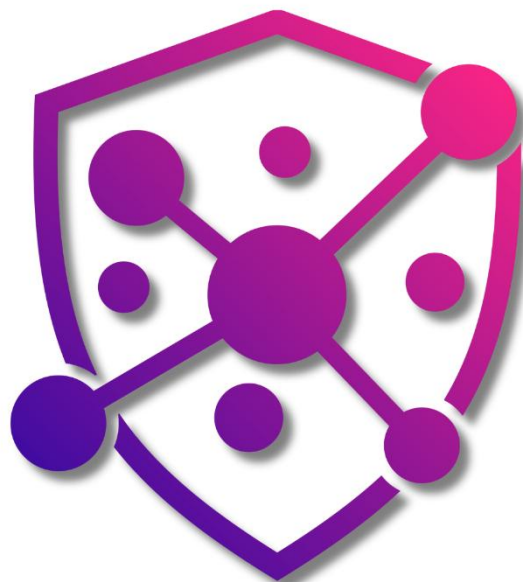


CURIMUM **CONTINUUM**



D P M A Digital Product Maturity Assessment

Step-by-Step User Manual

Purpose of the DPMA Tool

The Digital Product Maturity Assessment (DPMA) Tool is designed to support SMEs, micro-enterprises and start-ups in identifying relevant cybersecurity measures for digital products in a simple and practical way.

The tool provides access to a consolidated and structured dataset of cybersecurity measures, aligned with the Cyber Resilience Act (CRA) and widely adopted standards such as ISO 27001, ISO 27002, NIST 800-53, CIS V8 Controls and others.

Instead of consulting multiple standards or regulatory documents, users can search, filter, and explore cybersecurity measures and understand their maturity level, scope, and threat coverage.

The DPMA Tool helps organizations:

- understand the level of security afforded by the measures already implemented,
- identify further measures that could be implemented to cover a specific threat and
- gradually progress towards CRA readiness.

Intended Users

The DPMA Tool is intended for:

- Small and Medium-sized Enterprises (SMEs),
- micro-enterprises and start-ups,
- product managers and technical leads,
- non-expert users involved in product development, maintenance, or compliance planning.

No advanced cybersecurity or regulatory expertise is required to use the tool.

Accessing the Tool

Open a web browser (e.g. Chrome, Firefox, Edge).

Navigate to: <https://app.apiroservicestool.info>

No installation or local configuration is required.

Practical Use of the DPMA Tool

The DPMA Tool is designed to be:

- simple to use,
- transparent,
- and reusable over time.

Users may return to the tool whenever:

- the product evolves,
- new cybersecurity threats arise,
- they require an alteration of the measures already implemented or the level of security needs to change.

By combining free-text search, filtering and maturity-based structuring, the DPMA Tool enables SMEs to engage with cybersecurity requirements in a practical and accessible manner.

Main Interface Overview

The main screen consists of:

- a free-text search bar at the top,
- a Search button,
- Export CSV and Export Excel buttons,
- and a table displaying available cybersecurity measures.

At the top of the screen, the user can see:

- the number of results displayed,
- and a notification when the number of results exceeds a predefined threshold (no more than 30 results can be previewed on the screen).
- Each row in the table corresponds to one cybersecurity measure, while columns provide structured contextual information.

Excel Data

Search term1 AND/OR term2

Showing 30 of 1556 rows

Over 30 results — refine your search.

#	Category description	Description of Measures	Level	Numbering per par	Paragraph	Parent Clause or control	Secondary	Source	Threats	Unique Identifier
	Filter Category description	Filter Description of Measures	Filter Level	Filter Numbering	Filter Paragraph	Filter Parent Clause	Filter Secondary	Filter Source	Filter Threats	Filter Unique Identifier
1	Nonconformity and corrective action	Corrective actions shall be appropriate to the effects of the nonconformities encountered. The organization shall retain documented	1	1	10.1	10.1		27001	Malfeasance (exceeding authorizations) - acquiring the use of a system in excess of that which has been authorized, Improper / Inadequate Procedure - foreseeable events not supported by complete and accurate documentation and training, Cyberstalking, Back door/trap door, Communications Error - a communications facility that provides inaccurate	10.1ID.1
2	Nonconformity and corrective action	The reaction to the nonconformity should be based on a defined handling process. The process should include: — identifying the	2	2	10.1	10.1		27003	Malfeasance (exceeding authorizations) - acquiring the use of a system in excess of that which has been authorized, Improper / Inadequate Procedure - foreseeable events not supported by complete and accurate documentation and training, Cyberstalking, Back door/trap door, Communications Error - a communications facility that provides inaccurate	10.1ID.2
3	Nonconformity and corrective action	Corrective actions can occur after, or in parallel with, corrections. The following process steps should be taken: 1. decide if there is a need to	2	3	10.1	10.1		27003	Malfeasance (exceeding authorizations) - acquiring the use of a system in excess of that which has been authorized, Improper / Inadequate Procedure - foreseeable events not supported by complete and accurate documentation and training, Cyberstalking, Back door/trap door, Communications Error - a communications facility that provides inaccurate	10.1ID.3
4	Nonconformity and corrective action	Some organizations maintain registers for tracking nonconformities and corrective actions. There can be more than one register (for	3	4	10.1	10.1		27003	Malfeasance (exceeding authorizations) - acquiring the use of a system in excess of that which has been authorized, Improper / Inadequate Procedure - foreseeable events not supported by complete and accurate documentation and training, Cyberstalking, Back door/trap door, Communications Error - a communications facility that provides inaccurate	10.1ID.4
5	Continual improvement	The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.	1	1	10.2	10.2		27001	Acts of war (conventional), Improper / Inadequate Procedure - foreseeable events not supported by complete and accurate documentation and training	10.2 ID.1
6	Continual improvement	The assessment can also include an analysis of the efficiency of the ISMS and its elements, considering if their use of resources is	3	2	10.2	10.2		27003	Acts of war (conventional), Improper / Inadequate Procedure - foreseeable events not supported by complete and accurate documentation and training	10.2 ID.2
7	Continual improvement	Improvement opportunities can also be identified when managing nonconformities and corrective actions. Once opportunities for	3	3	10.2	10.2		27003	Acts of war (conventional), Improper / Inadequate Procedure - foreseeable events not supported by complete and accurate documentation and training	10.2 ID.3
8	Understanding the	The organization shall determine external and internal issues that are relevant to its purpose	1	1	4.1	4.1		27001	Misuse of audit tools, Loss of support services, Liability for employee actions, Insider trading, Disaster (human caused), Personnel Unavailability, - inability to contact operations or support personnel, Negligence, Theft, Embarrassment,	4.1 ID.1

Figure 1- DPMA main interface displaying the searchable dataset of cybersecurity measures

Searching for Cybersecurity Measures

Free-Text Search

The DPMA Tool allows users to search across all available fields using the search bar.

Users may:

- enter a single keyword (e.g. malware),
- combining keywords using AND / OR logic (e.g. malware AND risk),
- or search using broader terms related to cybersecurity, threats, or compliance.

After entering the desired terms, the user clicks Search to display results.

If the number of returned results exceeds the system limit, a message is displayed advising the user to refine the search. (no more than 30 results can be previewed on the screen).

Excel Data

malware

Showing 30 of 1556 rows

Over 30 results — refine your search.

#	Category description	Description of Measures	Level	Numbering per par	Paragraph	Parent Clause or control	Secondary	Source	Threats	Unique Identifier
	Filter Category	Filter Description of Measures	Filter	Filter Number	Filter Paragraph	Filter Parent	Filter Secondary	Filter Source	Filter Threats	Filter Unique
1	address risks and opportunities	The organization shall retain documented	1	10	6.1	6.1		27001	network by unauthorized persons, Malware , Spillage / Droppage - hazardous materials permitted near equipment (e.g. food, liquids), Cyberstalking, Man-in-the-middle spoofing, Electrical Noise / Bad Ground - suggested by flickering	6.1ID.10
2	Actions to address risks and opportunities	options, taking account of the risk assessment results;	1	11	6.1	6.1		27001	network by unauthorized persons, Malware , Spillage / Droppage - hazardous materials permitted near equipment (e.g. food, liquids), Cyberstalking, Man-in-the-middle spoofing, Electrical Noise / Bad Ground - suggested by flickering	6.1ID.11
3	Actions to address risks and opportunities	information security risk treatment option(s) chosen;	1	12	6.1	6.1		27001	network by unauthorized persons, Malware , Spillage / Droppage - hazardous materials permitted near equipment (e.g. food, liquids), Cyberstalking, Man-in-the-middle spoofing, Electrical Noise / Bad Ground - suggested by flickering	6.1ID.12
4	Actions to address risks and opportunities	The organization shall define and apply an	1	13	6.1	6.1		27001	network by unauthorized persons, Malware , Spillage / Droppage - hazardous materials permitted near equipment (e.g. food, liquids), Cyberstalking, Man-in-the-middle spoofing, Electrical Noise / Bad Ground - suggested by flickering	6.1ID.13

Figure 2 - Example of free-text search using keywords

The results can be exported in .csv and .xlsx formats. The exported information is restricted to the ones fulfilling the criteria mentioned above. The same constraints (regarding the number of results) apply.

Excel Data

malware and risk

Showing 30 of 1556 rows

Over 30 results — refine your search.

#	Category description	Description of Measures	Level	Numbering per par	Paragraph	Parent Clause or control	Secondary	Source	Threats	Unique Identifier
	Filter Category	Filter Description of Measures	Filter	Filter Number	Filter Paragraph	Filter Parent	Filter Secondary	Filter Source	Filter Threats	Filter Unique
1	address risks and opportunities	The organization shall retain documented	1	10	6.1	6.1		27001	network by unauthorized persons, Malware , Spillage / Droppage - hazardous materials permitted near equipment (e.g. food, liquids), Cyberstalking, Man-in-the-middle spoofing, Electrical Noise / Bad Ground - suggested by flickering	6.1ID.10
2	address risks and opportunities	The organization shall define and apply an	1	11	6.1	6.1		27001	network by unauthorized persons, Malware , Spillage / Droppage - hazardous materials permitted near equipment (e.g. food, liquids), Cyberstalking, Man-in-the-middle spoofing, Electrical Noise / Bad Ground - suggested by flickering	6.1ID.11
3	address risks and opportunities	The organization shall define and apply an	1	12	6.1	6.1		27001	Zero day attacks, Insufficient support by the Top Management to the Management System, Poor quality of the risk assessment process. Risks have not been identified or the results are not fully reliable, Misuse of audit tools,	6.1ID.12
4	address risks and opportunities	The organization shall define and apply an	1	13	6.1	6.1		27001	Zero day attacks, Insufficient support by the Top Management to the Management System, Poor quality of the risk assessment process. Risks have not been identified or the results are not fully reliable, Misuse of audit tools,	6.1ID.13

Figure 3 - Example of free-text search using keywords and AND/OR logic.

Refining Results with Column Filters

Below each column header, a column-specific filter field is available.

These filters can be used independently or in combination with the free-text search.

Users can refine results by:

- Category description (e.g. Controls against malware),
- Description of Measures (searching within measure text),
- Level of security,
- Source (e.g. ISO/IEC 27001, ISO/IEC 27002),
- Threats

This enables narrowing results even when starting from a broad search term.

Excel Data

malware and risk

Showing 27 of 1556 rows

#	Category description	Description of Measures	Level	Numbering per par	Paragraph	Parent Clause or control	Secondary	Source	Threats	Unique Identifier
	Filter Category	Filter Description of Mea	Filter	Filter Number	Filter Parag	Filter Pe	Filter Secon	27003	Filter Threats	Filter Uniq
1	address risks and	Opportunities that fall into this category can be opportunities	4	18	6.1	6.1		27003	network by unauthorized persons, Malware , Spillage / Droppage - hazardous materials permitted near equipment (e.g. food, liquids), Cyberstalking, Man-in-the-middle spoofing, Electrical Noise / Bad Ground - suggested by flickering	6.1D.18
2	address risks and	the organization defines and applies complete and	4	19	6.1	6.1		27003	network by unauthorized persons, Malware , Spillage / Droppage - hazardous materials permitted near equipment (e.g. food, liquids), Cyberstalking, Man-in-the-middle spoofing, Electrical Noise / Bad Ground - suggested by flickering	6.1D.19
3	address risks and	The actions required in 6.1.1 can be different for	5	20	6.1	6.1		27003	Zero day attacks, Insufficient support by the Top Management to the Management System, Poor quality of the risk assessment process. Risks have not been identified or the results are not fully reliable, Misuse of audit	6.1D.20

malware and risk

Showing 17 of 1556 rows

#	Category description	Description of Measures	Level	Numbering per par	Paragraph	Parent Clause or control	Secondary	Source	Threats	Unique Identifier
	actions	Filter Description of Mea	Filter	Filter Number	Filter Parag	Filter Pe	Filter Secon	27003	Filter Threats	Filter Uniq
1	Actions to address	Opportunities that fall into this category can be	4	18	6.1	6.1		27003	network by unauthorized persons, Malware , Spillage / Droppage - hazardous materials permitted near equipment (e.g. food, liquids), Cyberstalking, Man-in-the-middle spoofing, Electrical Noise / Bad Ground - suggested by flickering	6.1D.18
2	Actions to address	the organization defines and applies complete and	4	19	6.1	6.1		27003	network by unauthorized persons, Malware , Spillage / Droppage - hazardous materials permitted near equipment (e.g. food, liquids), Cyberstalking, Man-in-the-middle spoofing, Electrical Noise / Bad Ground - suggested by flickering	6.1D.19
3	Actions to address	The actions required in 6.1.1 can be different for	5	20	6.1	6.1		27003	plant, tank farm, munitions depot, Smokes, Vibration - nearby railroad track, jet traffic, construction site, illegal infiltration, Malicious code, Access to the network by unauthorized persons, Malware , Spillage / Droppage - hazardous	6.1D.20

Figure 4 - Examples of free-text search using filters

Understanding the Results Table

Each cybersecurity measure is presented with structured metadata to support interpretation and traceability.

Key columns include:

- **Category description (Broad & Sub-category)**
Indicates the thematic area of the measure.
- **Description of Measures**
A plain-language description explaining what the measure addresses.
- **Level**
Represents the level of security achieved / afforded by the measure.
Lower levels generally correspond to foundational practices, while higher levels indicate more advanced cybersecurity level.
- **Source**
Shows the originating standard (e.g. ISO 27001, ISO 27002).
- **Threats**
Lists the types of threats that the measure aims to address, such as malware, unauthorized access, procedural weaknesses or operational failures.

Users may scroll horizontally and vertically to explore the full set of information.

Exporting Results

Once relevant measures have been identified, users may export results for offline use (maximum 30 results).

Available options:

- Export CSV
- Export Excel

Category description	Category_New	Description of Measures	Level	Paragraph	Parent Clause or control	Source	Threats	Unique Identifier
Protection against malware	Protection against malware	Protection against malware should be 0	A.8.7	8.7		ISO 27002:2022	Corporate crime, Tr A.8.7.ID.1	
Protection against malware	Protection against malware	Use of malware detection and repair :0	A.8.7	8.7		ISO 27002:2022	Corporate crime, Tr A.8.7.ID.2	
Protection against malware	Protection against malware	The following guidance should be con 0	A.8.7	8.7		ISO 27002:2022	Corporate crime, Tr A.8.7.ID.3	
8.7	Protection against malware	Protection against malware	1	A.8.7	A.8.7	ISO 27001	Corporate crime, Tr A.8.7.ID.1	
Controls against malware	Controls against malware	the scan carried out should include: 1 2	A.8.7	A.12.2		ISO 27002:2013	Corporate crime, Tr A.12.2.ID.10	
Controls against malware	Controls against malware	g) installation and regular update of r 2	A.8.7	A.12.2		ISO 27002:2013	Corporate crime, Tr A.12.2.ID.9	
Controls against malware	Controls against malware	PR.AT-1: All users are informed and tr 2	A.8.7	A.12.2		NIST	Corporate crime, Tr A.12.2.ID.26	
Controls against malware	Controls against malware	the scan carried out should include: 2 3	A.8.7	A.12.2		ISO 27002:2013	Corporate crime, Tr A.12.2.ID.11	
Controls against malware	Controls against malware	the scan carried out should include: 2 3	A.8.7	A.12.2		ISO 27002:2013	Corporate crime, Tr A.12.2.ID.12	
Controls against malware	Controls against malware	a) establishing a formal policy prohibi 3	A.8.7	A.12.2		ISO 27002:2013	Corporate crime, Tr A.12.2.ID.2	
Controls against malware	Controls against malware	b) implementing controls that preven 3	A.8.7	A.12.2		ISO 27002:2013	Corporate crime, Tr A.12.2.ID.4	
Controls against malware	Controls against malware	c) implementing controls that preven 3	A.8.7	A.12.2		ISO 27002:2013	Corporate crime, Tr A.12.2.ID.5	
Controls against malware	Controls against malware	Ensure that the organization's anti-mi 3	A.8.7	A.12.2		CIS	Corporate crime, Tr A.12.2.ID.23	
Controls against malware	Controls against malware	Configure devices so that they automi 3	A.8.7	A.12.2		CIS	Corporate crime, Tr A.12.2.ID.24	
Controls against malware	Controls against malware	Communicate policy prohibiting the u 3	A.8.7	A.12.2		custom	Corporate crime, Tr A.12.2.ID.3	
Controls against malware	Controls against malware	h) defining procedures and responsibi 4	A.8.7	A.12.2		ISO 27002:2013	Corporate crime, Tr A.12.2.ID.13	
Controls against malware	Controls against malware	j) implementing procedures to regulai 4	A.8.7	A.12.2		ISO 27002:2013	Corporate crime, Tr A.12.2.ID.15	
Controls against malware	Controls against malware	d) establishing a formal policy to prot 4	A.8.7	A.12.2		ISO 27002:2013	Corporate crime, Tr A.12.2.ID.6	
Controls against malware	Controls against malware	e) reducing vulnerabilities that could 14	A.8.7	A.12.2		ISO 27002:2013	Corporate crime, Tr A.12.2.ID.7	
Controls against malware	Controls against malware	Utilize centrally managed anti-malwa 4	A.8.7	A.12.2		CIS	Corporate crime, Tr A.12.2.ID.22	
Controls against malware	Controls against malware	Configure devices to not auto-run con 4	A.8.7	A.12.2		CIS	Corporate crime, Tr A.12.2.ID.25	
Controls against malware	Controls against malware	Malware protection software should 14	A.8.7	A.12.2		custom	Corporate crime, Tr A.12.2.ID.19	
Controls against malware	Controls against malware	Malware protection software adminis 4	A.8.7	A.12.2		custom	Corporate crime, Tr A.12.2.ID.20	
Controls against malware	Controls against malware	The malware protection mechanisms 4	A.8.7	A.12.2		ENISA	Corporate crime, Tr A.12.2.ID.30	
Controls against malware	Controls against malware	PR.DS-6: Integrity checking mechanis 4	A.8.7	A.12.2		NIST	Corporate crime, Tr A.12.2.ID.27	
Controls against malware	Controls against malware	i) preparing appropriate business conti 5	A.8.7	A.12.2		ISO 27002:2013	Corporate crime, Tr A.12.2.ID.14	
Controls against malware	Controls against malware	k) implementing procedures to verify 5	A.8.7	A.12.2		ISO 27002:2013	Corporate crime, Tr A.12.2.ID.16	
Controls against malware	Controls against malware	l) isolating environments where catas 5	A.8.7	A.12.2		ISO 27002:2013	Corporate crime, Tr A.12.2.ID.17	
Controls against malware	Controls against malware	The use of two or more software proc 5	A.8.7	A.12.2		ISO 27002:2013	Corporate crime, Tr A.12.2.ID.18	
Controls against malware	Controls against malware	f) conducting regular reviews of the si 5	A.8.7	A.12.2		ISO 27002:2013	Corporate crime, Tr A.12.2.ID.8	

Figure 5 – Export in excel format

Category description	Category	New	Description of Measures	Level	Paragraph	Parent Clause or control	Source	Threats	Unique Identifier
Protection against malware	Protection against malware	Protection against malware	Use of malware detection and repair software alone is not usually adequate.	0	A.8.7.8.7	ISO 27002:2022	Corporate crime, Trojan, Malicious Software - software whose purpose is to degrade system performance, modify or destroy data, steal resources or subvert security in any manner, Malicious code		
Protection against malware	Protection against malware	The following guidance should be considered:							
a)	Implementing rules and controls that prevent or detect the use of unauthorized software [e.g. application allowlisting (i.e. using a list providing allowed applications)]								
b)	Implementing controls that prevent or detect the use of known or suspected malicious websites [e.g. blocklisting]								
c)	reducing vulnerabilities that can be exploited by malware [e.g. through technical vulnerability management]								
d)	conducting investigations of the presence of any unapproved files or unauthorized amendments								
e)	establishing								
f)	installing and regularly updating malware detection and repair software to scan computers and electronic storage media. Carrying out regular scans that include:								
1)	scanning any data received over networks or via any form of electronic storage media, for malware before use								
2)	scanning email and instant messaging attachments and downloads for malware before use. Carrying out this scan at different places (e.g. at email servers, desktop computers) and when entering the network of the organization								
3)	scanning webpages for malware when accessed								
g)	determining the placement and configuration of malware detection and repair tools based on risk assessment outcomes and considering:								
1)	defence in depth principles where they would be most effective. For example, this can lead to malware detection in a network gateway (in various application protocols such as email, file transfer and web) as well as user endpoint devices								
2)	the evasive techniques of attackers (e.g. the use of encrypted files) to deliver malware or the use of encryption protocols to transmit malware								
h)	taking care to protect against the introduction of malware during maintenance and emergency procedures, which can bypass normal controls against malware								
i)	implementing a process to authorize temporarily or permanently disable some or all measures against malware, including exception approval authorities, documented justification and review date. This can be necessary when the protection is required								
j)	preparing appropriate business continuity plans for recovering from malware attacks, including all necessary data and software backup (including both online and offline backup) and recovery measures								
k)	isolating environments where catastrophic consequences can occur								
l)	defining procedures and responsibilities to deal with protection against malware on systems, including training in their use, reporting and recovering from malware attacks								
m)	providing								
n)	implementing procedures to regularly collect information about new malware, such as subscribing to mailing lists or reviewing relevant websites								
o)	verifying that information relating to malware, such as warning bulletins, comes from qualified and reputable sources (e.g. reliable internet sites or suppliers of malware detection software) and is accurate and informative.	0	A.8.7.8.7	ISC					
8.7	Protection against malware	Protection against malware	1, A.8.7.8.7, ISO 27001, Corporate crime, Trojan, Malicious Software - software whose purpose is to degrade system performance, modify or destroy data, steal resources or subvert security in any manner, Malicious code						
Controls ag	2, A.8.7.8.7, ISO 27002:2013, Corporate crime, Trojan, Malicious Software - software whose purpose is to degrade system performance, modify or destroy data, steal resources or subvert security in any manner, Malicious code								
Controls ag	2, A.8.7.8.7, ISO 27002:2013, Corporate crime, Trojan, Malicious Software - software whose purpose is to degrade system performance, modify or destroy data, steal resources or subvert security in any manner, Malicious code								
Controls against malware	Controls against malware, PR-AT-1: All users are informed and trained	2, A.8.7.8.7, ISO 27002:2013, Corporate crime, Trojan, Malicious Software - software whose purpose is to degrade system performance, modify or destroy data, steal resources or subvert security in any manner, Malicious code							
Controls ag this scan s	3, A.8.7.8.7, ISO 27002:2013, Corporate crime, Trojan, Malicious Software - software whose purpose is to degrade system performance, modify or destroy data, steal resources or subvert security in any manner, Malicious code								
Controls ag	3, A.8.7.8.7, ISO 27002:2013, Corporate crime, Trojan, Malicious Software - software whose purpose is to degrade system performance, modify or destroy data, steal resources or subvert security in any manner, Malicious code								
Controls ag	3, A.8.7.8.7, ISO 27002:2013, Corporate crime, Trojan, Malicious Software - software whose purpose is to degrade system performance, modify or destroy data, steal resources or subvert security in any manner, Malicious code								
Controls ag	3, A.8.7.8.7, ISO 27002:2013, Corporate crime, Trojan, Malicious Software - software whose purpose is to degrade system performance, modify or destroy data, steal resources or subvert security in any manner, Malicious code								
Controls ag	3, A.8.7.8.7, ISO 27002:2013, Corporate crime, Trojan, Malicious Software - software whose purpose is to degrade system performance, modify or destroy data, steal resources or subvert security in any manner, Malicious code								

Figure 6 – Export in CSV format

Example Use Cases

Use Case 1: Identifying malware-related cybersecurity measures

Context

An SME wants to identify controls related to malware protection.

How the DPMA Tool is used

The user searches with keyword malware.

Outcome

Relevant measures are identified across different maturity levels, supporting informed prioritization.

Use Case 2: Identifying the level of security afforded by different measures

Context

A product team wants to focus on measures addressing event logging affording a specific level of security (e.g. 2).

How the DPMA Tool is used

The user enters event logging in the search bar, and 2 in the filter of the Level.

Outcome

A small, targeted set of relevant cybersecurity measures is identified for further review.

Use Case 3: Identifying the level of security by implemented measures

Context

A product team wants to see at which level a specific measure resides.

How the DPMA Tool is used

The user enters the specific measure in the filter of the corresponding column.

Outcome

The level of security of the measure is identified by reading the filtered line.