NIS2 ONTOLOGY:
EXTENDING DPV

Jenni Parry

Wednesday – 1st May 2024

INTRODUCTION

- Jenni Parry, Associate Director, Cyber Risk, Aon
- Honours B.Sc. in Computer Science from University College Dublin (UCD)
- Currently pursuing a Master's degree in Cybersecurity
- Research Project Supervisor: Rob Brennan

Research Project Question:	Research Project Plan:
To what extent can compliance with NIS2 Cybersecurity risk-management measures (Article 21) be assessed via gap analysis by utilising the Data Protection Vocabulary (DPV), and therefore assist organisations in meeting the compliance with NIS2?	Develop a regulatory assessment tool that utilises a unified knowledge model for NIS2 compliance. Data Privacy Vocabulary (DPV) provides a comprehensive, standardized set of terms, this assessment tool will extend DPV and utilise it to perform a NIS2 gap analysis against ISO 27001:2022 framework.

This has led to a new ontology based on RDF/OWL. This ontology has a new set of terms for each ISO27001:2022 control relevant to NIS2 cybersecurity measures, these are called NIS2V Terms.

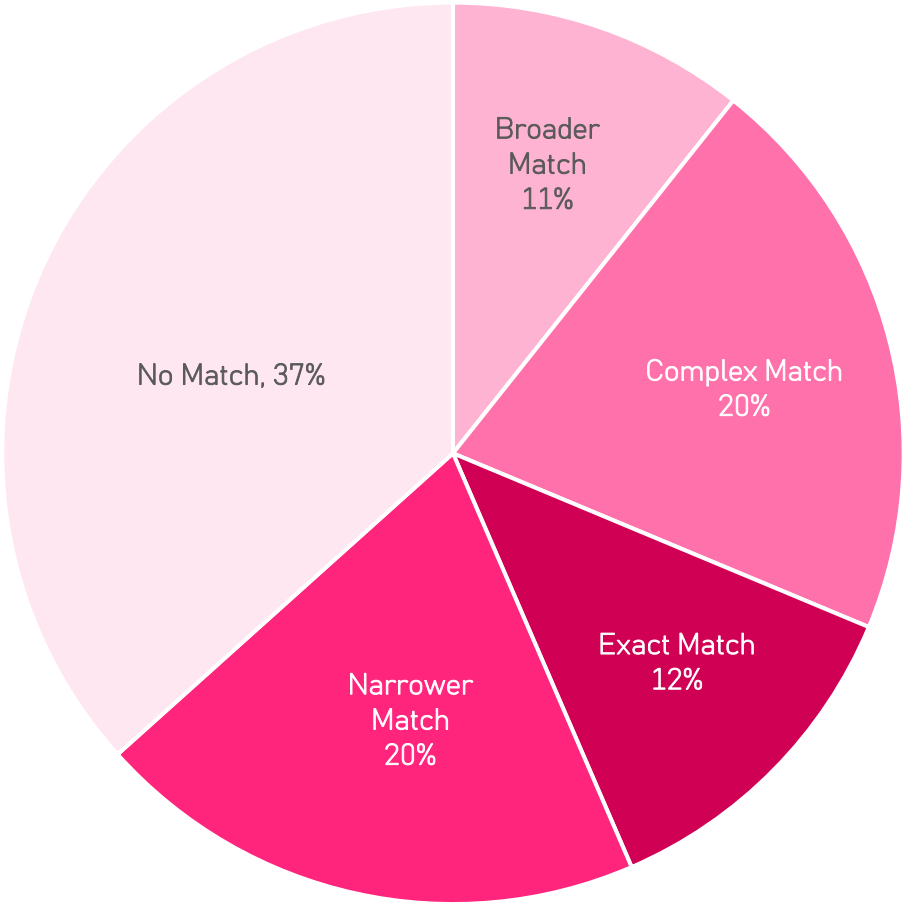
NIS2 CYBERSECURITY MEASURES

Cybersecurity Risk-Management Measures – Article 21			
(a)	Policies on risk analysis and information system security	(f)	Policies and procedures (including testing and auditing) to assess the effectiveness of cybersecurity risk management measures
(b)	Incident handling, such as the prevention, detection, and response to incidents	(g)	Basic cyber hygiene practices and cybersecurity training
(c)	Business continuity management, including backup management, crisis management and disaster recovery	(h)	Policies and procedures regarding the use of cryptography and, where appropriate, encryption
(d)	Supply chain security including security-related aspects concerning the relationships between each entity and its suppliers or service providers	(i)	Human resources security, access control policies and asset management
(e)	Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure	(j)	Multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate

METHODOLOGY

- Mapped NIS2 requirements against ISO 27001:2022 framework, using two sources:
  - NIS 2 Directive and ISO 27001:2022 (2.0 (extended) by Andrey Prozorov)
  - ENISA's Minimum Security Measures for Operators of Essential Services.
- This process was focused on the NIS2 cybersecurity risk-management measures (Article 21), aligning *101* ISO 27001 Controls (*89 unique*) and *30* ENISA Controls.
- Following this, the ISO 27001:2022 framework was mapped against DPV to define the common terminology.

DPV MAPPING & CHALLENGES



DPV Mapping Coverage	
ISO 27001:2022 Controls	101
Broader Match	14
Complex Match	26
Exact Match	14
Narrower Match	23
No Match	24
ENISA: Minimum Security Measures	30
Complex Match	1
Exact Match	2
Narrower Match	3
No Match	24

Challenges

- NIS2 Cybersecurity Risk-Management Measures wording is very high level, i.e. Basic cyber hygiene practices, this could be open to interpretation
- DPV is constantly expanding, with new terms being added regularly. Therefore, it's essential to ensure that these updates are reflected in the NIS2V vocabulary.
- ENISA: Minimum Security Measures for Essentials Services controls mapping had used the 2013 framework – this meant mapping to the 2022 version before assessing against DPV

APPENDIX

EXAMPLE TERMS: NIS2V TERMINOLOGY

Cybersecurity Measures	ISO Theme	ISO Control 27001:2022	Control Specification	NIS2V Term	Definition
Article 21.2 a) Policies on risk analysis and information system security	Organisational controls (Annex A)	A.5.7 Threat intelligence	Information relating to information security threats shall be collected and analysed to produce threat intelligence.	Threat Intelligence	Threat intelligence: Involves gathering and analysing information on potential cyber threats to help organisations pre-emptively identify and mitigate security risks.
Article 21.2 a) Policies on risk analysis and information system security	Organisational controls (Annex A)	A.5.37 Documented operating procedures	Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	Documented Operating Procedures	Documented Operating Procedures: Written instructions detailing the step-by-step processes and protocols to be followed in carrying out specific tasks or activities within an organisation.
Article 21.2 i) Human resources security, access control policies and asset management;	Organisational controls (Annex A)	A.5.3 Segregation of duties	Conflicting duties and conflicting areas of responsibility shall be segregated.	Segregation of Duties	Segregation of duties: A risk management practice that divides critical tasks among different people to prevent fraud and errors.
Article 21.2 i) Human resources security, access control policies and asset management;	Organisational controls (Annex A)	A.5.11 Return of assets	Personnel and other interested parties as appropriate shall return all the organisation's assets in their possession upon change or termination of their employment, contract or agreement	Return of Assets	Return of assets: The process of giving back property or resources to an organisation or individual after use or upon termination of employment or contract.

EXAMPLE TERMS: BROADER, COMPLEX & EXACT MATCHES

Cybersecurity Risk-Management Measures	ISO Theme	ISO Control 27001:2022	Control Specification	NIS2V Term	DPV Mapping Coverage	ISO - DPV Term Mapping #1	ISO - DPV Term Mapping #2
Article 21.2 j) The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communications systems within the entity, where appropriate	Technological controls (Annex A)	A.8.12 Data leakage prevention	Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.	Data Leakage Prevention	Broader Match	15.1.189 Data Security Management	
Article 21.2 i) Human resources security, access control policies and asset management;	Organisational controls (Annex A)	A.5.10 Acceptable use of information and other associated assets	Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.	Acceptable Use Policy	Complex Match	15.1.63 Code of Conduct	15.1.324 Information Security Policy
Article 21.2 i) Human resources security, access control policies and asset management;	Organisational controls (Annex A)	A.5.9 Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, shall be developed and maintained		Exact Match	15.1.31 Asset Management Procedures	