



## Digital Maturity Assessment Questionnaire for EDIH Customers

**Target group: Public Sector Organisations**

**Stage: T0 (prior to EDIH support start)**

### Version history

2.0	31 January 2024	Updated format
1.0	08 March 2023	First version of the document

Document created by



## Table of Contents

<b>1. Module 1: Customer Data</b> .....	<b>3</b>
<b>M1.1. General Data:</b> .....	<b>3</b>
<b>M1.2. Sector of Activity:</b> .....	<b>3</b>
<b>2. Module 2: Digital Maturity</b> .....	<b>5</b>
<b>M2.1. Digital Strategy and Investments</b> .....	<b>5</b>
<b>M2.2. Digital Readiness</b> .....	<b>6</b>
<b>M2.3. Human-centric digitalisation</b> .....	<b>7</b>
<b>M2.4. Data Management and Security</b> .....	<b>8</b>
<b>M2.5. Interoperability</b> .....	<b>9</b>
<b>M2.6. Green digitalisation</b> .....	<b>10</b>

# 1. Module 1: Customer Data

*In this module, please provide basic general information about the public sector organisation that is interested in receiving EDIH support. This data is needed in order to analyse how your organisation's level of digital maturity compares to that of similar others.*

## M1.1. General Data:

1. Date
2. Name of the organisation supported by the EDIH:
3. Other identification number (VAT or equivalent):
4. Contact person:
5. Role in the organisation:
6. Email address:
7. Telephone:
8. Website:
9. Type of public sector organisation:
  1. National authority
  2. Regional authority
  3. Province/municipal authority
  4. Other
10. Organisation's staff size
  1. Small-size (0-49)
  2. Medium-size (50-249)
  3. Large-size (250 or more)
11. Full address (Street, Postal code, City, Country)
12. PIC<sup>1</sup> number (if available, to be filled by EDIH)

## M1.2. Sector of Activity:

13. In which of the following government broad areas does your organisation belong<sup>2</sup>?  
Please select up to two options:

Primary (one mandatory):

1. General public services
2. Defence
3. Public order and safety
4. Economic affairs
5. Environmental protection
6. Housing and community amenities
7. Health
8. Recreation, culture and religion
9. Education
10. Social protection
11. Other

<sup>1</sup> Participant Identification Code

<sup>2</sup> Classification of the functions of government (COFOG): [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Classification\\_of\\_the\\_functions\\_of\\_government\\_\(COFOG\)](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Classification_of_the_functions_of_government_(COFOG))

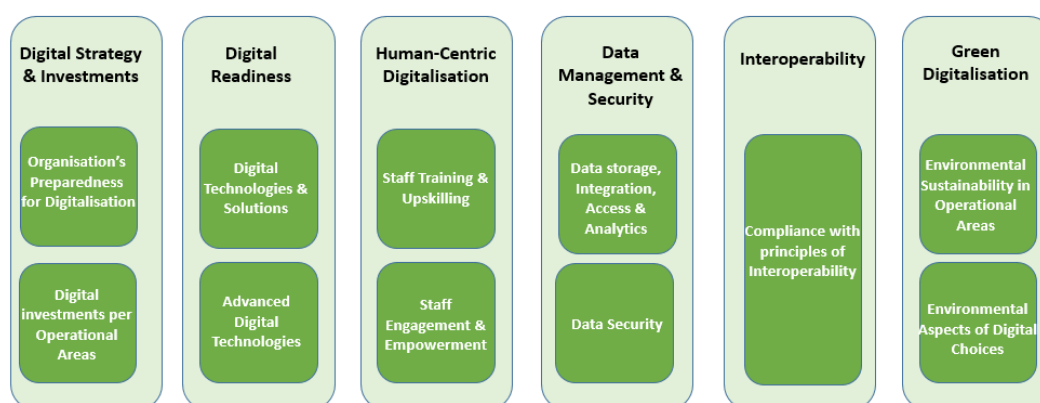
Secondary (one optional):

1. General public services
2. Defence
3. Public order and safety
4. Economic affairs
5. Environmental protection
6. Housing and community amenities
7. Health
8. Recreation, culture and religion
9. Education
10. Social protection
11. Other

## 2. Module 2: Digital Maturity

Questions in this module aim to measure the digital maturity of your organisation. This information will help to characterise the point of departure for the digital transformation journey of your organisation, identifying areas where it might need EDIH support. It will also help to assess the services eventually provided by the EDIH, as well as to help assess the EU policies and financial instruments supporting EDIHs. The following dimensions will be assessed (applying the scoring criteria detailed in the end page):

*Digital Maturity Assessment Framework for Public Sector Organisations (PSOs), Source: EC JRC own elaboration*



### M2.1. Digital Strategy and Investments

The questions of this dimension intend to capture the overall status of a digitalisation strategy in your organisation. They ask about the organisation's readiness to embark on a digital journey that might require organisational and economic efforts not yet foreseen and related investments in digitalisation per area of activity (either executed or planned).

#### 1. In which of the following ways is your organisation prepared for (more) digitalisation? Please select all options that apply

1. Digitalisation needs are identified and are aligned with policy making/administrative objectives
2. Financial resources (own funds, grants, loans) are identified to secure digitalisation projects during at least the following two years
3. ICT infrastructures<sup>3</sup> are ready to support digitalisation plans
4. ICT specialists are employed/sub-contracted (or hiring/subcontracting needs have been identified)
5. There is appropriate level of political commitment to lead the necessary organisational changes needed
6. Organisational units'/departments' management and their staff are prepared and ready to support digitalisation plans

<sup>3</sup> In general, it refers mainly to hardware but also includes network infrastructure, cloud infrastructure (data storage and service delivery), servers (data capture and management locally) and tablets/terminals/PCs for staff etc.

7. Internal and external operational processes can be adapted if required by digitalisation
8. Offline services are ready to be brought online or further modernised by digital technologies
9. Citizens' and other stakeholders' (businesses, NGOs etc) satisfaction with online services/interactions is monitored regularly (e.g. via feedback forms, emails exchanges, social media, etc.)
10. Risks of digitalisation (e.g. non-planned effects over other areas<sup>4</sup>) are considered

**2. In which of the following operational areas has your organisation already invested in digitalisation and in which ones does it plan to invest in the future? Please select all options that apply.**

	Already invested	Plan to invest
1. Internal operations (administrative, structural, organisational processes) <sup>5</sup>		
2. External operations (governance processes including new ways of citizen participation) <sup>6</sup>		
3. Policy making (Policy making cycle: agenda setting, policy formulation, policy adoption, policy implementation, policy evaluation) <sup>7</sup>		
4. Provision of public services <sup>8</sup> (or products)		
5. Financial administration (accounting, logistics, eInvoices etc.)		
6. Human resources management		
7. Purchasing and public procurement		
8. Project planning and management		

## M2.2. Digital Readiness

*The digital readiness dimension provides an assessment of the current uptake of digital technologies (both mainstream and more advanced technologies).*

**3. Which of the following digital technologies and solutions are already used by your organisation? Please select all options that apply:**

1. Connectivity infrastructure (e.g. high speed (fibre) Internet, cloud computing services, remote access to office systems)

<sup>4</sup> Risks from implementing advanced digitalisation could include: labor redundancy, introduction of technological bias and unfairness, threats to data privacy etc.

<sup>5</sup> Refers to the introduction of digitalisation to improve quality and efficiency of internal and external processes. Creation of new organisational forms, introduction of new management methods and techniques, new working methods.

<sup>6</sup> Refers to the introduction of digitalisation for the creation of new governance methods (for citizen (and/or) business to administration relationships), involvement of new actors, new patterns of co-creation and interaction.

<sup>7</sup> Refers to the introduction of digitalisation for the improvement in identifying the needs of constituents and shortening the time required to develop, test, implement and diffuse a policy.

<sup>8</sup> Refers to the introduction of digitalisation for the creation of new public services or products or improvement of the existing ones.

2. Website
3. Web-based forms or forums to communicate with citizens
4. Live chats, social networks and/or chatbots to communicate with citizens
5. Remote collaboration tools (e.g. teleworking platform, videoconferencing, virtual learning, service-specific platforms and tools)
6. Internal web portal (Intranet)
7. Information Management Systems (e.g. Enterprise Resources Planning, Accounting, HR Management, Customer Relationship Management, e-invoicing)
8. Tools for digital public services (online interaction with citizens and/or businesses, online service delivery)
9. Public procurement tools (eProcurement)

**4. Which of the following advanced digital technologies<sup>9</sup> are already used by your organisation? Please choose all options that apply using the provided scale.**

1. Artificial Intelligence (e.g. Machine learning, Deep learning; Expert and Rule based systems; Cognitive computing, predictive analytics; Robotic process automation; Natural Language Processing, Text Mining, Computer Vision)
2. Communication Technologies (e.g. 5G Networks and Handheld Devices; Software Defined Networks)
3. Computing Infrastructures (e.g. High Performance Computing; Cloud Computing; Edge Computing)
4. Distributed Ledger Technologies (e.g. Blockchain; Other Distributed Ledger Technologies)
5. Digital Identity and Security (e.g. Firewall and Protocols; Antivirus and Vulnerability Scanners; Biometric Screening; Cloud-oriented Cybersecurity; Advanced User Analytics; Mobile ID; Digital Identity Frameworks)
6. Immersive technologies (e.g. Augmented Reality; Virtual Reality)
7. Internet of things and Smart Devices (e.g. Mobile Devices, Wearables and Sensors; Internet of Things Platforms)
8. Software and Service Technologies (e.g. APIs, Web Services, Microservices including Registries and Marketplace; Enterprise Service Bus Technologies and Government Service Utilities)

### M2.3. Human-centric digitalisation

*This dimension looks at how staff are skilled, engaged and empowered with and by digital technologies, and their working conditions improved, with a view to increase their productivity and wellbeing.*

**5. What does your organisation do to re-skill and up-skill its staff for digitalisation? Please select all options that apply:**

1. Assesses digital skills gaps of the staff
2. Designs a training plan to train and up-skill staff

<sup>9</sup> Recently a JRC study has proposed a number of emerging and mature technologies in the public sector as relevant for the design and implementation of digital public service provision: European Commission, Joint Research Centre, Bruno, I., Schiavone Panni, A., Marchetti, V., et al., *A multi-dimensional framework to evaluate the innovation potential of digital public services : a step towards building an innovative public services observatory in the EU*, Misuraca, G.(editor), Lobo, G.(editor), Publications Office, 2020, <https://data.europa.eu/doi/10.2760/09628>

3. Organises short trainings, provides tutorials/guidelines and other e-learning resources
  4. Facilitates learning-by-doing/peer learning/experimentation opportunities
  5. Offers traineeships & job placements in key capacity areas
  6. Sponsors staff participation in trainings organised by external organisations (training providers, academia, vendors)
  7. Makes use of subsidised training and upskilling programmes
- 6. When adopting new digital solutions, how does your organisation engage and empower its staff and end-users (citizens/businesses in case of digital public services)? Please select all options that apply:**
1. Increases staff awareness about new digital technologies
  2. Communicates digitalisation plans to staff in a transparent and inclusive way
  3. Monitors staff acceptance and takes measures to mitigate the potential collateral effects (e.g. fear to change; 'always on' culture vs. work-life balance; safeguards to risks of privacy breaches etc.)
  4. Involves staff (including non-ICT staff) in the design and development of product/service/process digitalisation
  5. Gives staff more autonomy and appropriate digital tools to take and execute decisions
  6. Redesigns/Adapts jobs and workflows based on staff's feedback
  7. Sets up more flexible working arrangements enabled by digitalisation (e.g. telework, hybrid working)
  8. Puts at staff's disposal a digital support team/service (internal/external)
  9. Puts at end-users disposal a digital support team/service (internal/external)
  10. Uses feedback from end-users (citizens/businesses) to improve digital public services

## M2.4. Data Management and Security

*This dimension captures how data are digitally stored, organised within the organisation, made accessible across connected devices and exploited for business purposes, keeping an eye on ensuring sufficient data protection via cybersecurity schemes. The question covers data stored in all possible forms including documents.*

- 7. How are your organisation's data managed (i.e. stored, organised, accessed and exploited)? Please select all options that apply:**
1. The organisation has in place a data management policy/plan/set of measures
  2. The organisation does not use paper-based forms to collect data
  3. Data are stored only digitally in the organisation (e.g., in office applications, email folders, stand-alone applications, data bases, document management systems, ERP etc.)?
  4. Data are properly integrated (e.g. through interoperable systems, Application Programming Interfaces) even when they are distributed amongst different systems
  5. Data are accessible in real-time from different devices and locations
  6. Collected data are systematically analysed and reported for decision-making
  7. Organisation's data are enriched with third-party data (i.e. data from other public sector organisations and/or private sector actors)



- 8. Organisation’s data analytics are accessible without the need of expert assistance on a regular base (e.g. through dashboards)
- 9. Organisation’s data are available publicly via an Open Data policy plan

**8. Are your organisations’ data sufficiently secured? Please select all options that apply:**

- 1. A data security policy/set of measures is in place in our organisation
- 2. There are established plans and measures to safeguard organisation’s data from cyberattacks
- 3. Staff is regularly informed and trained on cybersecurity and data protection issues/risks
- 4. Cyber-threats are regularly monitored and assessed
- 5. A full backup copy of critical data is maintained (off-site/in the cloud)
- 6. A business continuity plan is in place in case of catastrophic failures (e.g. all data locked by a ransomware attack or physical damage to the IT infrastructure)

M2.5. Interoperability

*This dimension explores the level of interoperability<sup>10</sup> the organisation has reached measured against the level of planning/implementation of a number of the 12 interoperability principles of the new European Interoperability Framework (EIF)<sup>11</sup>.*

**9. While digitalising processes and services, what does your organization do to share data, information and knowledge with other public sector organizations? Please select all options that apply to your organisation using the provided scale:**

(Not implemented and/or no plans to implement, Plan to implement, Already implemented)

	Implemented	Planned
<ul style="list-style-type: none"> <li>1. Publish data as Open Data</li> <li>2. Ensure a level playing field for open source software</li> <li>3. Give preference to open specifications</li> <li>4. Ensure internal visibility and provide external interfaces for provided services</li> <li>5. Reuse and share solutions, information and data</li> <li>6. Do not impose any technology-specific solutions on end-user</li> <li>7. Ensure data portability</li> <li>8. Give end-users options to access services that best suits their needs</li> <li>9. Provide a single point of contact to access services</li> <li>10. Ask users once-only and relevant-only information</li> </ul>		

<sup>10</sup> For the purpose of the EIF, interoperability is the ability of organisations (public administration units or any entity acting on their behalf, or EU institutions or bodies) to interact towards mutually beneficial goals, involving the sharing of information and knowledge between these organisations, through the business processes they support, by the means of exchange of data between their ICT systems.

<sup>11</sup> The New EIF defines 12 interoperability principles as fundamental behavioural aspects to drive interoperability actions. They are general interoperability principles relevant to the process of establishing interoperable European public services. More info:

[https://ec.europa.eu/isa2/sites/default/files/eif\\_brochure\\_final.pdf](https://ec.europa.eu/isa2/sites/default/files/eif_brochure_final.pdf)

- |   |  |  |  |
|---|--|--|--|
| <ul style="list-style-type: none"> <li>11. Persons with disabilities, the elderly and other disadvantaged groups can access services</li> <li>12. Services are available in more than one language</li> <li>13. Ensure that data exchange with end-users is secure and trustworthy</li> <li>14. Give priority to using services via digital channels</li> <li>15. Data storage formats ensure long-term accessibility</li> <li>16. Digital solutions are evaluated considering user needs and balancing between costs and benefits</li> </ul> |  |  |  |
|---|--|--|--|

## M2.6. Green digitalisation

*This dimension captures the capacity of an organisation to undertake digitalisation with a long-term approach that takes responsibility and cares about the protection and sustainability of natural resources and the environment.*

### **10. How does your organisation make use of digital technologies to contribute to environmental sustainability? Please select all options that apply:**

1. Sustainable organisational model (e.g. environmental conscious operations)
2. Sustainable service provision (e.g. paperless digital public services)
3. Procurement of sustainable products (e.g. considering criteria such as: eco-design, end-to-end product lifecycle planning, end-of-life & extension of useful life)
4. Considering emissions, pollution and/or waste management
5. Sustainable energy generation in own facility
6. Optimisation of energy consumption/cost
7. Reduction of transport costs
8. Digital applications to encourage responsible citizens behaviour
9. Paperless administrative processes

### **11. Is your organisation taking into account environmental impacts in its digital choices and practices? Please grade all options that apply using this scale: No, Partially, Yes:**

1. Environmental concerns and standards are embedded in the organisation's digital strategy
2. An Environmental Management System/certification is implemented
3. Environmental aspects are part of digital technologies/suppliers' procurement criteria
4. Energy consumption of digital technologies and data storage are monitored and optimised
5. Recycling/re-use of old technological equipment is actively practised by the organisation