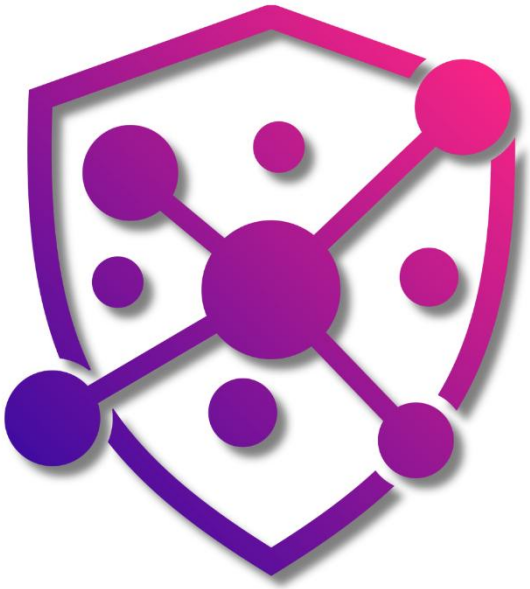
CONTINUUM



DPMA

Digital Product Maturity Assessment

Step-by-Step User Manual

The CURIUM project is supported by the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) under Grant Agreement No. 101190372. Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the ECCC

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.

The CURIUM project is supported by the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) under Grant Agreement No. 101190372. Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the ECCC

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.

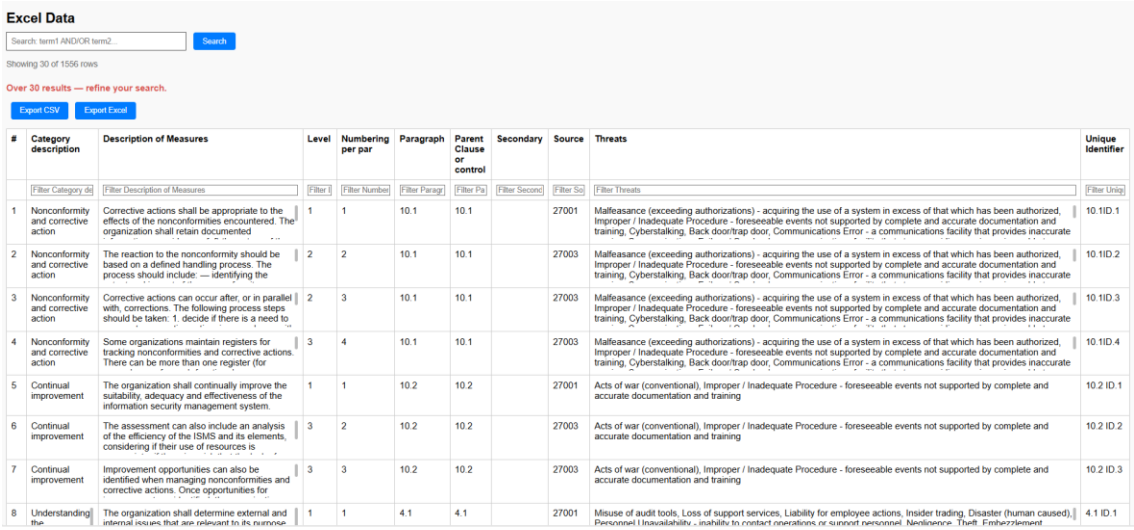


Figure 1- DPMA main interface displaying the searchable dataset of cybersecurity measures

The CURIUM project is supported by the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) under Grant Agreement No. 101190372. Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the ECCC

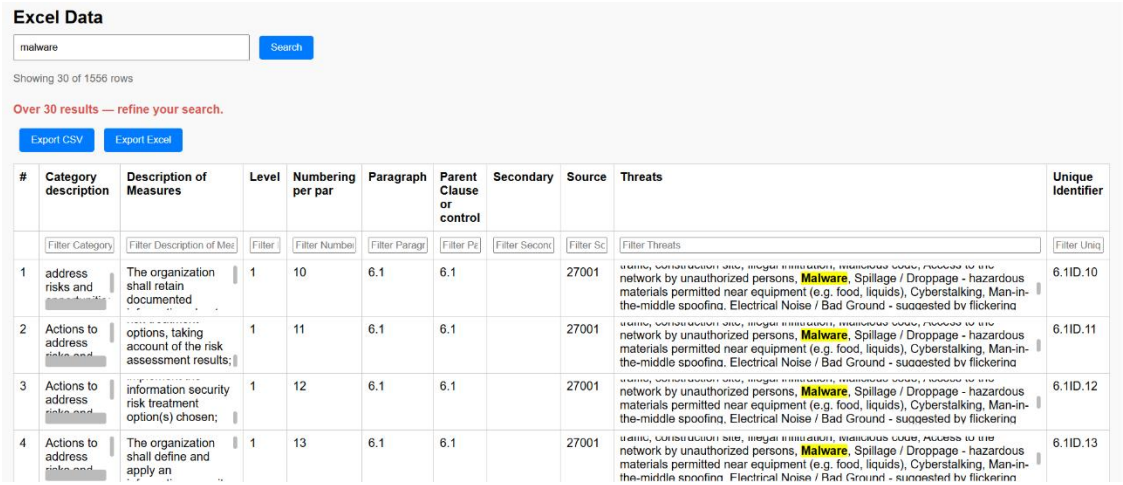
Searching for Cybersecurity Measures

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.

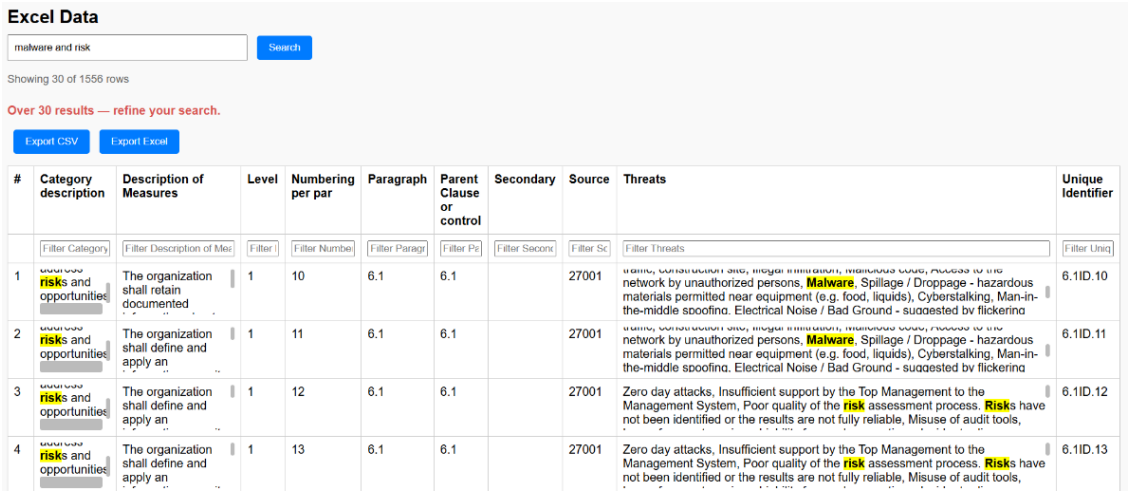
After entering the desired terms, the user clicks Search to display results.
If the number of returned results exceeds the system limit, a message is displayed advising the user to refine the search. (no more than 30 results can be previewed on the screen).



#	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 Numbe	Filter Paragr	Filter Pa	Filter Secon	Filter Sc	Filter Threats	Filter Uniq
1	address risks and	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	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	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	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.



#	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 Numbe	Filter Paragr	Filter Pa	Filter Secon	Filter Sc	Filter Threats	Filter Uniq
1	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	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	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	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.

The CURIUM project is supported by the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) under Grant Agreement No. 101190372. Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the ECCC

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.

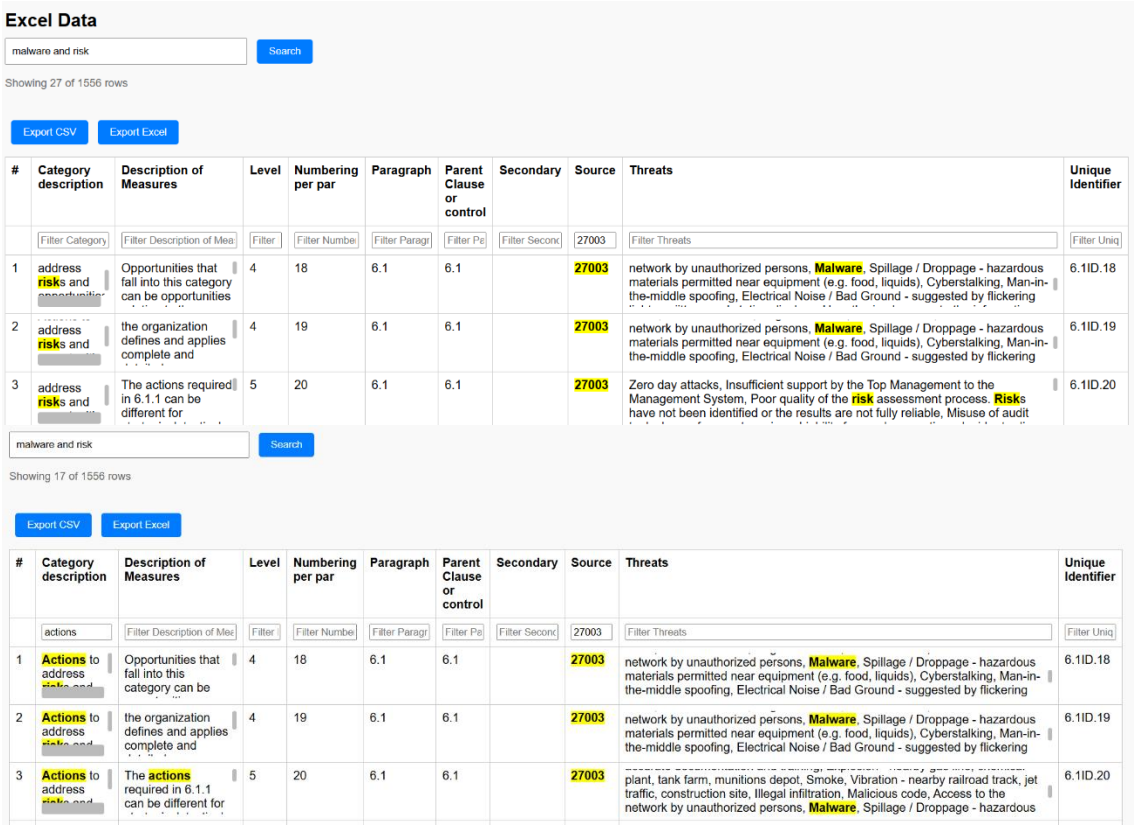


Figure 4 - Examples of free-text search using filters

The CURIUM project is supported by the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) under Grant Agreement No. 101190372. Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the ECCC

Understanding the Results Table

Each cybersecurity measure is presented with structured metadata to support interpretation and traceability.
Key columns include:

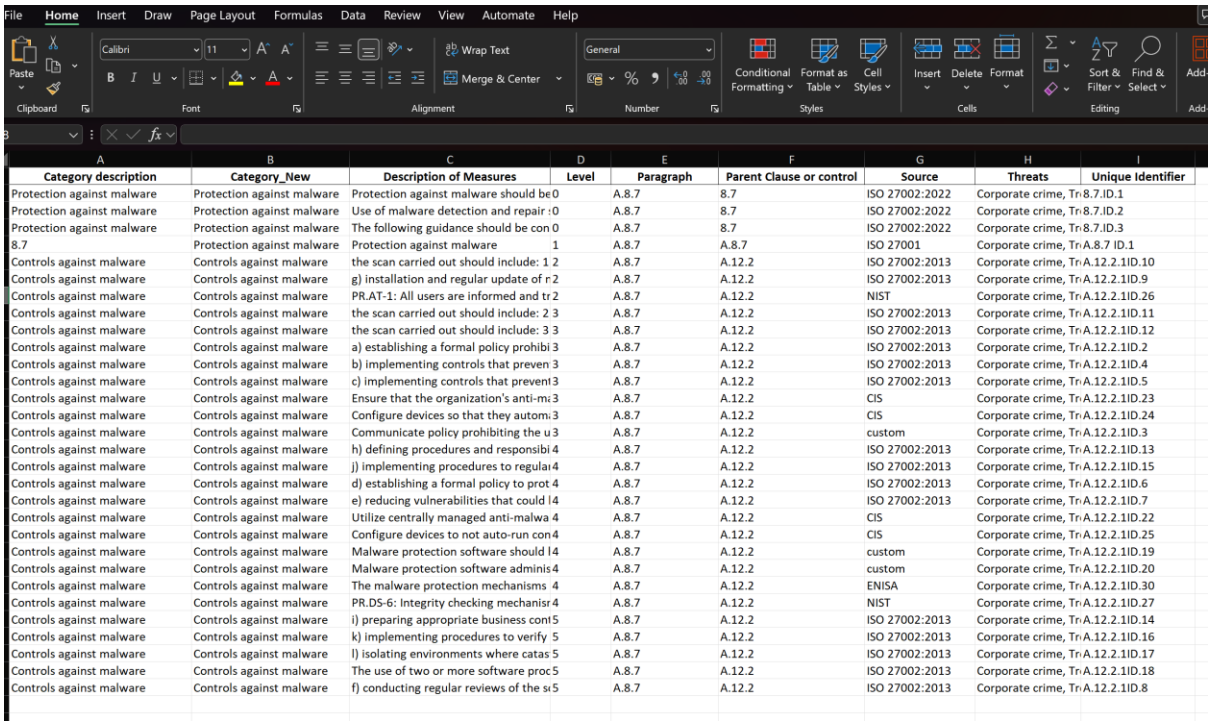
- **Category description (Broad & Sub-category)**
  Indicates the thematic area of the measure.
- **Description of Measures**
  A plain-language description explaining what the measure addresses.
- **Level**
  Represents the level of security achieved / afforded by the measure.
  Lower levels generally 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	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	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	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.12.2.1ID.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.12.2.1ID.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.12.2.1ID.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.12.2.1ID.11
Controls against malware	Controls against malware	the scan carried out should include: 3	3	A.8.7	A.12.2	ISO 27002:2013	Corporate crime, Tr	A.12.2.1ID.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.12.2.1ID.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.12.2.1ID.4
Controls against malware	Controls against malware	c) implementing controls that prevent	3	A.8.7	A.12.2	ISO 27002:2013	Corporate crime, Tr	A.12.2.1ID.5
Controls against malware	Controls against malware	Ensure that the organization's anti-ma	3	A.8.7	A.12.2	CIS	Corporate crime, Tr	A.12.2.1ID.23
Controls against malware	Controls against malware	Configure devices so that they autom	3	A.8.7	A.12.2	CIS	Corporate crime, Tr	A.12.2.1ID.24
Controls against malware	Controls against malware	Communicate policy prohibiting the u	3	A.8.7	A.12.2	custom	Corporate crime, Tr	A.12.2.1ID.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.12.2.1ID.13
Controls against malware	Controls against malware	j) implementing procedures to regulat	4	A.8.7	A.12.2	ISO 27002:2013	Corporate crime, Tr	A.12.2.1ID.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.12.2.1ID.6
Controls against malware	Controls against malware	e) reducing vulnerabilities that could l	4	A.8.7	A.12.2	ISO 27002:2013	Corporate crime, Tr	A.12.2.1ID.7
Controls against malware	Controls against malware	Utilize centrally managed anti-malwa	4	A.8.7	A.12.2	CIS	Corporate crime, Tr	A.12.2.1ID.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.12.2.1ID.25
Controls against malware	Controls against malware	Malware protection software should l	4	A.8.7	A.12.2	custom	Corporate crime, Tr	A.12.2.1ID.19
Controls against malware	Controls against malware	Malware protection software adminis	4	A.8.7	A.12.2	custom	Corporate crime, Tr	A.12.2.1ID.20
Controls against malware	Controls against malware	The malware protection mechanisms	4	A.8.7	A.12.2	ENISA	Corporate crime, Tr	A.12.2.1ID.30
Controls against malware	Controls against malware	PR.DS-6: Integrity checking mechanisr	4	A.8.7	A.12.2	NIST	Corporate crime, Tr	A.12.2.1ID.27
Controls against malware	Controls against malware	i) preparing appropriate business cont	5	A.8.7	A.12.2	ISO 27002:2013	Corporate crime, Tr	A.12.2.1ID.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.12.2.1ID.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.12.2.1ID.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.12.2.1ID.18
Controls against malware	Controls against malware	f) conducting regular reviews of the s	5	A.8.7	A.12.2	ISO 27002:2013	Corporate crime, Tr	A.12.2.1ID.8

Figure 5 – Export in excel format

The CURIUM project is supported by the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) under Grant Agreement No. 101190372. Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the ECCC

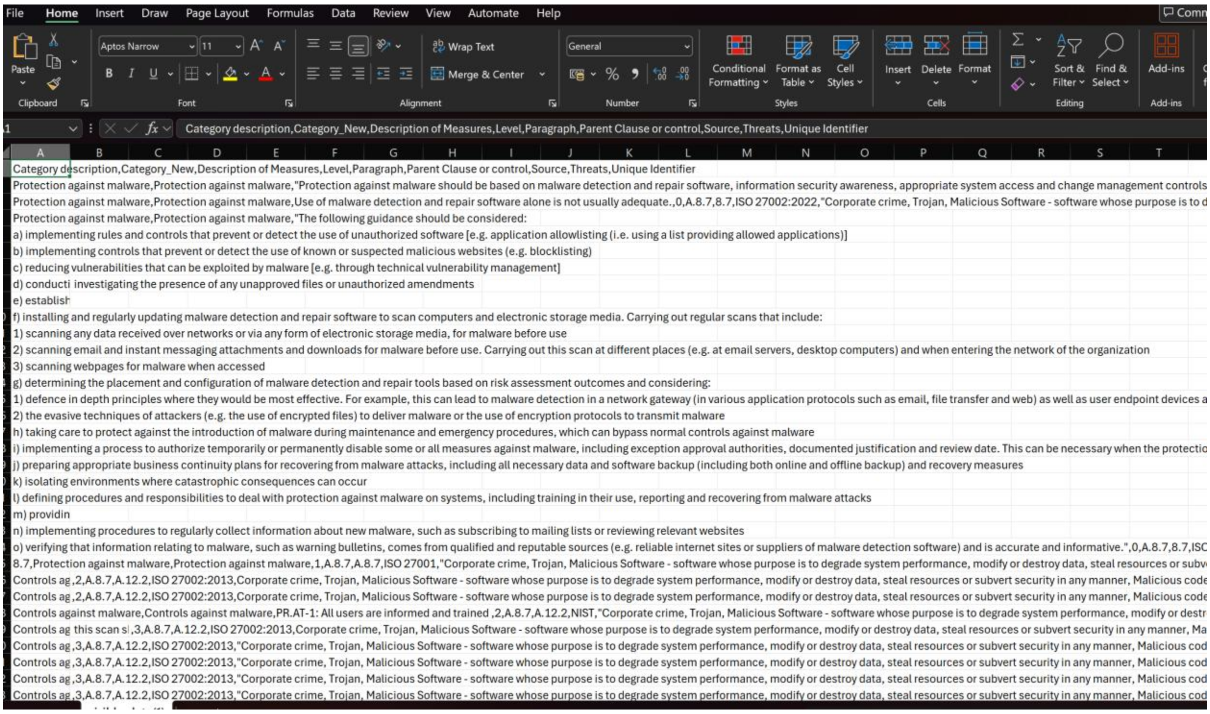


Figure 6 – Export in CSV format

The CURIUM project is supported by the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) under Grant Agreement No. 101190372. Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the ECCC

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.

The CURIUM project is supported by the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) under Grant Agreement No. 101190372. Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the ECCC