V2023-09-20 DRAFT https://ib1.org/assurance

Contents

Assurance

Trust Frameworks (TF's) codify and make public the technical and non-technical ('sociotechnical') rules for data sharing agreed by their member organisations. One function of a Trust Framework is to provide appropriate levels of verification and assurance of member organisations and the datasets they publish, covering both Open and Shared data publication.

The Icebreaker One Trust Framework approach provides a baseline requirement for organisation and data assurance.

This document describes the assurance levels for IB1 Trust Framework implementations. Definitions build upon existing examples from the Open Banking Implementation Entity (OBIE), Open Data Institute's (ODI) Open Data Certificates, and draws on both examples and direct experience from using standards and accounting practices.

Organisations are responsible for verifying that they and their data meet the assurance level requirements, including ensuring accurate and complete data. This may subsequently be ratified by machine testing and/or third-party audit.

The assurance approach and needs may vary between TF's. For example, Open Energy may draw on specific regulatory requirements such as UK Ofgem's Open Data Best Practice, whereas Perseus may draw on the specific needs to enable data assurance for compliance reporting.

Peer monitoring and foundations for modes of redress will be addressed in the design of Trust Frameworks. We propose that any member finding an assurance issue

regarding another member should, in the first instance, contact the other member directly to request that the assurance level be made good. In the second instance, we propose contacting partners@ib1.org to raise the issue(s). Over time, the rules of Trust Frameworks will, through a collaborative process, define modes of monitoring, reporting and redress mechanisms, including the potential to eject members from a Trust Framework if they are not compliant with its rules.

Organisational Assurance

Level 1

This is the minimum requirement for organisations to join the Trust Framework. At this level, organisations have:

- Signed the Icebreaker One Membership Agreement
- This includes endorsement of the Icebreaker Principles
- Paid their membership fees
- Demonstrated a current entity legal registration (GLEIF or Companies House) that matches their website and their Icebreaker One membership information
- Registered with the Information Commissioner's Office (ICO) if a UK entity, or international equivalent
- Have named individual(s) within their organisations registered as a "Trust Framework Licence Controller". This individual has legal authority in the organisation to sign, or provide consent to, Open Data or Data Sharing licences on behalf of the legal entity.
- Have named individual member(s) as "Trust Framework Data Controller". This individual is responsible for the technical security and integrity of data sharing (including consent-based access controls where relevant).

Level 2

The organisation meets all the requirements of Level 1, plus they have:

- For Shared Data, publishers or consumers
    - Agreed the Operational Guidelines addendum to the Icebreaker One Membership Agreement
- Published a data strategy that commits to meeting IB1 Dataset Assurance Level 2 for all published data
- Agreed corporate communications to be used for the promotion of the data being shared
- Have commercially reasonable cyber security standards for processing data.

Level 3

The organisation meets all the requirements of Level 2, plus they have:

- Provided 3rd party documentation (e.g. an auditor) to externally confirm/assure ownership and company control.
- Published a data strategy that commits to meeting IB1 Dataset Assurance Level 3 for all published data

- Provided a forum or mailing list for data users (e.g. via an IB1 or 3rd party operated forum)

Level 4

The organisation meets all the requirements of Level 3, plus they have:

- Published a data strategy that commits to meeting Icebreaker One Dataset Assurance Level 4 for all published data
- A dedicated team building user community

Dataset assurance

Each dataset published by a member of a Trust Framework is assessed against the following assurance levels:

Level 1

Assurance that:

- The metadata is available publicly on the web in a location recorded in the organisation's IB1 Registry entry
- Both metadata and underlying data use a machine-readable format
- The dataset contains no personal data and is not subject to GDPR
- For Open Data
    - The dataset is published on the web with a licence that is compatible with Open Data
    - The metadata specifies IB1-O for the Data Sensitivity Class
- For Shared Data
    - The metadata specifies the access conditions for the data
    - The metadata specifies IB1-SA or IB1-SB for the Data Sensitivity Class

Level 2

The dataset meets all the requirements of Level 1, plus assurance that:

- Legal
    - Metadata includes definitions of usage rights for derived data (e.g. a URL to the conditions for derived data)
    - Metadata includes commercially reasonable citations and/or provenance
    - Metadata includes definitions of potential risks (e.g. a URL to such a definition)
    - Where relevant or required, ensure privacy issues addressed within the published data and the data publication mechanism(s)
- Practical
    - Metadata includes dates of creation and publication
    - Where a dataset covers a temporal range, this is defined in the metadata
    - That the dataset will be maintained and available for a minimum of one calendar year

- Technical
    - Data is published in content-appropriate formats that enable data to be used in an interoperable manner by machine-based systems
    - For Shared Data, the dataset is immediately available via a FAPI endpoint to any IB1 Trust Framework-registered application that meets the terms of that Trust Framework implementation.
- Social
    - Data is documented on publicly available URLs
    - A mechanism is available for people to provide feedback and ask questions (e.g. human technical support)

Level 3

The dataset meets all the requirements of Level 2, plus assurance that:

- Practical
    - A schedule is published at a public URL documenting the process of maintaining the data's availability
    - Commercially reasonable backups are in place
    - A document is published at a public URL detailing the process or data collection, curation, quality assurance and publishing
- Technical
    - Inclusion in the metadata of citation(s) to, the underlying open standard(s) used in publishing content-appropriate data is published in machine-readable format(s)
    - Publication of a single consistent URL, or clear rules for how URLs are constructed, are made to access the dataset
    - machine-readable metadata describing the contents of the dataset is provided (e.g. JSON-LD, CSVW)
    - where data is provided by an API, the API has a machine-readable definition (e.g. OpenAPI)
    - Assurance that the dataset has availability of at least 99.5%.

Level 4

The dataset meets all the requirements of Level 3, plus assurance that:

- Legal
    - The licence terms themselves are machine-readable and available at a persistent URL in a consistent manner
- Practical
    - Quality parameters and processes shall be published in a machine-readable format at a persistent URL in a consistent manner
- Technical
    - Provenance shall be published in a machine-readable format at a persistent URL in a consistent manner
    - URIs shall be used as identifiers within data
    - The dataset has availability of at least 99.9%

How Assurance fits with Trust Frameworks

Data Assurance and Trust Frameworks

Data assurance is a critical component within a trust framework, and it plays a significant role in ensuring the reliability, integrity, and confidentiality of data shared and processed within the framework. Here's how data assurance links with a trust framework:

1. **Data Protection**: Trust frameworks often include policies and standards related to data protection and privacy. Data assurance ensures that the data shared and processed within the framework is adequately protected against unauthorized access, disclosure, or misuse. This includes encryption, access controls, and compliance with relevant data protection regulations.

2. **Data Integrity Assurance**: Data assurance measures help ensure the integrity of data exchanged within the trust framework. Assurance processes and technologies, such as digital signatures and data hashing, can be used to verify that data has not been tampered with during transmission or storage.

3. **Data Accuracy Assurance**: Trust frameworks may include mechanisms for verifying the accuracy of data, particularly in contexts where data quality is critical. Assurance processes can be used to validate the accuracy of data provided by participants within the framework, reducing the risk of erroneous or fraudulent data.

4. **Data Availability Assurance**: Ensuring data availability is crucial within a trust framework, especially for services and applications that rely on timely access to data. Data assurance includes measures to prevent data loss due to system failures, cyberattacks, or other disruptions, thus ensuring data availability when needed.

5. **Data Lifecycle Management**: Data assurance encompasses the entire data lifecycle, from data creation and collection to storage, processing, and eventual disposal. It ensures that data is managed in a way that aligns with the framework's policies and compliance requirements, reducing the risk of data breaches or non-compliance.

6. **Audit and Monitoring**: Data assurance includes audit and monitoring processes to track and log data-related activities within the trust framework. This helps in identifying and responding to security incidents, policy violations, or breaches promptly.

7. **Data Sharing and Consent**: In trust frameworks that involve data sharing, data assurance includes mechanisms for obtaining user consent for data sharing and ensuring that data is shared in accordance with user preferences and legal requirements.

8. **Compliance with Data Standards**: Trust frameworks often require participants to adhere to specific data standards and formats. Data assurance processes ensure that data exchanged within the framework complies with these standards, promoting interoperability and consistency.

9. **Data Encryption and Secure Transmission**: Data assurance typically includes encryption and secure transmission protocols to protect data while in transit. This helps prevent unauthorized interception and access during data transmission.

10. **Data Governance and Accountability**: Data assurance involves establishing data governance practices and holding participants accountable for their data-related actions within the framework. It ensures that responsibilities for data management and security are clearly defined.

Data assurance is closely intertwined with a trust framework, as it addresses the **trustworthiness of data shared and processed within the framework**. By implementing data assurance measures, trust frameworks can enhance the reliability and security of data-driven transactions and interactions, ultimately contributing to the trust and confidence of participants and users.

Organizational Assurance and Trust Frameworks

Organizational assurance is a critical element within a trust framework, and it plays a significant role in building and maintaining trust among participants in the framework. Here's how organizational assurance fits with trust frameworks:

1. **Trustworthiness of Organizations**: Trust frameworks are often designed to facilitate interactions and transactions between various organizations or entities. Organizational assurance assesses and verifies the trustworthiness of these participating organizations. It evaluates factors such as the organization's reputation, compliance with security and privacy standards, and its track record in trustworthy behavior.

2. **Identity Verification**: Organizational assurance includes processes for verifying the identity of participating organizations. Just as individuals' identities are verified within a trust framework, organizations' identities are also subject to validation. This ensures that the organization claiming to be a participant is, indeed, who they say they are.

3. **Security and Compliance**: Trust frameworks typically define security and compliance standards that participating organizations must adhere to. Organizational assurance evaluates the extent to which these organizations comply with these standards, ensuring that they meet the framework's security and compliance requirements. This may involve security audits and assessments.

4. **Data Handling Practices**: Organizational assurance includes an assessment of how participating organizations handle data, particularly sensitive or personal data. It

evaluates data protection measures, encryption practices, access controls, and data governance procedures to ensure that data is handled securely and responsibly.

5. **Service Level Agreements (SLAs) and Contracts**: Trust frameworks often involve contractual agreements between participating organizations. Organizational assurance ensures that these contracts and SLAs are adhered to and that organizations fulfill their obligations as agreed upon in the framework.

6. **Reputation and Track Record**: Trust frameworks may take into account the reputation and track record of participating organizations. Organizational assurance considers factors such as previous data breaches, legal disputes, or incidents that may affect an organization's trustworthiness.

7. **Interoperability and Compatibility**: Organizational assurance helps ensure that participating organizations can work together seamlessly within the framework. This includes assessing their systems' interoperability and compatibility, which is crucial for the success of cross-organizational transactions.

8. **Accountability and Redress**: In cases where issues or disputes arise, organizational assurance includes mechanisms for holding participating organizations accountable. It also defines procedures for addressing grievances and resolving disputes in a fair and transparent manner.

9. **Auditing and Monitoring**: Organizational assurance involves ongoing auditing and monitoring of participating organizations to ensure that they continue to meet the framework's trust and security requirements. This helps maintain the trustworthiness of organizations over time.

10. **Trust Authorities**: In some trust frameworks, trust authorities or oversight bodies may play a role in providing assurance about the participating organizations. These authorities may grant certifications or trust marks to organizations that meet specific criteria.

In summary, organizational assurance is an integral part of trust frameworks as it focuses on evaluating and verifying the trustworthiness, security, and compliance of the organizations that participate in the framework. By providing assurance about the reliability and integrity of these organizations, trust frameworks can instil confidence and trust among participants and users, ultimately enhancing the success and effectiveness of the framework.

What is a Trust Framework?

A **Trust Framework (TF)** represents a set of standards, policies, and technologies that facilitate secure and trustworthy interactions among individuals, organizations, and systems in a digital environment. Trust frameworks are essential for establishing and maintaining trust in various contexts, particularly in the realm of digital identity, authentication, and data sharing. Here are some key components and aspects of a trust framework:

1. **Identity Verification**: Trust frameworks often include mechanisms for verifying the identity of entities participating in digital transactions. This may involve various forms of identity proofing, such as document verification, authentication, or knowledge-based authentication.

2. **Authentication and Authorization**: Trust frameworks define protocols and methods for authenticating users or systems and granting them appropriate access rights based on their verified identities. This ensures that only authorized individuals or entities can access specific resources or services.

3. **Privacy and Data Protection**: Where relevant, Trust frameworks can incorporate privacy principles and data protection measures to safeguard individuals' personal information. This includes compliance with data protection regulations like GDPR or HIPAA.

4. **Interoperability**: Trust frameworks often promote interoperability by establishing common standards and protocols that enable different systems and organizations to work together seamlessly. This is crucial for cross-border transactions and collaboration.

5. **Compliance and Certification**: Many trust frameworks require participants to adhere to certain security and privacy standards. Compliance is often assessed through certification processes to ensure that organizations meet specific trust and security requirements.

6. **Trust Authorities**: Trust frameworks may involve the presence of trusted entities or authorities that oversee and enforce the framework's rules and standards. These authorities play a role in maintaining trust and resolving disputes.

7. **Digital Signatures and Encryption**: Trust frameworks commonly include cryptographic techniques like digital signatures and encryption to ensure the integrity and confidentiality of data exchanged in digital transactions.

8. **Audit and Accountability**: Trust frameworks often include mechanisms for auditing and tracking digital transactions to ensure accountability and traceability.

9. **Revocation and Suspension**: Trust frameworks establish procedures for revoking or suspending trust credentials or privileges in case of security breaches or non-compliance.

10. **User Consent**: Some trust frameworks require explicit user consent for data sharing and transactions, emphasizing the importance of informed and voluntary participation.

Trust frameworks are critical in various contexts, such as digital identity management, the exchange of electronic records, financial services, and secure data sharing among organizations. They help build confidence and trust in the digital ecosystem, enabling safe and secure online interactions while protecting individuals' privacy and security.