the car manufacturer itself, but it had to stop 14 plants.
  - **Github:** In April 2022, GitHub's security team [revealed](#) a security incident, in which attackers stole OAuth user tokens issued to third-party integrators and leveraged them to download data from dozens GitHub's customers who had been using OAuth applications maintained by the vendors
- Effective governance of 3<sup>rd</sup> party identities is essential
  - Do you know who those individual are that have access to your systems and data?
  - Do you know if they still work for your supply chain partner?
  - Have contractors moved through your business acquiring access?

## Art 21 – Policies and procedures to assess the effectiveness of Cybersecurity risk management measures

- Identity Security is crucial to assess the risk posture related to identities and their accesses
- Assessing effectiveness of identity security measures and level of risk requires answers to these questions:
  - Do you have accounts with no **identified owner** in your Information system?
  - Do you have **generic accounts** used by different people to use applications or perform administrative tasks?
  - Do you have active accounts that have **not been used during the last 3 months**?
  - Do you have active **accounts that belong to people who stopped working** for your company?
  - Do you know who has **high privileges accounts** and what they can do with them?
  - Are some users **violating SOD policies** and putting your company at risk?
  - Are you implementing least privilege and regularly reviewing access?
  - Etc...

## Art 21 – HR security, access control policies and asset management

- An always accurate and reactive **user lifecycle management** is required for efficient and timely access control
- Identity Governance determines **who has access to what** based on policies (Roles)
- Access Management usually enforces these policies at the time of access.
- Access Reviews should be part of access control policy validation
- **Non-employee identities** are as important, however often not governed by a formal HR system and team, requiring additional attention.



# Conclusion

NIS2 in a nutshell



# The path to NIS2 Compliance

- Cybersecurity **training** for everyone!
- Implement **Least Privilege** and **Zero Trust** principles
- Privileged Access Management
- **Strong Authentication** mechanisms relying on **solid identity management**
- Manage **ALL identities**, employees as well as **non-employees**, ALL systems, ALL data

# NIS2 – In Summary


- Better alignment and collaboration across all members states
- 10x affected companies, 35 sectors of activity
- Now talking about **essential entities** (EEs) and **important entities** (IEs)
- NIS2 makes **senior management accountable** for the development and execution of an effective cyber security strategy.
- Like GDPR, NIS2 will be real and **non-compliance will be a serious business concern.**
- **SailPoint actively helps** to achieve NIS2 compliance in the areas of:
  - Policies on risk analysis and information system security
  - Supply chain security
  - Policies and procedures to assess effectiveness of cybersecurity risk-management measures
  - Basic cyber hygiene practices and cybersecurity training
  - HR security, access control policies and asset management

**You do not implement  
Identity Security  
overnight.  
Start now, be ready, be  
prepared!**

# The NIS2 Directive

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555>

An official website of the European UnionHow do you know?

EUR-Lex  
Access to European Union law

EnglishENMy EUR-Lex  
Experimental features

MENUSearch tips

QUICK SEARCH

Need more search options? Use the Advanced search

EUROPAEUR-Lex homeEUR-Lex - 32022L2555 - EN

Text

Document information

Procedure

Document summary

Save to My items

Up-to-date link

Permanent link

Download notice

Follow this document

Table of contents

Document 32022L2555

Share

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) (Text with EEA relevance)

PE/32/2022/REV/2

OJ L 333, 27.12.2022, p. 80–152 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)

In force

ELI: <http://data.europa.eu/eli/dir/2022/2555/oj>

Expand allCollapse all

Languages, formats and link to OJ

	BG	ES	CS	DA	DE	ET	EL	EN	FR	GA	HR	IT	LV	LT	HU	MT	NL	PL	PT	RO	SK	SL	FI	SV
HTML																								
PDF																								
Official Journal																								

To see if this document has been published in an e-OJ with legal value, click on the icon above (For OJs published before 1st July 2013, only the paper version has legal value).

Multilingual display

English (en)Please choosePlease chooseDisplay

Text

27.12.2022ENOfficial Journal of the European UnionL 333/80

**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)**  
**(Text with EEA relevance)**

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,  
Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,  
Having regard to the proposal from the European Commission,  
After transmission of the draft legislative act to the national parliaments,  
Having regard to the opinion of the European Central Bank <sup>(1)</sup>,  
Having regard to the opinion of the European Economic and Social Committee <sup>(2)</sup>,  
After consulting the Committee of the Regions,  
Acting in accordance with the ordinary legislative procedure <sup>(3)</sup>,  
Whereas:

© 2022 SailPoint Technologies, Inc. All Rights Reserved. 28

# 17th of October 2024

Due date for transposition into national legislation



**Thank You!**