# D1.10 – Regulation and Trustworthy System v2

WP1 – NEED: Industrial Scenarios and Requirements Analysis

European Commission

i4Q has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 958205.

## Document Information

| | | | | |
|---|---|---|---|---|
| GRANT AGREEMENT NUMBER | 958205 | ACRONYM | | i4Q |
| FULL TITLE | Industrial Data Services for Quality Control in Smart Manufacturing | | | |
| START DATE | 01-01-2021 | | DURATION | 41 months |
| PROJECT URL | https://www.i4q-project.eu/ | | | |
| DELIVERABLE | D1.10 – Regulation and Trustworthy System v2 | | | |
| WORK PACKAGE | WP1 – NEED: Industrial Scenarios and Requirements Analysis | | | |
| DATE OF DELIVERY | CONTRACTUAL | 31-Dec-2023 | ACTUAL | 29-Dec-2023 |
| NATURE | Report | | DISSEMINATION LEVEL | Public |
| LEAD BENEFICIARY | TUB | | | |
| RESPONSIBLE AUTHOR | Jan Mayer | | | |
| CONTRIBUTIONS FROM | LIF | | | |
| TARGET AUDIENCE | 1) i4Q Project partners 2) Project officer | | | |
| DELIVERABLE CONTEXT/ DEPENDENCIES | This document has no further iterations as it is the second and updated version in the topic of Trustworthy Systems and Regulations. | | | |
| EXTERNAL ANNEXES/ SUPPORTING DOCUMENTS | None | | | |
| READING NOTES | None | | | |
| ABSTRACT | The i4Q project, focused on developing trustworthy industrial systems, has made significant strides as evidenced in Deliverables D1.6 and D1.10. D1.6 established a foundation by aligning i4Q solutions with regulatory standards as a benchmark for trust and compliance. Building on this, D1.10 provides an update on regulatory changes and an evaluation of trustworthiness requirements, highlighting a shift towards prioritizing user experience, ethical standards, and regulatory compliance. D1.10 collectively underscore the project's adaptive approach, balancing technical requirements with emerging trends and stakeholder needs, thereby establishing the i4Q project as a paradigm in developing robust, reliable, and secure systems in the evolving technological landscape. | | | |

## Document History

| VERSION | ISSUE DATE | STAGE | DESCRIPTION | CONTRIBUTOR |
|---|---|---|---|---|
| 0.1 | 27-Sep-2023 | ToC | Distribution of ToC | TUB |
| 0.2 | 02-Oct-2023 | ToC | Evaluation of ToC | ITI |
| 0.3 | 10-Oct-2023 | 1st Draft | Survey Distribution | TUB |
| 0.4 | 28-Nov-2023 | 2nd Draft | Final Contribution - Regulations | LIF |
| 0.5 | 30-Nov-2023 | 3rd Draft | Draft available for internal review | TUB |
| 0.6 | 08-Dec-2023 | Internal Review | Internal Review Process | EXOS, IKER |
| 0.7 | 15-Dec-2023 | 4th Draft | Address comments from the internal review | TUB, LIF |
| 1.0 | 29-Dec-2023 | Final Doc | Quality check and issue of final document | CERTH |
| | | | | |
| | | | | |

## Disclaimer

Any dissemination of results reflects only the author's view and the European Commission is not responsible for any use that may be made of the information it contains.

## Copyright message

# TABLE OF CONTENTS

# LIST OF FIGURES

# LIST OF TABLES

# ABBREVIATIONS/ACRONYMS

| | |
|---|---|
| **ACM** | Association for Computing Machinery |
| **AHP** | Analytical Hierarchy Process |
| **AI** | Artificial Intelligence |
| **ALTAI** | Assessment List for Trustworthy Artificial Intelligence |
| **ASEW** | Automated Software Engineering Workshop |
| **BS** | British Standards |
| **EU** | European Union |
| **GPAI** | Global Partnership on AI |
| **HPC** | High-Performance Computing |
| **IEC** | International Electrotechnical Commission |
| **IEEE** | Institute of Electrical and Electronics Engineers |
| **ISO** | International Standardisation Organisation |
| **ML** | Machine Learning |
| **NIST** | National Institute of Standards and Technology |
| **OECD** | Organisation for Economic Cooperation and Development |
| **PDF** | Portable Document Format |
| **RI** | Relative Importance |
| **SME** | Small and medium-sized enterprise |
| **TSFr** | Trustworthiness Framework |
| **TL** | Trust Levels |
| **UI** | User Interface |
| **UK** | United Kingdom |
| **US** | United States |

# Executive summary

The i4Q project has made significant strides in developing trustworthy systems, as evidenced by the key deliverables D1.6 and D1.10. Deliverable D1.6, titled "Regulations and Trustworthy System," has been instrumental in laying the foundational framework for the project. By incorporating the British Standard BS 10754-1:2018, this deliverable initiated a comprehensive evaluation of i4Q solutions, focusing on trust and regulatory compliance (British Standards Institution, 2018). It set a precedent for aligning the project with international best practices and legal standards, establishing a robust baseline for trustworthiness.

Expanding upon this strong foundation, D1.10 presents a comprehensive update on the progression of the i4Q project, examining the latest regulatory changes. This exploration is crucial in ensuring that i4Q solutions continue to adhere to evolving contemporary standards, thereby maintaining their relevance and compliance in a rapidly changing regulatory environment. In addition to addressing regulatory shifts, D1.10 also undertakes an extensive evaluation of the trustworthiness requirements, demonstrating an agile response to the evolving priorities of pilot partners. This process involves developing strategic recommendations for solution providers, aimed at enhancing the overall quality and reliability of the i4Q solutions. A key revelation from D1.10 is the apparent shift in focus towards prioritizing user experience and ethical standards, alongside maintaining regulatory compliance. This shift underscores an increasing emphasis on developing software that is not only functionally robust but also user-friendly and ethically responsible. Attributes such as error-free coding, intuitive user interfaces, and adherence to ethical practices in software development have gained heightened importance, reflecting a broader industry trend towards more human-centric and ethically guided technology solutions. Concurrently, D1.10 observes a diminishing focus on certain technical aspects such as system interoperability and version control. This observation suggests a re-evaluation of these elements, possibly influenced by advancements in technology and a deeper understanding of stakeholder needs and expectations. Such changes highlight the project's commitment to staying attuned to the latest technological advancements and aligning its strategies accordingly.

The future trajectory of the i4Q project when outcomes are being transferred to industry, includes deepening its engagement with emerging technologies while maintaining a strong commitment to ethical standards and user experience. This balanced approach is expected to not only meet but anticipate the complex demands of the industry, ensuring that the solutions developed are not just reactive but proactive in addressing the needs of a rapidly evolving industrial landscape, especially in trustworthiness and reliability. In doing so, D1.10 serves as a potential basis for future initiatives which develop innovative, trustworthy systems that resonate with the nuanced requirements of the industry.

## Document structure

**Section 1:** This section delves into the integral role of trustworthy systems within the i4Q project, including a short recap of the former version of this deliverable (D1.6). It discusses the project's commitment to ensure that systems adhere to high standards of reliability and security, catering to the evolving landscape of industrial quality control.

**Section 2:** The section outlines recent regulatory changes, focusing on the implications of EU directives and international standards. It emphasizes the project's alignment with these updates to maintain compliance and address global market needs.

**Section 3:** An analysis of the latest survey results compares current findings with previous data, reflecting changes in stakeholder priorities. The section concludes with targeted recommendations for solution providers to enhance system trustworthiness.

**Section 4:** Provides the conclusions.

# 1. Trustworthy Systems in i4Q

## 1.1 Overview

D1.10 represents a significant advancement in the i4Q project, offering a thorough and detailed update on the progress made towards establishing highly trustworthy systems. Building upon the groundwork laid by Deliverable D1.6, it not only revisits and reinforces the core objectives and methodologies of the project but also introduces new perspectives and findings. This deliverable is particularly focused on assimilating the latest regulatory changes and standards, ensuring that the i4Q systems remain at the forefront of compliance and best practices in the rapidly evolving technological landscape. Furthermore, it delves into an extensive evaluation of the trustworthiness requirements, reflecting the project's commitment to adapting and responding to the dynamic needs of its stakeholders. Through comprehensive analysis and forward-looking insights, D1.10 plays a pivotal role in guiding the i4Q project's journey towards achieving its goal of developing robust, reliable, and secure systems.

## 1.2 Recap from D1.6

The previously submitted Deliverable D1.6 serves as a cornerstone in the i4Q project's endeavours, primarily aimed at forging a platform that embodies trustworthiness through stringent adherence to both current and emerging regulatory standards. It provides an in-depth assessment of the i4Q solutions, scrutinizing them through the lens of trustworthiness and compliance with regulatory norms. Hence, it employs the British Standard BS 10754-1:2018 (2018) as its central guiding principle, ensuring that the approach to trustworthiness is grounded in recognized and respected standards. This deliverable not only sets the stage for future developments within the project but also establishes a benchmark for evaluating the extent to which i4Q solutions align with international best practices and legal requirements. By systematically addressing the various dimensions of regulatory compliance and trust, D1.6 lays a robust foundation for the project, positioning it to navigate the complexities of the contemporary digital landscape effectively. It serves as a critical reference point for all subsequent initiatives within the i4Q project, ensuring that every solution developed is not only technologically advanced but also ethically sound and legally compliant.

The document begins by defining the necessity of a trustworthy system and its contextual relevance to other project deliverables, emphasizing its impact on future work packages. A systematic literature review then establishes a knowledge base, drawing from current research and standards to identify project limitations and inform subsequent steps. A critical component of the deliverable is Section 3, which delves into existing and forthcoming EU regulations, particularly concerning AI integration in i4Q solutions. It outlines five key requirements for future compliance and exploitation of AI-based software: Data and Data Governance, Transparency for Users, Human Oversight, Accuracy, Robustness and Cybersecurity, and Technical Documentation and Record-keeping. This section also considers the international legal landscape, offering a guideline for AI-based solutions that encompasses the entire software life cycle. Moreover, the i4Q Trustworthiness Framework (TSFr) is introduced, which incorporates findings from the literature review. The framework includes three main elements: the five pillars of trust (safety, reliability, availability, resilience, and security), the core i4Q services, and the broader environment affecting the trustworthiness of i4Q solutions. This framework serves as a baseline for developing a trustworthy system and defines the project's scope. In addition, the i4Q TSFr is designed to establish a reliable and trustworthy structure for the i4Q solutions, focusing on Zero Defect Manufacturing. The framework incorporates various elements, each contributing to the overall trustworthiness of the system:

1. **Trustworthy Pillars:** These pillars are derived from the literature review and the structure of i4Q solutions. They are based on the British Standard BS 10754-1:2018, which outlines facets of trustworthiness applicable to all systems, including the i4Q core services.

2. **Environment:** The framework acknowledges that the system's trustworthiness is influenced by its environment. This primarily involves compliance with European Union regulations, while also considering the regulations of other countries where i4Q solutions will be deployed, emphasizing the significance of European standards in accordance with the Commission's focus on benefiting Europe through its funded projects. These regulations encompass laws and standards, ensuring compliance in the development of i4Q core solutions.

3. **Technical Infrastructure:** Trustworthiness is heavily impacted by the technical infrastructure in customers' factories and within i4Q solutions themselves. This includes a focus on various aspects such as data quality, trustiness, communication, security, and storage, all addressed in different work packages of the project.

4. **Human Factors:** Given that i4Q solutions are mostly semi-automatized, human interaction with the system is a significant factor. Human users and operators are considered both as potential risks and essential contributors to the system's trustworthiness, necessitating the development of conceptual models and control methods for proper system understanding.

5. **Process:** This includes all hardware and software-related processes and procedures involving human interaction in the operative state of i4Q solutions. Any flaws or potential faults in these processes could impact the system's overall trustworthiness.

6. **Software Libraries:** The use of open-source software libraries in i4Q solutions is seen as a potential risk to trustworthiness. To mitigate this, strict quality checks are required for all libraries used in the solutions.

7. **Events:** The framework considers both external and internal events that could impact the system's operation. External events include accidents, attacks, or natural disruptions, while internal events are system failures or malfunctions.

8. **Core Services:** Inspired by Bose et al.'s (2019) framework, the i4Q TSFr employs different layers—edge, storage, analytical, and visualization—to structure the i4Q platform. Each layer has its own functionalities, with specific solutions assigned to them or connections between them. This structure ensures secure data integration, transformation, and communication across the platform, addressing security and workload distribution across different layers.

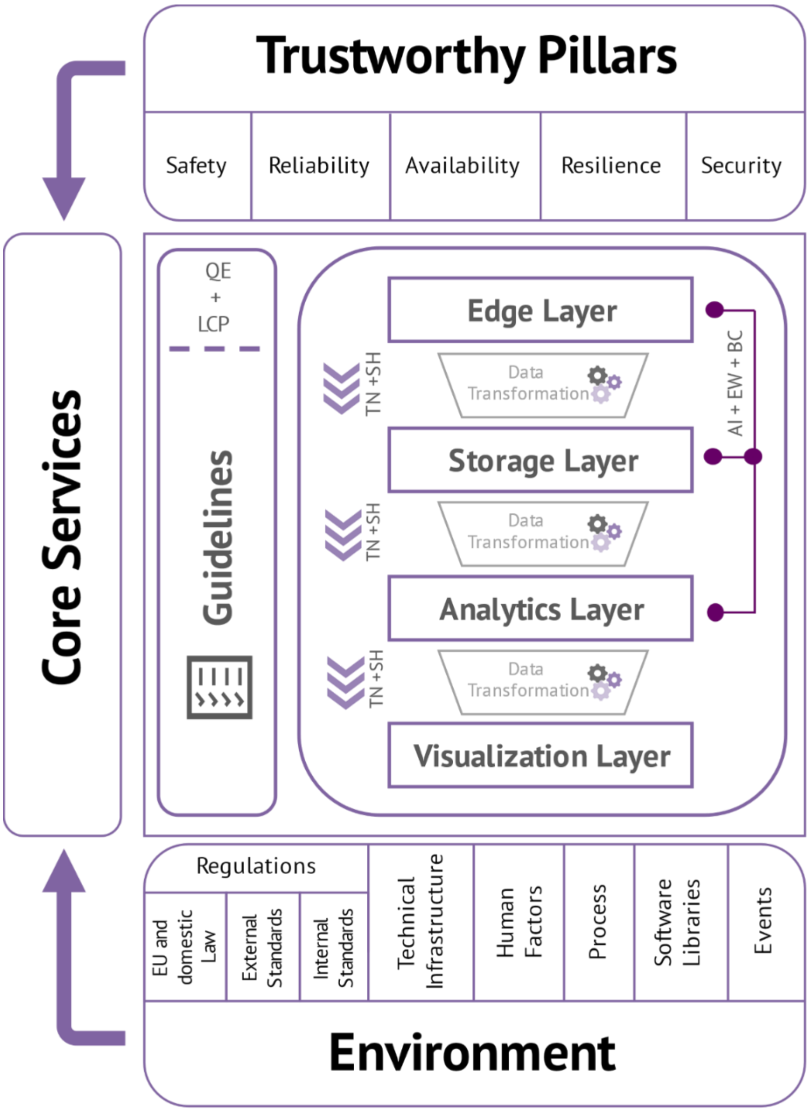


**Figure 1.** TSFR developed in D1.6

In an innovative approach, the requirement elicitation process is detailed, adapted from the British Standard BS 10754-1:2018 for the i4Q context. This involves defining Trust Levels (TLs) for i4Q solutions and developing a set of requirements for each of the five Trustworthy Pillars. These requirements were then transformed into a survey for prioritization by pilot partners. Furthermore, an analysis of the current state of trustworthiness of i4Q solutions was conducted, identifying potential risks and gaps. This analysis involved mapping requirements to individual solutions and comparing pilots' needs with solution providers' offerings and concludes with a Trustworthy Score for each layer of the framework and a gap analysis to inform future development actions.

D1.6 establishes a comprehensive set of requirements for ensuring trust in i4Q solutions across their entire software life cycle. It highlights the importance of continuous observation of identified risks in the development process and sets the stage for the next iteration of the document, which will evaluate and compare the achieved trustworthiness of i4Q solutions against the current state.

# 2. Updates from Regulations

## 2.1 EU-Dimension

With the development and progress of the AI-driven technologies, the need for relevant and up-to-date legal regulations has further emerged. While aiming to support research and industrial capacity, the ensuring of safety and protection of fundamental rights is of utmost importance.[1] EU legislators have been working in this direction, aiming to cover all needed grounds and potential risks and these efforts resulted in the Artificial Intelligence Act[2].

### 2.1.1. Timeline of the EU Approach on AI

The EU has been developing and expanding its approach on AI for a couple of years, working on different areas and identifying the most important standards and aspects that need to be addressed by the legislative response. The timeline with all significant steps that have been taken prior to the AI Act can be seen below[3]:

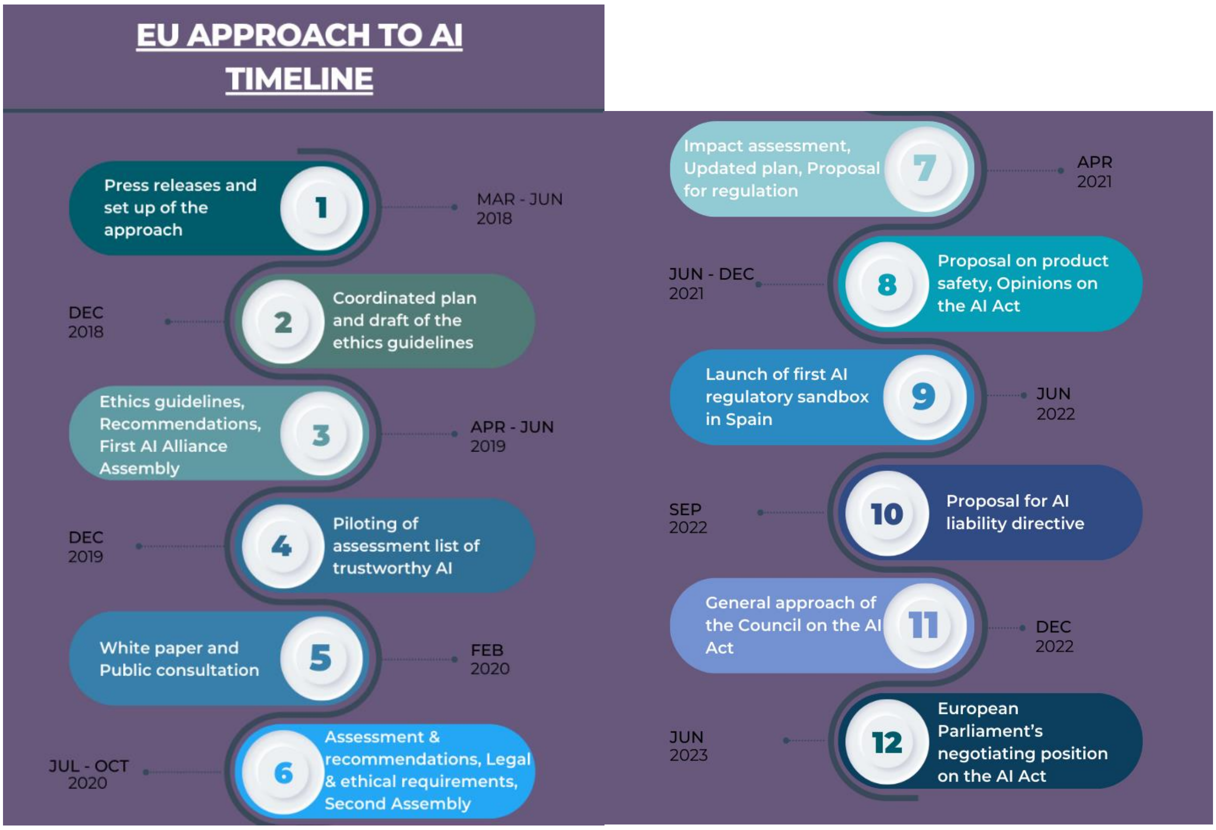

EU APPROACH TO AI TIMELINE
1 Press releases and set up of the approach
MAR - JUN 2018
2 Coordinated plan and draft of the ethics guidelines
DEC 2018
3 Ethics guidelines, Recommendations, First AI Alliance Assembly
APR - JUN 2019
4 Piloting of assessment list of trustworthy AI
DEC 2019
5 White paper and Public consultation
FEB 2020
6 Assessment & recommendations, Legal & ethical requirements, Second Assembly
JUL - OCT 2020
7 Impact assessment, Updated plan, Proposal for regulation
APR 2021
8 Proposal on product safety, Opinions on the AI Act
JUN - DEC 2021
9 Launch of first AI regulatory sandbox in Spain
JUN 2022
10 Proposal for AI liability directive
SEP 2022
11 General approach of the Council on the AI Act
DEC 2022
12 European Parliament's negotiating position on the AI Act
JUN 2023

**Figure 2.** Timeline of the EU approach regarding the AI Act

[1] https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

[2] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts COM/2021/206 final, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206

[3] Ibid 1.

In the first half of 2018 several important documents have been released, marking the initial European approach and its set up. In addition, the establishment of the AI expert group and the European AI alliance is also communicated as well as the initial versions concerning liabilities in the field. The documents are the following:

- Press release: AI expert group and European AI alliance
- Press release: Artificial intelligence for Europe ;
- Communication: Artificial intelligence for Europe ;
- Staff working document: Liability for emerging digital technologies ;
- Declaration of cooperation on artificial intelligence ;
- Launch of the European AI alliance ;
- Set up of the high-level expert group on AI

At the end of 2018, the European Commission released the Coordinated plan on AI and the ethics guidelines for a trustworthy AI system have been drafted.

- European Commission: Coordinated plan on AI ;
- European Commission (Press release): AI made in Europe ;
- European Commission Communication: AI made in Europe ;
- Stakeholder consultation on draft ethics guidelines for trustworthy AI

In April 2019, the High-level expert group on AI released the Ethics guidelines for trustworthy AI, putting the focus further on the trustworthy standards and requirements. In addition, policy and investment recommendations have as well been disseminated in June.

- European Commission Communication: Building trust in human-centric artificial intelligence ;
- High-Level expert group on AI: Ethics guidelines for trustworthy AI ;
- First European AI Alliance Assembly ;
- High-Level Expert Group on AI: Policy and investment recommendations of AI

At the end of 2019, the Assessment List for Trustworthy AI was released, acting as a support instrument for the Ethics Guidelines for Trustworthy AI. Its purpose is the users' benefit from AI and the mitigation of any unnecessary risks.

- High-Level Expert Group on AI: Piloting of assessment list of trustworthy AI ;

In February 2020, the European Commission has disseminated its first while paper on AI, which explains the EU approach "aims to promote Europe's innovation capacity in the area of AI while supporting the development and uptake of ethical and trustworthy AI across the EU economy. AI should work for people and be a force for good in society".

- European Commission: White paper on AI: a European approach to excellence and trust ;
- Public consultation on a European approach to excellence and trust in AI ;

In the second half of 2020, the concept of trustworthy AI is further developed, resulting in a number of important reports that have been released.

- Inception impact assessment: Ethical and legal requirements on AI ;
- High-Level Expert Group on AI: Final assessment list on trustworthy AI (ALTAI) ;
- High-Level Expert Group on AI: Sectorial recommendations of trustworthy AI ;
- 2nd European AI Alliance Assembly ;

In April 2021, the European Commission released 4 crucial documents, outlining and confirming the European approach on AI. One of them includes a proposal for AI rules at EU level that should support the consistent implementation throughout the Member States. These 4 documents are as follows:

- European Commission: Communication on Fostering a European approach to AI ;
- European Commission: Proposal for a regulation laying down harmonised rules on AI ;
- European Commission: updated coordinated plan on AI ;
- European Commission: Impact assessment of an AI regulation ;

For the rest of 2021, several opinions on the proposed AI Act have been disseminated, aiming at enhancing and improving the areas needed.

- Public consultation on Civil liability – adapting liability rules to the digital age and artificial intelligence ;
- European Commission: Proposal for a Regulation on Product Safety ;
- Council of the EU: SI Presidency compromise text on the AI Act (.PDF) ;
- High-Level Conference on AI: From Ambition to Action (3d European AI Alliance Assembly) ;
- European Economic and Social Committee, Opinion on the AI Act ;
- Committee of the Regions, Opinion on the AI Act ;
- European Central Bank, Opinion on the AI Act (.PDF) ;

In June 2022, the first regulatory sandbox was launched in Spain. It aimed to support the implementation of the future regulatory rules and the testing of specific technical solutions and processed. In addition, it facilitated the transition to the respective rules and obligations of the affected companies and SMEs.

- Launch of first AI regulatory sandbox in Spain: Bringing the AI Regulation forward ;

In September 2022, the AI liability directive proposal aimed to improve the internal market by imposing consistent rules for non-contractual civil liability aspects for damage caused by AI systems or such that were connected to them.

- Proposal for an AI liability directive ;

At the end of 2022 the Council's approach on the AI Act have been disseminated, outlining the main points that will be covered as well as the objectives that will be considered.

- General approach of the Council on AI Act ;

In June 2023, the Parliament has also released its position on the Act and the main requirements that will have to be included such as the ban of biometric surveillance, emotion recognition, predictive policing, the need of disclosure that content was AI-generated, and the high-risk effect of the involvement of AI systems in the election process.

- European Parliament's negotiating position on AI Act ;

### 2.1.2. AI Act

The purpose of the European Parliament envisaged in the AI Act, is to ensure that the created and used AI systems are "safe, transparent, traceable, non-discriminatory and environmentally friendly".[4] The importance of the human monitoring is also strongly outlined, aiming at preventing harmful outcomes.

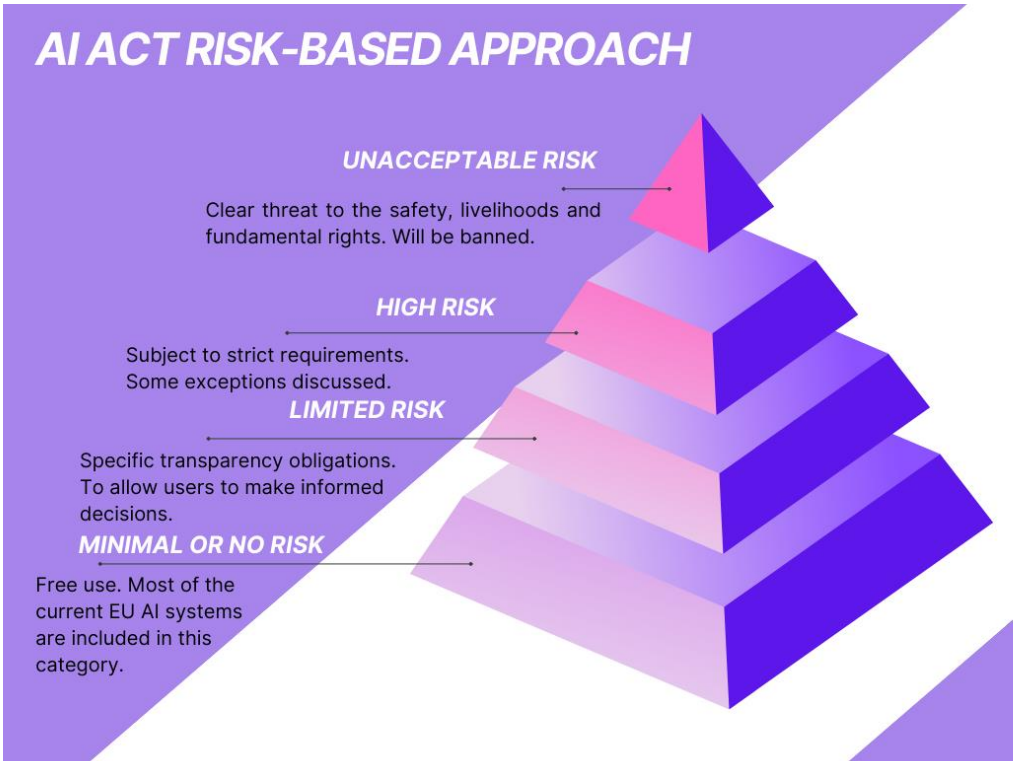

AI ACT RISK-BASED APPROACH
UNACCEPTABLE RISK
Clear threat to the safety, livelihoods and fundamental rights. Will be banned.
HIGH RISK
Subject to strict requirements. Some exceptions discussed.
LIMITED RISK
Specific transparency obligations. To allow users to make informed decisions.
MINIMAL OR NO RISK
Free use. Most of the current EU AI systems are included in this category.

**Figure 3.** AI Act risk-based approach

[4] https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

The approach that the Parliament has chosen to use for this legislation is based on a risk assessment methodology. The level of potential risks must be assessed and depending on that, obligations can be imposed on providers or users. The types of identified risks are the following:

**Unacceptable risk:** The AI systems that fall under this category are considered as people threatening and are going to be prohibited. They could include: "Cognitive behavioural manipulation of people or specific vulnerable groups: for example, voice-activated toys that encourage dangerous behaviour in children; Social scoring: classifying people based on behaviour, socio-economic status or personal characteristics; Real-time and remote biometric identification systems, such as facial recognition". Potential exceptions could be introduced such as related to crime prevention.

**High risk:** The high-risk AI systems are such that can be a treat to safety or fundamental rights. Parties that are creating them should comply with regulations that demand thorough testing, appropriate documentation and a responsibility structure that envisages human oversight. They will have to be analysed and evaluated prior to being allowed to be distributed, as well as after that. In addition, they will be divided into 2 categories:

- Falling under the scope of EU product safety legislation
- 8 areas that will have to be registered in an EU database:
    - Biometric identification and categorization of people;
    - Management and operation of critical infrastructure;
    - Education and vocational training;
    - Employment, worker management and access to self-employment;
    - Access to essential private and public services and benefits;
    - Law enforcement;
    - Migration, asylum and border control management;
    - Legal assistance.

**Limited risk:** Only minimal transparency requirements shall be imposed for this group. The aim is to give the opportunity to users to make informed decisions. Part of this is for the system to make clear to the users that they are interacting with AI.

**Minimal or no risk:** The majority of the current AI systems in the EU are in this category, including applications such as AI-enabled video games or spam filters.

**Generative AI** shall have to implement transparency requirements:

- AI generated content disclosure;
- Designing models to prevent generating illegal content;
- Publishing summaries of copyrighted data used for training.

The next steps for this piece of legislation are the discussions of the Member States in the Council about the finalization of the Act.

In addition to evaluating the risk of the AI systems, the protection of citizens' rights is also strongly considered. However, to also support innovation, the researching of AI-based systems may be done under open-source licenses. The system is integrated into an open test environment so that the public can test if prior to its release on the market. Furthermore, citizens are encouraged to file complaints when needed and be informed of the decisions based on high-risk AI systems that could amount to risks for their rights.[5]

## 2.2 International Regulation

In order to make i4Q solutions competitive at international level, it is important to consider regulatory efforts in the area of AI. What is more, the international regulation might inform the processes taking place in the EU. Additionally, some EU member states would be affected by international regulation given their membership and participation in international organization.

Similarly, to the EU, the international response to the AI systems and the legislations systems are still in draft and adaptation phases. Many countries have started their attempts to achieve a consistent approach, however, few have achieved tangible results.[6]

The UK response to the developments in the area of AI differs from the EU. They have outlined 5 high-level principles that should act as guiding points in the matters concerning AI systems:

- safety, security and robustness;
- appropriate transparency and explainability;
- fairness;
- accountability and governance; and
- contestability and redress.

Instead of working on harmonized AI legislation, the UK has taken the approach of giving this responsibility to the different existing regulators so that they can create their own AI responses. This, however, means that these individual regulators will have to have a significant expertise on AI so that they can be able to take decisions and impose adequate measures.[7] In addition to this, the UK together with the US has established the Atlantic Declaration[8] that aims to established cooperation between the two countries in achieving a suitable approach towards AI, focusing on safety and security.

Another international response to AI is the G7 Hiroshima AI process. The G7 has announced that it will work with the Global Partnership on AI (GPAI) and the Organization for Economic Cooperation and Development (OECD) on AI Governance, however, no major announcements have been disseminated so far.[9]

In 2022, the Canadian Parliament introduced a draft AI regulation using a modified risk-based approach. It has three pillars, aiming to support consistency of the private companies' design and

[5] https://www.europarl.europa.eu/news/en/press-room/20230609IPR96212/meps-ready-to-negotiate-first-ever-rules-for-safe-and-transparent-ai

[6] https://iapp.org/media/pdf/resource_center/global_ai_legislation_tracker.pdf

[7] https://www.osborneclarke.com/insights/what-status-eu-uk-and-international-regulation-artificial-intelligence

[8] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1161879/THE_ATLANTIC_DECLARATION.pdf

[9] https://www.osborneclarke.com/insights/what-status-eu-uk-and-international-regulation-artificial-intelligence

development of AI. The Canadian draft differs from the EU's approach as it does not prohibit the use of automated decision-making tools. However, a mitigation plan to mitigate risks and increase transparency when using AI in high-risk systems is required, ensuring that no anti-discrimination laws are violated.[10]

The United States are also in the process of defining a legislation process dedicated to the AI systems as there are many areas and technology field that have been affected by them. AI Bill of Rights has been released, which covers the AI misuse and safety recommendations for the public and private sectors, however, this AI strategy would not be legally binding. It puts a focus on safety approaches for data privacy, algorithmic discrimination, safe and effective AI tools prioritization. It should serve as a guide for lawmakers at all levels that shall be responsible for the potential AI regulation. In addition, an agency in the Department of Commerce – NIST, has published standards for managing AI bias. Furthermore, the individual states are also working in this direction, some of them even already passing laws for AI bias.[11]

China has recently introduced a regulation on how private companies can use algorithms for consumer marketing that involves the informing of users and bans the use of customer financial information for advertising different prices of the same items. This does not apply to the Chinese government's use of AI. Shanghai has become the first province to approve a law for private-sector AI development. It provides a framework about developing AI products in line with non-Chinese AI regulations.[12]

The changing regulations at international and European level will require for all AI-related companies to be able to transform their processes and technologies, accordingly, focusing on the ethics and compliance of their products.

## 2.3 Standards

The changes and progress of the AI systems requires rapid adaptations in both their legal regulations and standards. Currently, the following standards have crucial impact on the AI technologies[13]:

**Foundational Standards:**

ISO/IEC 22989: Provides definitions and terminologies and covers over 110 concepts such as datasets, bias, transparency, and explain ability, etc.

ISO/IEC 23053: Building on first one, it sets up a framework for AI systems explanation that uses Machine Learning (ML). It also describes the different components of the system and their roles.

**Process standards:**

[10] https://www.progressivepolicy.org/blogs/an-overview-and-of-global-ai-regulation-and-whats-next/

[11] https://www.progressivepolicy.org/blogs/an-overview-and-of-global-ai-regulation-and-whats-next/

[12] Ibid

[13] https://www.holisticai.com/blog/ai-governance-risk-compliance-standards

ISO/IEC CD 42001: Includes a template for responsibly integrating and using AI management systems. It is still at a draft stage, but will target organizations that will have to comply with conformity assessment requirements such as the ones that will fall under the EU AI Act.

ISO/IEC CD 42006: Guiding and specifying requirements for enabling relevant bodies to reliably audit and assure the management systems for organizations that develop and/or use AI systems according to ISO/IEC 42001.

ISO/IEC 38507: Guiding the governing body of an organization which is using or shall potentially use AI systems. Focusing on the governance structures to support effective, efficient, and acceptable AI use, outlining the relevant standards for effective governance in AI implementation.

ISO/IEC 23894:2023(E): Guidance on risk management for development, deployment and usage of AI systems. Describes the processes for the integration and implementation of AI Risk Management.

**Measurement standards:**

ISO/IEC DTS4213: Provides methodologies and tools for measuring and evaluating the performance of classification algorithms and ML models.

ISO/IEC TR 24027: Provides measurement metrics for evaluating bias in AI-enabled decision-making.

**Performance standards:**

IEEE 2937: Outlines methodologies for evaluating the performance of AI servers, server clusters and other AI High-Performance Computing (HPC) systems. It provides guidance on performance testing, metrics and measurement, and technical requirements for benchmarking tools.

ISO/IEC AWI 27090: Currently in draft phase, this standard shall guide organizations to address, detect and mitigate information security risks, threats and failures in AI systems.

The implementation of all these standards in the context of AI systems provides monitoring mechanisms for these systems and hence the products that they are being used for not only before it is released to the market, but also after that. The testing and measuring tools and approaches can closely monitor the compliance of the system as well as the emergence of any potential risks, hence increasing the chance of a timely risk mitigation reaction.

# 3. Evaluation of Requirements for Trustworthiness

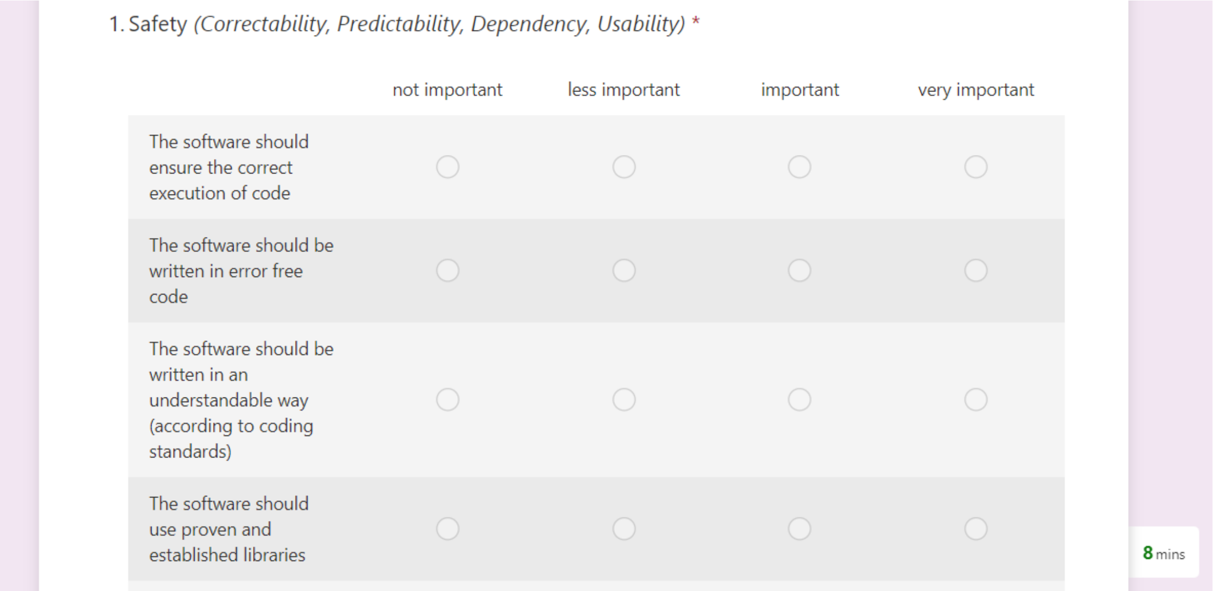
## 3.1 Survey for Pilot Partners

To reassess and update the requirements, a second survey was conducted among the pilot partners. This iteration of the survey continued to utilize a Likert scale ranging from 1 to 4, which gauges the importance of each requirement from the perspective of the participating companies. Using an even-numbered scale like this intentionally prompts participants to lean towards a particular preference, indicating a more decisive stance on the significance of each requirement (Chyung et al., 2017). The meanings assigned to each Likert point remain consistent with the previous survey, as detailed in Table 1:

| Likert Point | Description |
|---|---|
| 1 | Not important |
| 2 | Less important |
| 3 | Important |
| 4 | Very important |

**Table 1.** Likert scale description

This follow-up survey was once again distributed using Microsoft Forms, integrated into the i4Q working platform through Microsoft SharePoint. Invitations to participate were extended to the six Pilot partners and an additional generic presentation pilot from UPV. The survey was structured to present general aspects, the primary objective, and the expected completion time. To ensure comprehensive feedback, the survey was designed so that participants could not submit incomplete responses or provide multiple answers to a single question. A screenshot of the survey interface is depicted in **Figure 4**.



1. Safety *(Correctability, Predictability, Dependency, Usability)* *

| | not important | less important | important | very important |
|---|---|---|---|---|
| The software should ensure the correct execution of code | ○ | ○ | ○ | ○ |
| The software should be written in error free code | ○ | ○ | ○ | ○ |
| The software should be written in an understandable way (according to coding standards) | ○ | ○ | ○ | ○ |
| The software should use proven and established libraries | ○ | ○ | ○ | ○ |

**Figure 4.** Example of conducted survey

With the initial preparation and information gathering complete, the subsequent step for the pilots is to undertake a thorough analysis and comparison of the results from the second survey.

The comprehensive feedback from this survey is detailed in the annex. The primary objective of this analysis is to identify the most critical requirements as perceived collectively by all pilot partners. For this comparative analysis, a method akin to the Analytic Hierarchy Process (AHP) (Saaty, 1994) is employed.

**Weighted Requirements**

The first phase involves tallying the occurrences of each Likert point and then squaring these counts. This approach not only prioritizes the more important requirements but also distinguishes those with lesser interest. Next, the data is categorized using even bin sizes in a histogram. This process is formally described by the equation C, where:

- 'i' represents the number of pilots.
- 'j' indicates each stated requirement.
- 'x' denotes the level of Likert points, corresponding to the survey's semantics and embodying an ordinal hierarchy.
- 's' is the frequency of occurrence of 'x'.

The equation is as follows:

$$C(x)= \sum_{i=1}^{I}\sum_{j=1}^{J}[s(i,j)=x]*x$$

$$\forall\ x=1,2,3,4;\ s=1,\ \dots,\ S;\ i=1,\ \dots,\ I;\ j=1,\ \dots,\ J$$

Upon applying this formula to the received survey feedback, the resultant heatmap in Table 2 visually displays the distribution of the weighted importance of the requirements. This representation allows for an initial, nuanced interpretation of the survey results. Generally, most requirements are deemed important by the pilot companies, although some are of less concern than others. Notably, the Security Pillar emerges as a focal point of attention among the pilots, a finding that could be particularly informative for guideline usage, which was conducted in Work Package 3.

## 3.2 Comparison of Results with D1.6 – for Pilots

A histogram, as shown in **Figure 5**, visualizes the distribution of these RIs, grouping the requirements into classified bins. From the perspective of the pilots, a significant observation is that the majority of the 'very important' requirements fall under the categories of reliability and security. This indicates a strong preference for system attributes that guarantee service delivery as specified and robust protection against both accidental and intentional security breaches. This concentration suggests that the pilot partners prioritize a software system's dependability and its ability to safeguard against various threats. Reliable systems are expected to perform consistently, delivering services accurately as per specifications under varying conditions. Security, on the other hand, encompasses the system's capacity to defend against both inadvertent errors and deliberate attempts at compromise, which includes the integrity of data, the resilience of operations, and the privacy of sensitive information. In extending this understanding, the histogram also serves as a tool for identifying potential areas of improvement. It can direct focus towards those categories where the requirements have not been rated as 'very important' but still play a critical role in the overall user experience and system performance. For instance, while not all requirements in the safety category may have been marked as 'very important', their role in preventing system failures and ensuring user safety cannot be understated.

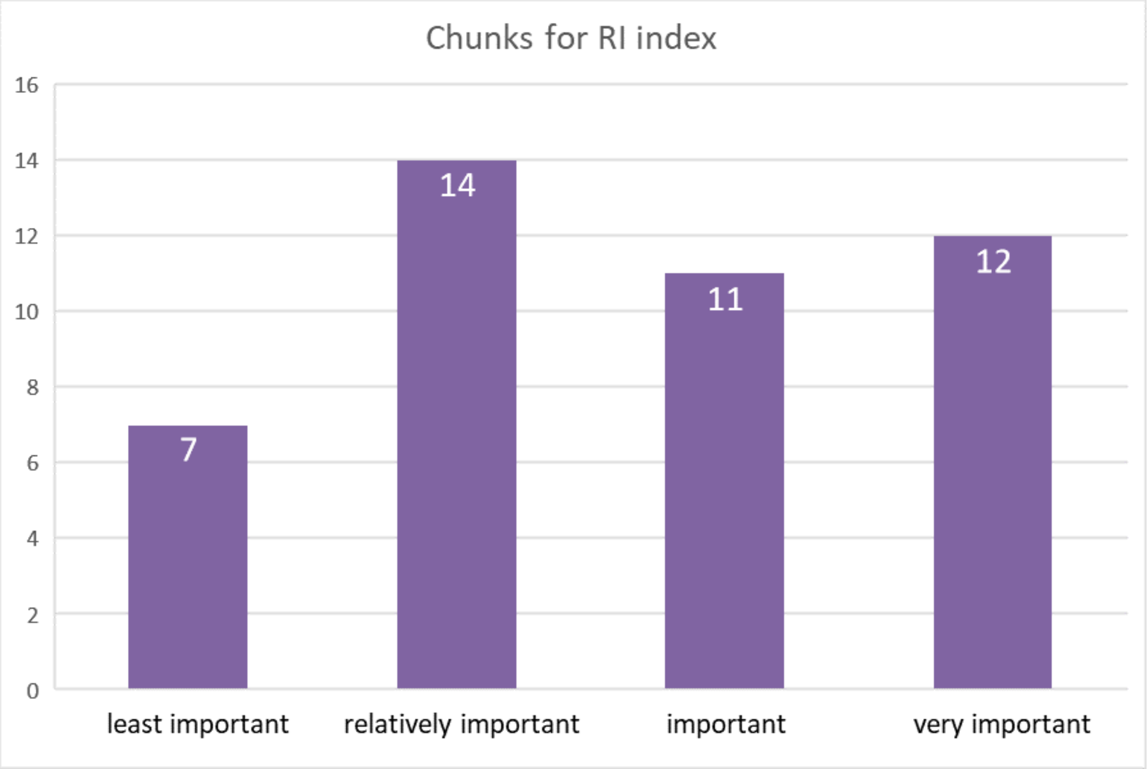


**Figure 5.** Distribution of RI among all requirements

In comparison to the previously mentioned deliverable D1.6, which identified the prevention of data loss and corruption due to harmful events as the most important requirements, the current table offers a more detailed breakdown within different categories of software attributes like Safety, Reliability, Availability, Resilience, and Security. As can be seen in Table 2 it is clear that requirements related to 'ensuring protection against data corruption (harmful events)' and 'proceeding according to ethical standards' within the Resilience category are rated as 'very important' by 20 and 16, respectively, reflecting a high level of consensus on their critical nature. Similarly, in the Security category, 'ensuring secure data transfer processes' and 'being restricted in functionalities according to EU law' are rated 'very important' by 16 pilots each, indicating a significant concern for adherence to regulatory standards and data security.

Contrastingly, some requirements like 'ensuring the correct execution of code' in the Safety category and 'ensuring consistent data formats' in Reliability are also highly rated as 'very important', suggesting that pilots place a strong emphasis on the foundational aspects of software functionality and data integrity. Comparing both sets of data, it becomes evident that while the prevention of data loss and corruption remains a top priority, there is also a broad recognition of the importance of ethical standards, regulatory compliance, and fundamental operational reliability. This nuanced view underscores the multi-faceted nature of trustworthiness in software systems as perceived by the pilot partners.

|  | Requirement | very important | important | less important | not important |
|---|---|---|---|---|---|
| SAFETY | The software shall ensure the correct execution of code. | 20 | 6 | 0 | 0 |
|  | The software shall be written in error free code. | 12 | 12 | 0 | 0 |
|  | The software shall be written in an understandable way (according to coding standards). | 4 | 12 | 2 | 1 |
|  | The software shall use proven and established libraries. | 4 | 12 | 2 | 1 |
|  | The software shall behave as from stakeholders intended. | 4 | 15 | 2 | 0 |
|  | The software shall be self-optimizing (monitor own mistakes) in terms of false predictions. | 4 | 15 | 2 | 0 |
|  | The software shall only use appropriate and established data formats. | 0 | 12 | 4 | 1 |
|  | The software shall behave in interaction with other solutions as intended. | 0 | 6 | 8 | 1 |
|  | The software shall ensure proper data exchange. | 8 | 12 | 2 | 0 |
|  | The software shall be intuitive to use. | 12 | 12 | 0 | 0 |
|  | The software shall proceed user input in a proper way. | 12 | 12 | 0 | 0 |
| RELIABILITY | The software shall be developed by experts. | 8 | 12 | 0 | 1 |
|  | The software shall be used by instructed users only. | 8 | 12 | 2 | 0 |
|  | The software shall ensure appropriate storage capacity. | 4 | 0 | 10 | 1 |
|  | The software shall ensure consistent data transfer. | 12 | 9 | 2 | 0 |
|  | The software shall ensure consistent data formats. | 16 | 6 | 2 | 0 |
|  | The software shall ensure stable operations. | 8 | 12 | 2 | 0 |
|  | The software shall not be harmful to other components (Workload). | 12 | 12 | 0 | 0 |
|  | The software shall work in different infrastructures (os, hardware). | 12 | 9 | 2 | 0 |
|  | The software shall provide the needed confidence levels. | 12 | 6 | 2 | 1 |
|  | The software shall provide the desired confidence in changing environment (algorithm). | 4 | 12 | 4 | 0 |

| | | | | | |
|---|---|---|---|---|---|
| | The software shall provide backup functionalities. | 8 | 6 | 4 | 1 |
| | The software shall ensure proper data transformation processes. | 4 | 6 | 8 | 0 |
| | The software shall ensure the minimization of fault-forecasting. | 0 | 18 | 2 | 0 |
| **AVAILABILITY** | The software shall ensure the interoperability with other solutions. | 4 | 9 | 6 | 0 |
| | The software shall ensure its stand-alone operability. | 4 | 9 | 6 | 0 |
| | The software shall (automatically or manually) update its libraries. | 8 | 12 | 2 | 0 |
| | The software shall (automatically or manually) update itself for its environment. | 0 | 9 | 6 | 1 |
| | The software shall ensure its integration to other software systems. | 4 | 9 | 4 | 1 |
| | The software shall ensure the convenient processing of unseen data. | 12 | 6 | 2 | 1 |
| **RESILIENCE** | The software shall ensure protection against data loss (harmful events). | 12 | 6 | 2 | 1 |
| | The software shall ensure protection against data corruption (harmful events). | 20 | 6 | 0 | 0 |
| | The software shall proceed according to ethical standards. | 16 | 9 | 0 | 0 |
| | The software shall ensure the minimization of fault-tolerance. | 4 | 18 | 0 | 0 |
| | The software shall include control/monitor processes for data input. | 0 | 18 | 2 | 0 |
| | The software shall be developed in connection to version controls. | 4 | 9 | 4 | 1 |
| **SECURITY** | The software shall provide critical security update functionalities. | 12 | 6 | 4 | 0 |
| | The software shall ensure protection against data loss (human errors). | 8 | 15 | 0 | 0 |
| | The software shall ensure protection against data corruption (human errors). | 16 | 6 | 2 | 0 |
| | The software shall include an authorized user login. | 16 | 6 | 2 | 0 |
| | The software shall be restricted in its functionalities according to EU law. | 16 | 9 | 0 | 0 |
| | The software shall ensure secure data transfer processes. | 16 | 9 | 0 | 0 |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
|  | The software shall ensure secure data storage. | 8 | 15 | 0 | 0 |

**Table 2.** Heatmap of weighted Requirements

The summary comparison of both surveys reflects an increase in the perceived importance of several software requirements. The 'very important' classification has become more prevalent in the second survey compared to the first. Notably, requirements such as ensuring the correct execution of code, writing error-free code, user interface intuitiveness, and proper processing of user input have all seen an uptick in their relative importance, moving from 'important' or 'relatively important' classifications to being considered 'very important' by the respondents. This shift indicates a growing emphasis on user experience and error reduction in software development. The consistency of data formats and the prevention of software from being harmful to other components maintained their 'very important' status, with a 92% relative importance, indicating a steady recognition of their critical nature. The requirement for the software to ensure protection against data corruption due to harmful events continues to hold the utmost importance, with a consistent 100% relative importance and 'very important' classification across both surveys. Ethical standards in software, protection against data corruption due to human errors, inclusion of authorized user login, and restriction of functionalities according to EU law have all seen an increase in their relative importance, solidifying their 'very important' classification. Lastly, ensuring secure data transfer processes remains a top priority with a consistent 96% relative importance and 'very important' classification, underscoring the continuous and unwavering focus on data security.

|  | Second Survey |  | First Survey |  |
|---|---|---|---|---|
| Requirement | Relative Importance | Classification | Relative Importance | Classification |
| The software should ensure the correct execution of code | 100% | very important | 88% | important |
| The software should be written in error free code | 92% | very important | 77% | relatively important |
| The software should be intuitive to use | 92% | very important | 85% | important |
| The software should proceed user input in a proper way | 92% | very important | 85% | important |
| The software should ensure consistent data formats | 92% | very important | 92% | very important |
| The software should not be harmful to other components (Workload) | 92% | very important | 92% | very important |

| | | | | |
|---|---|---|---|---|
| The software should ensure protection against data corruption (harmful events) | 100% | very important | 100% | very important |
| The software should proceed according to ethical standards | 96% | very important | 88% | important |
| The software should ensure protection against data corruption (human errors) | 92% | very important | 88% | important |
| The software should include an authorized user login | 92% | very important | 88% | important |
| The software should be restricted in its functionalities according to EU law | 96% | very important | 96% | very important |
| The software should ensure secure data transfer processes | 96% | very important | 96% | very important |

**Table 3.** Comparison of most important Requirements of D1.10 and D1.6

The comparison of the least important requirements between the two surveys indicates a significant shift in the perception of importance for several software requirements. In the current case, the requirement for the software to behave correctly in interaction with other solutions and to ensure its integration with other software systems saw a considerable decrease in relative importance, dropping from 'very important' with a 92% rating in the first survey to being classified as 'least important' in the second survey. Similarly, ensuring appropriate storage capacity also saw a decrease, moving from 'important' with an 88% rating to 'least important'. The requirement for the software to ensure proper data transformation processes also experienced a decline in relative importance, moving from 'relatively important' at 77% to 'least important'. Additionally, the need for software to be developed in connection to version controls was downgraded from 'relatively important' at 73% to 'least important'. In contrast, the relative importance of the software only using appropriate and established data formats and the requirement for the software to update itself for its environment remained largely consistent, maintaining their status as 'least important' in both surveys, with a slight variation in their percentage ratings.

| | Second Survey | | First Survey | |
|---|---|---|---|---|
| Requirement | Relative Importance | Classification | Requirement | Relative Importance |
| The software should only use appropriate and established data formats | 65% | least important | 62% | least important |

| | | | | |
|---|---|---|---|---|
| The software should behave in interaction with other solutions as intended | 58% | least important | 92% | very important |
| The software should ensure appropriate storage capacity | 58% | least important | 88% | important |
| The software should ensure proper data transformation processes | 69% | least important | 77% | relatively important |
| The software should (automatically or manually) update itself for its environment | 62% | least important | 65% | least important |
| The software should ensure its integration to other software systems | 69% | least important | 92% | very important |
| The software should be developed in connection to version controls | 69% | least important | 73% | relatively important |

**Table 4.** Comparison of least important Requirements of D1.10 and D1.6

The analysis of the two tables comparing the relative importance and classification of software requirements from the first and second surveys provides several insightful conclusions:

1. **levation of Certain Requirements:** There has been a marked increase in the perceived importance of fundamental software requirements between the two surveys. Requirements such as the correct execution of code, error-free coding, user interface intuitiveness, and the ethical standards of software have seen a rise in their relative importance. This suggests a growing focus on the quality, user experience, and ethical implications of software development.

2. **Consistency in Top Priorities:** Some requirements, like protecting against data corruption due to harmful events and ensuring secure data transfer processes, have consistently remained 'very important' with high relative importance ratings across both surveys. This consistency underlines the continuous emphasis on security and reliability as non-negotiable pillars of software systems.
3. **Downgrading of Certain Requirements:** Conversely, some requirements have seen a significant decrease in relative importance. Notably, the ability of the software to integrate with other systems and to behave as intended in interaction with other solutions was downgraded from 'very important' to 'least important'. This could indicate a reassessment of priorities or an increased confidence in the interoperability of current solutions.
4. **Stability in Lower Priorities:** There are requirements that consistently stayed at the bottom of the priority list across both surveys, such as the use of appropriate and established data formats and the software's ability to update itself. This could suggest that these aspects are considered standard practice, hence not a differentiation point, or that they are overshadowed by more critical requirements.
5. **Shifts in Storage and Transformation Needs:** The requirement for appropriate storage capacity and proper data transformation processes has seen a notable decrease in importance, hinting at a possible reassessment of needs, possibly due to advancements in technology or a better understanding of actual versus perceived needs.

The comparison reflects a dynamic landscape where the significance of certain requirements has evolved, possibly due to shifts in technology trends, regulatory landscapes, or organizational priorities. Furthermore, the data from the second survey points to a heightened awareness and demand for high-quality, user-centric, and ethically aligned software solutions, while showing a potential reassessment or satisfaction in the areas of interoperability and standard functionalities.

## 3.3 Recommendations for Solution Providers

Based on the extensive analyses of pilot partners' feedback and the evolving landscape of software development priorities, the following recommendations are proposed for the solution/software providers of the i4Q projects:

1. **Enhance Reliability and Security:** Prioritize the development of features that enhance the reliability and security of the software. Focus on robust error handling, data protection mechanisms, and compliance with security standards, as these are consistently rated as 'very important'.
2. **Emphasize Ethical Standards and Regulatory Compliance:** Integrate ethical standards into the software development lifecycle and ensure that software functionalities are in strict adherence to EU law and other relevant regulations. The growing importance of these areas suggests a competitive advantage for software that excels in ethical design and regulatory compliance.
3. **User Experience Focus:** Allocate resources towards improving the intuitiveness and user-friendliness of the software. This includes refining user interfaces and ensuring the

software is responsive to user input. The increased importance of these areas highlights the need for a user-centric approach to design.

4. **Data Integrity and Consistency:** Maintain a high standard for data consistency and integrity. Ensure that the software employs consistent data formats and handles data transformations correctly, as these are critical for the overall performance and trustworthiness of the system.
5. **Monitor and Adapt to Changing Priorities:** Stay vigilant to the shifting importance of various requirements. For instance, the decreased emphasis on the software's behavior in interaction with other solutions may suggest a changing technological context or improved confidence in compatibility standards.
6. **Proactive Update Mechanisms:** Despite their consistent lower priority, continue to implement and refine mechanisms for software updates, both manual and automatic, to adapt to changing environments. This is essential for maintaining long-term viability and security of the software.
7. **Version Control and Development Practices:** Re-evaluate the approach to version control and the associated development practices in light of their reduced importance. While they are now rated as 'least important', they remain fundamental to the software development process and quality assurance.
8. **Storage Capacity and Transformation:** Address the decreased importance placed on storage capacity and data transformation processes. Investigate whether this reflects an actual reduction in need or if it suggests a gap between perceived and actual requirements among pilots.
9. **Ongoing Dialogue with Stakeholders:** Maintain an ongoing dialogue with pilot partners and stakeholders to ensure that the software continues to align with their evolving needs and priorities. This will also help in identifying emerging trends and requirements that may not yet be fully recognized in the industry.

# 4. Conclusion

The extensive discourse and analysis presented throughout our exchange offer a comprehensive understanding of the i4Q project's journey in developing trustworthy systems. The project, as detailed in Deliverables D1.6 and D1.10, has been pivotal in shaping an environment that not only meets the stringent criteria of trust and regulatory compliance but also aligns with the dynamic needs and expectations of pilot partners.

Deliverable D1.6, as a foundational document, set a high standard in the assessment of i4Q solutions against trustworthiness and compliance, employing the British Standard BS 10754-1:2018 as a guiding framework. This initial step was crucial in establishing a baseline for the project's alignment with international regulations and best practices. The thorough evaluation of trustworthiness in D1.6 laid the groundwork for continuous improvement and adaptation within the i4Q project. Building upon this, Deliverable D1.10 marks a significant progression in the project. It provides a detailed update on regulatory changes, ensuring that the i4Q systems remain at the forefront of compliance. Moreover, the deliverable's in-depth evaluation of trustworthiness requirements, coupled with the analysis of shifting stakeholder priorities, highlights a nuanced understanding of what constitutes a trustworthy system in the contemporary technological landscape. One of the key findings from these deliverables is the evolving focus on user experience, ethical standards, and regulatory compliance in software development. The growing importance of attributes such as error-free code, intuitive user interfaces, and adherence to ethical standards signifies a paradigm shift towards more user-centered and ethically aligned software systems. Conversely, the decreased relative importance of factors like system interoperability and version control suggests a re-evaluation of priorities, likely influenced by technological advancements and changing stakeholder needs. The project's trajectory, as observed through these deliverables, emphasizes the dynamic nature of trustworthiness in software systems. It reflects an adaptive approach that balances foundational technical requirements with emerging trends and evolving stakeholder expectations. The project's commitment to this holistic approach is evident in the continuous updates, evaluations, and recommendations provided throughout the project lifecycle.

In conclusion, the i4Q project stands as a testament to the importance of developing robust, reliable, and secure systems in an ever-changing technological world. Its focus on aligning with regulatory standards, coupled with a keen awareness of user needs and ethical considerations, positions it as a model for future endeavours in the realm of trustworthy system development. The project's journey highlights the necessity of agility, foresight, and a commitment to excellence in the pursuit of creating systems that not only perform optimally but also earn the trust and confidence of their users.

# References

Bose, R. P. J. C., Singi, K., Kaulgud, V., Phokela, K. K., & Podder, S. (2019). Framework for Trustworthy Software Development. In *2019 34th IEEE/ACM International Conference on Automated Software Engineering Workshop (ASEW)* (pp. 45–48). IEEE. https://doi.org/10.1109/ASEW.2019.00027

British Standards Institution (2018). *Information technology - Systems trustworthiness - Part 1: Governance and management specification* (BS 10754-1:2018).

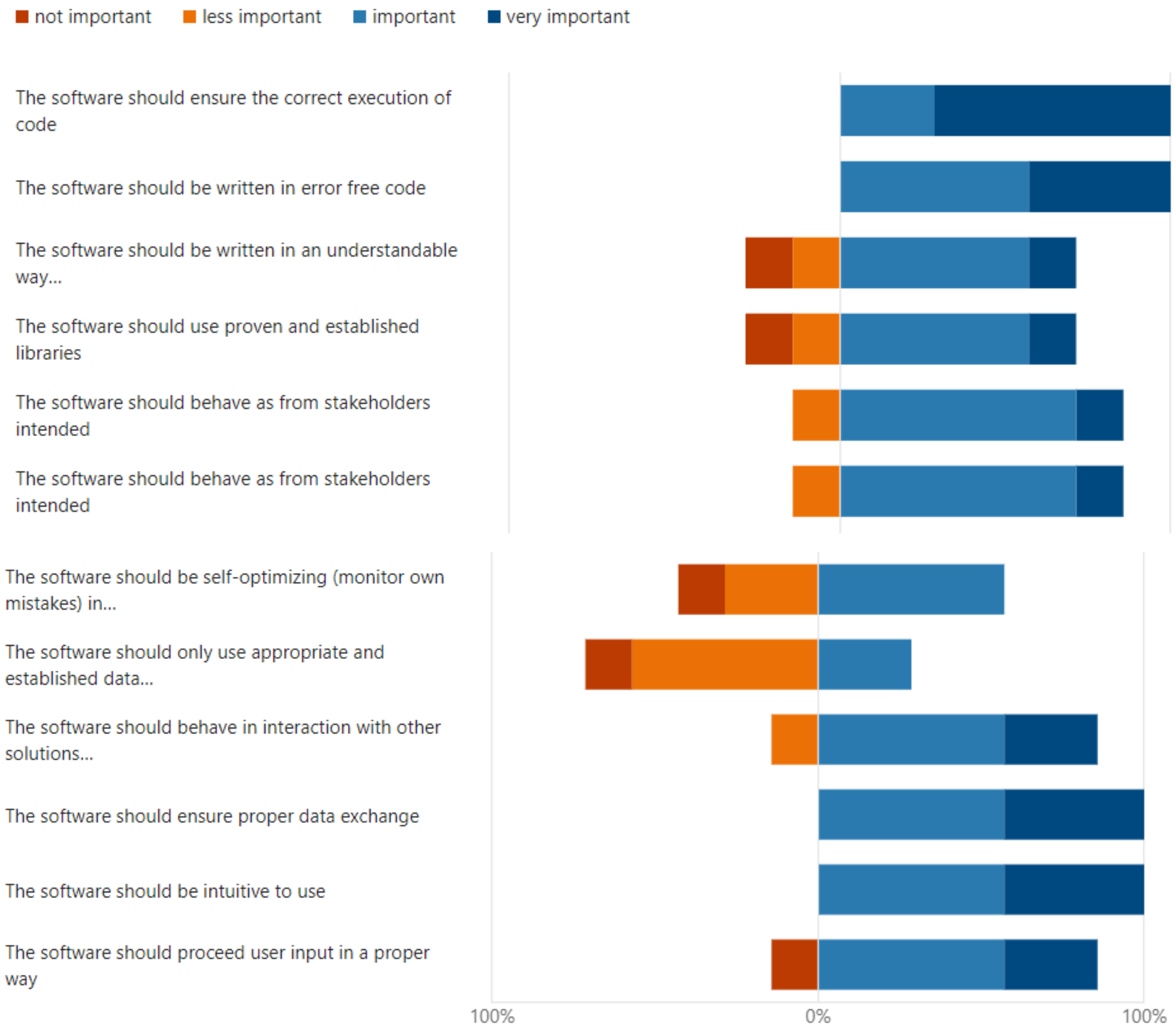
Chyung, S. Y. Y., Roberts, K., Swanson, I., & Hankinson, A. (2017). Evidence-Based Survey Design: The Use of a Midpoint on the Likert Scale. *Performance Improvement*, *56*(10), 15–23. https://doi.org/10.1002/pfi.21727

# Annex

Visual results of the survey.

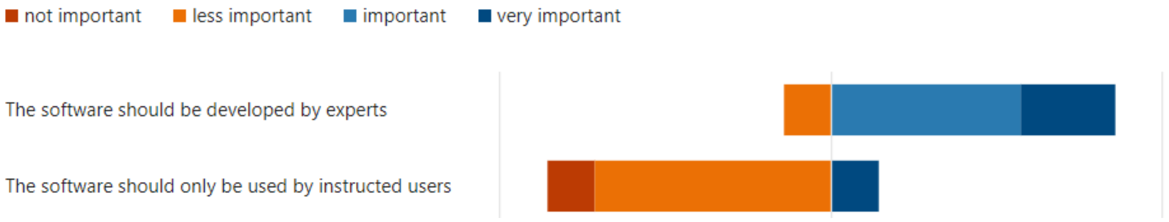
1. Safety *(Correctability, Predictability, Dependency, Usability)*

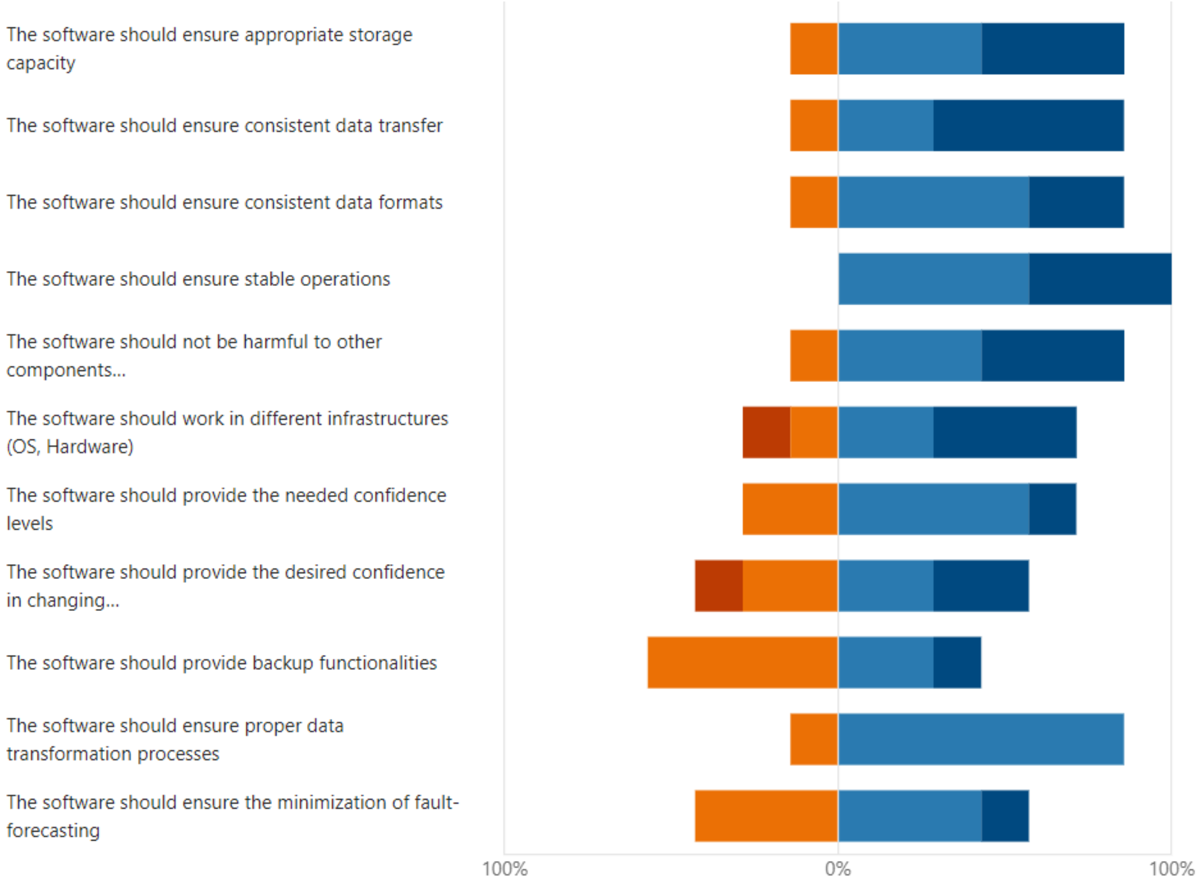
Weitere Details



2. Reliability (*Capability, Consistency, Stability, Certainty, Robustness, Assurance, Credibility, Maintainability)*

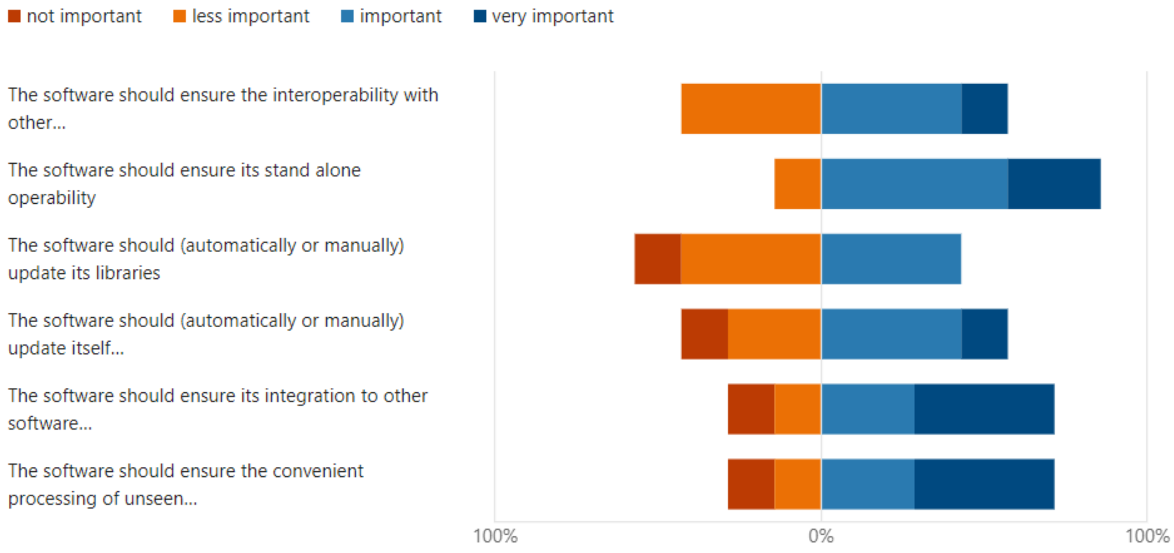
Weitere Details





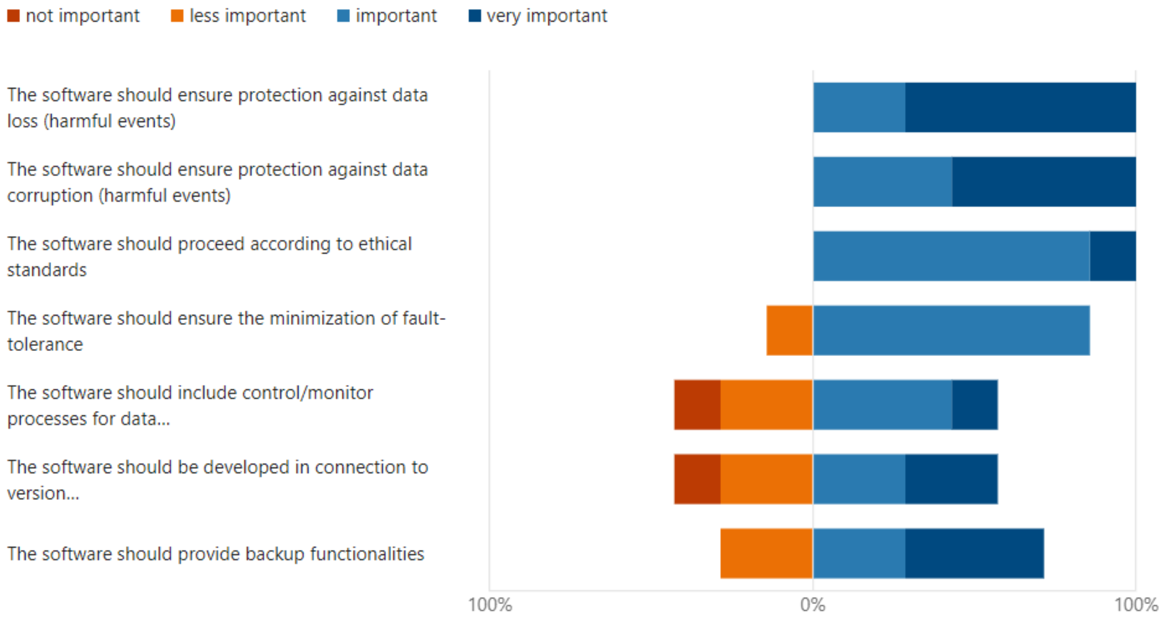
3. Availability *(Dependency, Maintainability, Stability, Survivability, Adaptability)*

Weitere Details



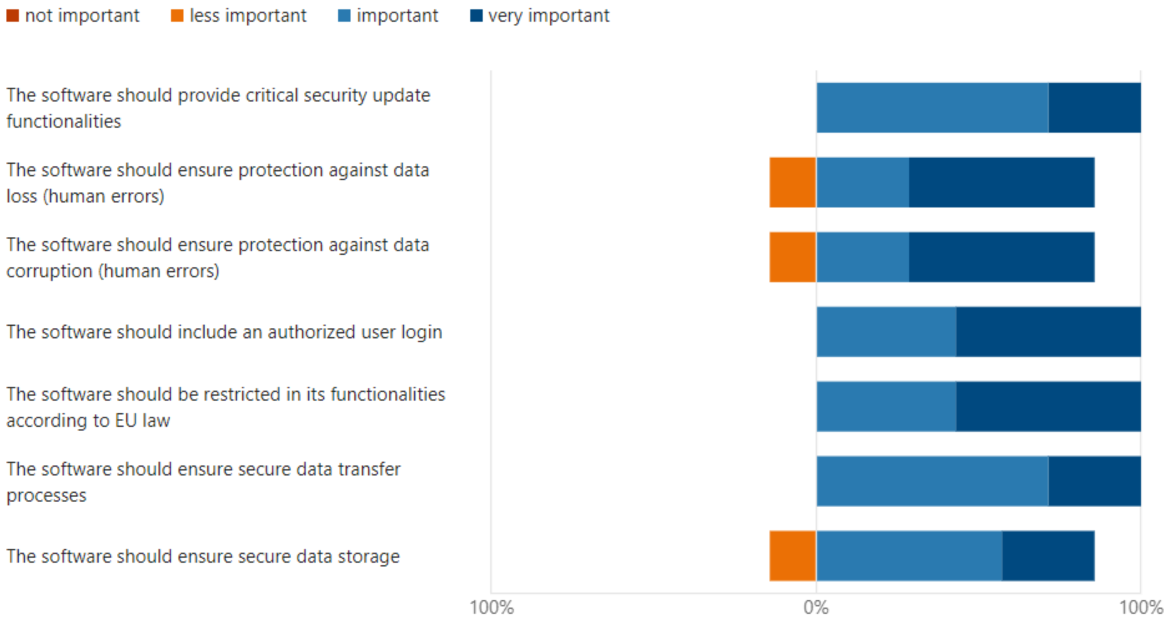
4. Resilience *(Integrity, Robustness, Recoverability)*

Weitere Details



5. Security *(Maintanability, Integrity, Confidentiality)*

Weitere Details


■ not important ■ less important ■ important ■ very important
The software should provide critical security update functionalities
The software should ensure protection against data loss (human errors)
The software should ensure protection against data corruption (human errors)
The software should include an authorized user login
The software should be restricted in its functionalities according to EU law
The software should ensure secure data transfer processes
The software should ensure secure data storage