Open Data
Maturity Report
2024

Methodology Appendix

data.europa.eu

This study has been prepared as part of data.europa.eu. data.europa.eu is an initiative of the European Commission and is the official portal for European open data. The Publications Office of the European Union manages data.europa.eu.

Appendix: Methodology

This appendix describes the methodology of the 10th edition of the annual open data maturity (ODM) assessment conducted by data.europa.eu.

Contents

Objectives of the open data maturity assessment

Since its launch in 2015, data.europa.eu ([1]) has been the main point of access at the EU level to public sector information published across Europe. The portal aims to improve access to open data, as well as to foster both high-quality open data publication and the reuse of open data to create impact.

Within this remit, data.europa.eu conducts an annual landscaping exercise of European countries on their ODM. Participation is voluntary, and the scope of the assessment includes the EU Member States, European Free Trade Association (EFTA) countries and candidate countries for EU membership.

The purpose of the ODM assessment is to evaluate the development of countries in making public sector information available and stimulating its reuse. The landscaping exercise offers a benchmarking and learning tool for use at both the national and European levels. The results of the assessment support countries in better understanding their relative level of maturity compared with other countries. The results also capture year-on-year developments in countries' ODM and help in identifying areas for improvement. Furthermore, the exercise also results in evidence-based recommendations on the activities that European countries could adopt to increase their ODM.

The ODM assessment is informed by the EU's open data policies, primarily the open data directive (Directive (EU) 2019/1024) and the implementing regulation on high-value datasets (Commission Implementing Regulation (EU) 2023/138). The ODM assessment also includes questions about data that cannot be made open, such as data covered by the Data Governance Act (Regulation (EU) 2022/868), since having an overview of such data is helpful when making publication plans, and open data portals can be used to assist potential reusers in finding information on what protected data can be reused under specific conditions.

([1])   data.europa.eu is the official portal for European open data. The portal was launched in 2021, formed from the merger of the European Data Portal and the European Union Open Data Portal into a single coherent core component of the public sector data infrastructure that has been set up by the EU, its institutions and the Member States.

History of the open data maturity assessment

The first three editions of the ODM assessment (2015–2017) used two dimensions to assess ODM: (1) open data readiness and (2) portal maturity, which evaluated policy developments at the national level and the degree of sophistication of national open data portals, respectively. In 2018, a major update to the landscaping methodology was carried out to better reflect open data developments across Europe. This revision of the methodology made the assessment more comprehensive and placed a stronger emphasis on the quality of metadata and the reuse of and impact derived from open data. The scope of the evaluation was broadened to cover four dimensions: (1) policy, (2) portal, (3) quality and (4) impact.

In 2019, additional layers of granularity were added to the four dimensions. The updates to the assessment aimed to provide further stimulus for national open data teams to redirect their focus onto new strategic areas – such as greater prioritisation of high-quality open data publication, active fostering of mechanisms to monitor open data reuse, and the development of advanced portal features such as multifaceted search and user feedback functionalities – and to raise awareness of the need for more inclusive and participative governance structures.

In 2022, the methodology underwent another structured revision. To this end, all four dimensions and related questions were reviewed. Across the four dimensions, questions were streamlined to better include initiatives at the regional and local levels and specific types of open data, such as real-time data and high-value datasets. In addition, the revision introduced a focus on countries' level of preparedness for the European Commission's upcoming implementing regulation on high-value datasets. A major change in the 2022 methodological update was the restructuring of the impact dimension. This was done to better acknowledge the challenge that countries face in assessing the impact of open data and to better distinguish between measuring the reuse of open data and measuring the impact created through that reuse. This involved adding a new indicator, on measuring impact, to the impact dimension.

In 2024, the method underwent another planned revision. The dimensions and indicators remained unchanged from the previous version of the methodology. In the policy dimension, more detailed explanations were requested regarding the national governance structure, and a question was added about the processes in place to update policies/strategies. In the portal dimension, some mature portal functionalities, such as search and download, were removed from the questionnaire. More detailed explanations were requested regarding how data about portal usage and user feedback are used to improve the portal. In the quality dimension, more detailed explanations were requested regarding the workflows and activities of the portal team to ensure that several aspects of high-quality metadata are achieved. Some questions about the type of support offered to data providers were merged due to overlapping responses from survey respondents. No major changes were made to the impact dimension, except that survey respondents needed to provide only one example of a reuse case for each category (instead of a maximum of three) and explain that case in more detail. Questions about high-value datasets were added across all dimensions, since the related implementing regulation was applicable from June 2024. EFTA and candidate countries could choose 'not applicable' when answering questions regarding specific EU legislative provisions and still be awarded full points under the scoring system.

Work approach

The data for the ODM assessment is collected through a voluntary self-assessment questionnaire sent to national open data representatives. This is done in collaboration with the European Commission and the Expert Group on Public Sector Information. Most questions have a predefined list of response options (e.g. 'Yes' or 'No') from which the respondents select. In addition, most questions request additional supporting information, such as a URL linking to relevant material or a description of related activities. Questions for which data from 2023 was available were prefilled in the questionnaire, enabling survey respondents to confirm if last year's response was still valid or provide a new response. This feature was newly introduced to support year-on-year consistency in responses.

Once the completed questionnaires are submitted, the research team validates the responses. First, the team performs a high-level check of each questionnaire for completeness. Following this, countries are given the opportunity to provide input on any missing answers. Then, an in-depth review of the completed questionnaires is conducted. The reviewers assess whether the explanations accompanying the answers are complete, relate to the question and sufficiently justify the response selected. The reviewers mark questions that are insufficiently answered and therefore require further input from the countries. Since the questionnaires were prefilled, allowing the survey respondents to confirm or change their responses, only answers that survey respondents changed from the previous year and answers for new questions were reviewed in detail.

Finally, a consultation round was held in which the survey respondents were invited to provide additional inputs and revise their responses to and supporting explanations for flagged questions. A preliminary scoresheet was shared with the survey respondents to validate the results. The research team finalised the scores based on the responses to the flagged questions.

Indicators and metrics

The indicators within each dimension are assessed through several questions that pertain to specific concepts. The tables below summarise the key concepts assessed for each indicator.

Dimension 1: Open data policy	
1.1. Policy framework	
1.1.1.	- Open data policies and strategies are in place at the national, regional and/or local levels. - The open data policies/strategies include action plans with concrete measures.
1.1.2.	- The (national) open data strategy incentivises the public and private sectors to reuse open data. - The (national) open data policies/strategies incentivise access to real-time and dynamic data, citizen-generated data and geospatial data. - The (national) open data policies/strategies incentivise the development of data inventories in national, regional and local public bodies.
1.1.3.	- Measures are in place to implement the regulation on high-value datasets. - Progress has been made in ensuring that public bodies holding high-value datasets are prepared to denote those datasets as such in their metadata.
1.2. Governance of open data	

Dimension 1: Open data policy	
1.2.1.	▪ An open data governance structure that ensures open data publication at all government levels is in place. ▪ The governance structure enables the development of open data initiatives at the local and regional levels.
1.2.2.	▪ Details of the person or team responsible for open data activities in the country are publicly available. ▪ A document describing the responsibilities and working approach of the national open data team (and possibly those of regional and/or local teams) is publicly available. ▪ Regular exchanges between the national open data team and the team maintaining the national and/or local portal(s) are ensured.
1.2.3.	▪ Open data officers have been appointed at each public body level. ▪ Regular exchanges between the national open data team and open data officers are ensured. ▪ Regular exchanges between open data officers, data providers and data reusers are ensured.
1.3. Open data implementation	
1.3.1.	▪ Data publication plans exist at the public body level, and progress against these plans is monitored at the national level. ▪ The number of public bodies still charging above the marginal costs for datasets is monitored.
1.3.2.	▪ Measures are in place to address the challenges faced in implementing the aforementioned open data policies/strategies. ▪ There are activities to assist data holders in making their data publicly available. ▪ There are processes in place to update the policies/strategies.
1.3.3.	▪ Training activities for civil servants working with (open) data are in place. ▪ Training activities result in certification and/or are formally recognised as professional development for civil servants. ▪ Society-wide open data literacy initiatives are in place.

Dimension 2: Open data portal	
2.1. Portal features	
2.1.1.	▪ Portal features ensure the discoverability of and access to datasets (including through APIs) and relevant content. ▪ Portal users can find documentation about using APIs and other tools that enable working with metadata, such as through search functionalities.
2.1.2.	▪ Advanced features enable users to provide content for the portal, give feedback on existing content and rate featured datasets.
2.1.3.	▪ The portal enables users to find information and news on relevant open data topics in the country.
2.1.4.	▪ The portal enables interaction and exchange between reusers and publishers.
2.1.5.	▪ Use cases are promoted through a designated section on the portal and mapped to the open data on which they are based. ▪ Reusers can submit use cases to the portal.
2.1.6	▪ Preview functions for both tabular and geospatial data are available.
2.1.7.	▪ The portal has features to promote the visibility and reuse of high-value datasets.
2.2. Portal usage	
2.2.1.	▪ Traffic to the portal (e.g. number of unique visitors, visitor profiles, percentage of outgoing portal traffic generated through APIs, number of downloads) is monitored by the portal team.
2.2.2.	▪ Analytics tools are used to derive insights into users' behaviour and needs. ▪ These insights are embedded in the portal update cycles.
2.2.3.	▪ The most and least consulted categories and datasets are known. ▪ The most used search keywords are known, and updates are performed to ensure greater discoverability of available content.
2.2.4.	▪ API usage is monitored and the results are used to gain insights into user profiles.
2.3. Data provision	
2.3.1.	▪ Most data providers can submit data to the national portal. ▪ Data providers that do not contribute to the national portal have been identified, and actions have been taken to enable data publication from these sources.
2.3.2.	▪ Local or regional data sources are discoverable through the national portal. ▪ Metadata from local or regional data sources is harvested automatically.

Dimension 2: Open data portal	
2.3.3.	▪ Access to real-time data is provided through the national portal. ▪ The percentage of real-time data in all data featured on the portal is known.
2.3.4.	▪ A separate section exists on the portal where community-sourced/citizen-generated data can be uploaded.
2.4. Portal sustainability	
2.4.1.	▪ Measures are in place to ensure that the portal reaches its target audience. ▪ The national portal has accounts and an active presence on social media platforms. ▪ The portal team helps to enhance the visibility of the portal and the featured datasets by organising/attending information sessions and/or events to promote the national portal.

Dimension 3: Open data quality	
3.1. Metadata currency and completeness	
3.1.1.	▪ A predefined approach is in place to ensure that metadata is up to date.
3.1.2.	▪ Mechanisms are in place to ensure that changes at the source are reflected with minimal delay on the national portal.
3.1.3.	▪ The portal provides access to a vast range of historical and current data.
3.1.4.	▪ Mechanisms are in place to ensure the interoperability of high-value datasets with those of other countries.
3.2. Monitoring and measures	
3.2.1.	▪ Mechanisms are in place to monitor the quality of metadata. ▪ Information on metadata quality is available to the broader public.
3.2.2.	▪ Guidelines and/or tools are available to assist data providers in choosing the correct licence for their data. ▪ The compliance level in terms of correct licensing information is monitored.
3.2.3.	▪ Support (e.g. documentation, tools, a helpline) is in place to assist data providers in improving data quality.
3.3. DCAT-AP compliance	
3.3.1.	▪ The national portal follows the DCAT-AP framework or is interoperable with it.
3.3.2.	▪ Compliance with the DCAT-AP standard regarding mandatory, recommended and optional classes is monitored.

Dimension 3: Open data quality	
3.3.3.	▪ Monitoring activities on the percentage of accessible distributions (i.e. the availability of 'accessURL' and 'downloadURL' properties) are in place.
3.4. Deployment quality and linked data	
3.4.1.	▪ A model (e.g. the 5-star open data model or similar) is used to assess the quality of data deployment. ▪ Activities are in place to familiarise data providers with ways to ensure the provision of high-quality data.
3.4.2.	▪ The percentage of published open data that complies with the chosen quality model is known.

Dimension 4: Open data impact	
4.1. Strategic awareness	
4.1.1.	▪ Reuse of open data is monitored at the national, regional or local level, for example through the national portal. This includes monitoring the reuse of high-value datasets.
4.1.2.	▪ Activities are in place at the public body level to boost and monitor the reuse of bodies' own published data.
4.1.3.	▪ A definition of reuse is in place. ▪ A methodology to measure the impact of open data is in place.
4.2. Measuring reuse	
4.2.1.	▪ Activities are in place to understand which datasets are reused and how, for example: o automated feedback mechanisms are in place to track users' access to datasets; o interviews/workshops are conducted with reusers to gather feedback; o surveys / other extensive research tools are used to measure the reuse of open data.
4.2.2.	▪ Activities are in place to better understand reusers' needs, for example: o feedback sessions with portal users are conducted regularly; o social media sentiment analysis is used.
4.2.3.	▪ A process is in place to systematically gather reuse cases. ▪ Reuse cases are classified according to categories (e.g. environmental, social, economic)
4.3. Created impact	
4.3.1.	▪ Data on the impact created by open data on governmental challenges is

Dimension 4: Open data impact	

	available in the country.
	
	 ▪ Various reuse examples exist that showcase the impact of open data on:
	
	    o increasing government efficiency and effectiveness in delivering public services;
	    o increasing the transparency and accountability of public administrations;
	    o enabling better policy- and decision-making.

4.3.2.	▪ Data on the impact created by open data on societal challenges is available in the country.
	
	 ▪ Various reuse examples exist that showcase the impact of open data on:
	
	    o better including marginalised groups and reducing inequality;
	    o raising awareness of urban housing issues;
	    o raising awareness of health- and well-being-related issues;
	    o raising awareness of educational issues.

4.3.3.	▪ Data on the impact created by open data on environmental challenges is available in the country.
	
	 ▪ Various reuse examples exist that showcase the impact of open data on:
	
	    o raising awareness of biodiversity-related topics (e.g. air and water quality);
	    o enabling more environmentally friendly cities;
	    o raising awareness of climate change and related disasters;
	    o encouraging lower energy consumption by reducing fuel use and switching to renewables.

4.3.4.	▪ Data on the impact created by open data on the economy is available in the country.
	
	 ▪ Various reuse examples exist that showcase the impact of open data on the following indicators of economic growth:
	
	    o employment,
	    o technology and innovation,
	    o entrepreneurship and business creation,
	    o productivity.

Scoring

Countries are scored on a list of questions relating to each indicator. Each question-and-answer selection is worth a different number of points. Where relevant, choosing 'not applicable' as an answer is worth full points, for example when EU legislation does not apply to a country. The scores for the individual questions sum together to provide a total score for the indicator. In turn, the indicator scores are added together to give scores for the dimensions. The maximum scores for the indicators and dimensions are shown in the table below. The overall maturity score is calculated as the weighted percentage of all the dimensions, meaning that each dimension contributes 25 % towards the overall maturity score.

Dimension	Indicator	Number of scored questions	Maximum score per indicator	Maximum score per dimension
Policy	Policy framework	13	320	640
	Governance of open data	8	180	
	Open data implementation	7	140	
Portal	Portal features	21	230	670
	Portal usage	9	180	
	Data provision	8	150	
	Portal sustainability	5	110	
Quality	Metadata currency and completeness	6	140	630
	Monitoring and measures	8	160	
	DCAT-AP compliance	7	165	
	Deployment quality and linked data	7	165	
Impact	Strategic awareness	7	140	580
	Measuring reuse	4	120	
	Created impact	20	320	

Pilot indicator: automated metrics of metadata quality

Metrics were extracted from the metadata quality assessment (MQA) to quantitatively evaluate metadata quality. The MQA evaluates the quality of metadata of each catalogue harvested by data.europa.eu.

Five metrics were reported in the MQA as a pilot indicator of ODM quality. The level of compliance with these five metrics was taken for one catalogue per participating country. These metrics are evaluated largely based on the use of specific data catalogue vocabulary application profile (DCAT-AP) properties and the content of these properties in relation to specific controlled vocabularies across distributions in the catalogue. A summary of the metrics and their definitions is provided in Table 1.

Table 1: Selected metrics from the metadata quality assessment

Metric	What is being measured?	How is it measured?
DCAT-AP compliance	DCAT-AP compliance is calculated across all sources and datasets available in a catalogue. This check is only performed if the metadata is originally harvested as a DCAT-AP or as a valid derivate. DCAT-AP is a specification for describing linked public data in Europe.	The metadata is validated against a set of SHACL shapes. The metadata is not compliant if the SHACL validation reports at least one issue. The MQA uses data.europa.eu's DCAT-AP SHACL validation service.
Machine-readable	Checks if the format of the distribution is machine-readable.	The distribution is considered machine-readable if the specified format is contained in the corresponding data.europa.eu GitLab repository vocabulary. Distribution: **dct:format**
DownloadURL	The downloadURL is a direct link to the referenced data.	It is checked whether the property is set or not. Distribution: **dcat:downloadURL**
Licence information	A licence is valuable information for the reuse of data.	Whether the property is set or not is checked. Distribution: **dct:license**
Licence vocabulary	We would like to limit the provision of incorrect licence information. For example, we encounter many Creative Commons licences that lack versioning.	This metric describes all dimensions that the MQA examines to determine the quality. The dimensions are derived based on the principles of findability, accessibility, interoperability and reusability. The MQA recommends and credits the use of controlled vocabularies. The data.europa.eu portal publishes its controlled vocabularies in GitLab. The vocabularies are derived from the EU vocabularies. Distribution: **dct:license**

Pilot indicator: automated metrics of portal performance

In addition to gathering qualitative information on portals, there are technical/quantitative ways to evaluate portals. These tests extend the scope of ODM through standardised tools. Automated tools are online tests through which website URLs are entered and assessed on several criteria. As a pilot, four indicators (mobile friendliness, page speed, security and web accessibility) were measured using standardised online tests. The home page of the main open data portal reported in the ODM survey for each participating country was evaluated.

Mobile-friendliness

The mobile-friendliness indicator assesses how well a website is adapted for access on mobile devices, ensuring a seamless user experience for visitors on smartphones and tablets. This indicator is measured through the Bing Mobile Friendliness Test Tool, which runs checks on the following key factors.

- **Viewport and zoom control configuration.** The viewport meta tag needs to be set correctly in order for mobile-friendly pages to work well on devices of different sizes and orientations. In general, this means that the viewport is set with the content width equal to the device width. While it is possible for pages with an alternate viewport configuration to be mobile friendly on certain devices, they may not work equally well on all devices. The zoom control check verifies if the configuration of the viewport hampers the user's ability to pinch and zoom the page. In general, not using the scale-related viewport settings should result in your page being zoomable on most mobile browsers. However, the improper use of these settings (user scalable, maximum scale, minimum scale) could result in hampering access to some content on the page. Some mobile-friendly pages prevent user zoom by design, and the Bing test takes that into account before flagging an error.
- **Width of page content.** In general, the content width should not exceed the screen width. The Bing test has some tolerance built in, but any page that requires excessive horizontal panning will be flagged for the error 'Page content does not fit device width'.
- **Readability of text on the page.** It is important to understand that readability is a function not just of font size, but also of viewport scaling. It is useful to think of readability as the average area occupied by text when the page is fully zoomed out to fit the device's width.
- **Spacing of links and other elements on the page.** This indicator is related to touch friendliness. The Bing test looks at all input elements and hyperlinks on the page to see if they occupy an area considered 'tap-friendly' at maximum zoom-out. If that is not the case, the page will be flagged with 'Links and tap targets are too small'.
- **Use of incompatible plug-ins.** Another warning that Bing detects is when the page is incompatible with plug-ins (e.g. Flash) or the page is otherwise not intended for use on mobile devices. The Bing tool detects any error messages that are produced by the page on a typical mobile device and currently captures those as warnings in the mobile friendliness test.

Additionally, the tool checks for and reports on resources that are needed to analyse the page fully but that the Bing tool was not able to assess due to robots.txt constraints. This way, rendering issues can be fixed by webmasters by updating robots.txt in such a way that Bing can accurately determine the mobile friendliness of the sites. To analyse a website, the Bing mobile crawler fetches and renders the page, extracting important features that are used by the tool to determine how the page performs

against each of the above factors. The outcomes are then aggregated to provide a consolidated mobile friendliness verdict for the page.

The scoring is as follows:

- if a website passes all the tests, a score of 100 % is attributed;
- if a website fails any of the tests, a score of 0 % is attributed.

Speed and performance

The speed and performance of a website are important parts of its usability. This indicator measures a selection of speed and performance standards from Google's page speed insights.

The following indicators are included:

- **Time to interactive** is the amount of time it takes for the page to become fully interactive. This is an important user-centric metric because it measures how quickly visitors are able to fully interact with the page. It measures a page's load responsiveness and helps identify situations in which a page looks interactive but, in fact, it is not.
- **First contentful paint** measures the time from the start of loading to when elements of the content of the page appear on the user's screen (including images, text, scalable vector graphics and non-white elements). It measures the time from when the page is completely blank until the first element appears on the screen
- **Largest contentful paint** measures the time a website takes to show the user the largest piece of content on the screen, complete and ready for interaction.
- **Cumulative layout shift** measures the largest burst of layout shift scores for every unexpected layout shift that occurs during the entire lifespan of a page. A layout shift occurs whenever a visible element changes its position from one rendered frame to the next.

Each website either passes or fails based on the thresholds set by the tool (Table 2).

Table 2: Google page speed insights thresholds

Test	Pass threshold
Time to interactive	Less than 3.8 seconds
First contentful paint	Less than 1.8 seconds
Largest contentful paint	Less than 2.5 seconds
Cumulative layout shift	Less than 0.1 milliseconds

Security

All URLs were run through the publicly available security testing tool internet.nl, which was developed by the Dutch national government. This tool tests several complementary items, which are considered to contribute to basic cybersecurity hygiene. Each test results in either a pass or fail based on whether or not the URL meets the requirements set.

- **IPv6: reachable through a modern internet address?** Overall, this test checks if the website is reachable for visitors using a modern address (IPv6), making it fully part of the modern internet. The test includes the following subtests.
    - **IPv6 addresses for name servers.** This test checks if your domain name has at least two name servers with an IPv6 address.

- **IPv6 reachability of name servers.** This test checks if all name servers that have an AAAA record with an IPv6 address are reachable through IPv6.
- **IPv6 addresses for web servers.** This test checks if there is at least one AAAA record with an IPv6 address for a web server.
- **IPv6 reachability of web servers.** This test checks if it is possible to connect to a web server through IPv6 on any available ports (80 and/or 443). Additionally, all IPv6 addresses that are received from the name servers are tested. A partial score is given if not all IPv6 addresses are reachable. If an IPv6 address is (syntactically) invalid, it is considered unreachable.
- **Same website on IPv6 and IPv4.** This test compares the response and content received from a web server over IPv6 with that received over IPv4.

- **Domain name system security extensions (DNSSEC): domain name signed?** This test checks if the domain is signed with a valid signature (DNSSEC). If so, visitors with domain signature validation enabled are protected against manipulated translation from the domain into rogue internet addresses.
  - **DNSSEC existence** checks if the domain, more specifically its start of authority record, is DNSSEC signed. If a domain redirects to another domain through a canonical name (CNAME), then it also checks if the CNAME domain is signed (which is conformant with the DNSSEC standard). If the CNAME domain is not signed, the result of this subtest will be negative.
  - **DNSSEC validity** checks if the domain, more specifically its start of authority record, is signed with a valid signature, making it 'secure'.

- **Hypertext transfer protocol secure (HTTPS): secure connection?** Overall, this test checks if information in transit between the website and its visitors is protected against eavesdropping and tampering. This includes the following subtests.
  - **HTTPS available** checks if the website is reachable on HTTPS. If so, it also checks in the below subtests whether HTTPS is configured sufficiently securely in conformance with the *IT Security Guidelines for Transport Layer Security (TLS)* from National Cyber Security Centre in the Netherlands. HTTPS guarantees the confidentiality and integrity of the information exchanged. Because how (privacy) sensitive and valuable information is depends on the situation, a secure HTTPS configuration is important for every website. Note that, for performance reasons, the tests in the HTTPS test section are only run for the first available IPv6 and IPv4 addresses.
  - **HTTPS redirect** checks if a web server automatically redirects visitors from HTTP to HTTPS on the same domain (through a 3xx redirect status code like 301 or 302) or if it offers support for only HTTPS and not HTTP. If the server does redirect visitors, a domain should first upgrade itself by redirecting to its HTTPS version before it redirects to another domain. This also ensures that the HTTP strict transport security (HSTS) policy will be accepted by the web browser. Note that this subtest is only conducted if the given domain correctly redirects from HTTP to HTTPS. An eventual further redirect to a different domain (including a subdomain of the tested domain) is not tested.
  - **HTTP compression** makes a secure connection with a web server vulnerable to a browser Reconnaissance and exfiltration via adaptive compression of hypertext attack. However, HTTP compression is commonly used to make more efficient use of the available bandwidth. This subtest checks if a web server supports HTTP compression at the root

directory level. However, it does not check additional website sources like images and scripts.

— **HSTS** checks if your web server supports HSTS. Browsers remember HSTS per (sub)domain. Not adding a HSTS header to every (sub)domain (in a redirect chain) may leave users vulnerable to man-in-the-middle attacks. Therefore, this subtest checks for HSTS on first contact (i.e. before any redirection).

— **Transport layer security (TLS) version** checks if a web server supports only secure TLS versions. A web server may support more than one TLS version.

— **Cyphers (algorithm selections)** checks if a web server only supports secure (i.e. 'good' and/or 'sufficient' cyphers (also known as algorithm selections)). An algorithm selection consists of cyphers for four cryptographic functions: (a) key exchange, (b) certificate verification, (c) bulk encryption and (d) hashing. A web server may support more than one algorithm selection.

— **Cypher order** checks if a web server enforces its own cypher preference ('I') and offers cyphers in accordance with the prescribed ordering ('II').

— **Key exchange parameters** checks if the public parameters used in Diffie–Hellman key exchange by a web server are secure.

— **Hash function for key exchange** checks if a web server supports secure hash functions to create the digital signature during key exchange.

— **TLS compression** checks if a web server supports TLS compression. The use of compression can give an attacker information about the secret parts of encrypted communication. An attacker that can determine or control parts of the data sent can reconstruct the original data by performing a large number of requests. TLS compression is used so rarely that disabling it is generally not a problem.

— **Secure renegotiation** checks if a web server supports secure renegotiation.

— **Client-initiated renegotiation** checks if a client (usually a web browser) can initiate a renegotiation with a web server. Allowing clients to initiate renegotiation is generally not necessary and leaves a web server open to denial-of-service attacks inside a TLS connection. An attacker can perform similar denial-of-service attacks without client-initiated renegotiation by opening many parallel TLS connections, but these are easier to detect and defend against using standard mitigation procedures.

— **Zero round trip time resumption** checks if a web server supports zero round trip time resumption.

— **Online Certificate Status Protocol stapling** checks if a web server supports the TLS certificate status extension, also known as Online Certificate Status Protocol stapling.

— **Trust chain of certificate** checks if it is possible to build a valid chain of trust for a website certificate. To have a valid chain of trust, the certificate must be published by a publicly trusted certificate authority, and the web server must present all necessary intermediate certificates.

— **Public key of certificate** checks if an elliptic curve digital signature algorithm or a Rivest–Shamir–Adleman algorithm digital signature of a website certificate uses secure parameters.

— **Signature of certificate** checks if the signed fingerprint of a website certificate was created with a secure hashing algorithm.

— **Domain name on certificate** checks if the domain name of a website matches the domain name on the certificate.

— **Domain-name-system-based authentication of named entities (DANE) existence** checks if the name servers of a website domain contain a correctly signed TLS authentication record for DANE. As DNSSEC are a precondition for DANE, this test will fail if DNSSEC are missing on the website domain or if there are DANE-related DNSSEC issues (e.g. no proof of 'denial of existence').

— **DANE validity** checks if the DANE fingerprint presented by a domain is valid for the web certificate.

Accessibility foundations

This indicator evaluates the accessibility status of websites, assessing how usable websites are for a large variety of users (regardless of, for instance, their visual abilities). The open-source [Axe-core tool](#) (browser extension) is used to measure this indicator. This indicator can also be defined as the extent to which websites comply with the foundational parts of the EN 301 549 standard (web content accessibility guidelines (WCAGs) level AA).

The tool takes into account the most recent WCAGs and covers 20 of the 50 success criteria, with tests across all of the four main principles (perceivability, operability, understandability and robustness). For this pilot indictor, the following seven success criteria were measured.

- **Alternative text (WCAG 1.1.1)** evaluates whether a website offers text alternatives for non-text content, enabling it to be transformed into formats like large print, braille, speech, symbols or simplified language to meet diverse user needs.

- **Colour contrast (WCAG 1.4.3)** evaluates if the visual presentation of text and images of text on a website has a contrast ratio of at least 4.5:1.Exceptions include cases of large text, text or images part of an inactive user interface component and text that is part of a logo or brand name.

- **Page/document title (WCAG 2.4.2)** evaluates if a website has titles that describe the topic or purpose.

- **Link name (WCAG 2.4.4)** evaluates the clarity and accessibility of links on a website.

- Language attribute (WCAG 3.1.1) evaluates if the primary language of each web page is specified in a way that can be identified by software, such as screen readers and search engines.

- **Valid language code (WCAG 3.1.2)** evaluates if the language of each passage or phrase in a website's content can be identified and defined by software, allowing assistive technologies (e.g. screen readers) to accurately convey content in the appropriate language.

- **Name, role and value (WCAG: 4.1.2)** evaluates the accessibility and compatibility of user interface components of a website with assistive technologies.

If no violations are found, the website is at least potentially accessible. If violations are found, the website is at least not fully accessible. The tool reports on the number and types of violations found.

ODM