

## Definitions

In this publication we use a number of key terms in a particular way. These terms are identified and defined below.

**Accuracy:** includes concepts such as correctness and precision of calculation, measurement or estimation as well as consistency of processing over time and across items

**Change:** one of three stages of the system and **Information lifecycle** (the others being **Creation, Operation and Use**) used to organize risks in this publication; includes replacement of a pre-existing organizational element, business practice, infrastructure, or software with a revised version; also includes departure or replacement of personnel, archiving and destruction of information

**Completeness:** the completeness of processing, including all the time periods, data items and attributes of the data items required for the intended purpose as well as the **Metadata** with the **Contextual Information** required to understand the **Information**

**Complexity:** presence of a large number and/or variety of interacting components

**Content:** all types of data used to generate **Information**, including **Raw Data**, sensor data, semi-processed **Information**, **Metadata**, and parameters

**Contextual Information:** see **Meta-information**

**Control:** feature or activity that monitors and checks elements of content, processing or the IS environment against criteria to prevent, detect or correct **Information Integrity** impairments; can be thought of as the tactical subset of enablers whose role is to monitor and check whether other enablers are properly designed and implemented, are operating effectively and are updated as required

**Creation:** one of three key stages of the system lifecycle (the others are **Operation and Use** and **Change**) used to organize risks in this publication; consists of activities such as definition, design, acquisition, development and deployment

**Currency:** evaluated relative to the time period or cut-off date of the **Information** relative to its purpose and the timing of its use

**Data:** a recorded set of qualitative and quantitative measurements of the characteristics or attributes of events and instances; may be presented in various formats, ranging from structured alphanumeric data to unstructured text to audio to images (see **Raw Data**)

**Data quality:** a label for a variety of concepts describing desirable attributes of data ranging from relevance and usefulness to integrity; at a minimum, the level of completeness and accuracy of valid data captured and processed for a specific purpose

**Downstream:** the subsequent use of current **Information** (see **Upstream**)

**Enabler:** component, feature or practice associated with the content, process or IS environment domain that contributes to **Information Integrity**

**Event:** category of occurrences to be captured by a system of business rules

**Event Instance:** actual and particular occurrence of the event type to be captured

**Fit for purpose:** relevant for its actual or intended use; applicable, clear, understandable, and at an appropriate level of granularity or aggregation

**Information activities:** individual components or tasks that aggregate into a process (see **Process**).

**Information:** data presented to a user in a meaningful context for a given purpose (see **Data** and **Raw Data**)

**Information assurance:** incremental **Information** or **Meta-information** attached to subject matter that serves to increase the confidence of a user in the integrity of that subject matter

**Information governance:** policies, standards, procedures and other mechanisms established by the board of directors and executive management to make **Information Integrity** a high priority within the organization

**Information integrity impairment risk:** see **Risk**

**Information Integrity: Representational Faithfulness** of the **Information** to the condition or subject being represented by the **Information**

**Information lifecycle:** the process running from the **Creation of Information** out of **Raw Data** to its retirement (archiving or destruction); in this publication: creation, operation and use, and change (including retirement, permanent archiving, anonymization or destruction)

**Information processing lifecycle:** a part of the overall **Information lifecycle**, including the following phases:

- a) input: creation or identification of **Data**, observation or measurement, documentation or recording
- b) processing: analysis, calculation, transformation or aggregation (to transform data into information)
- c) storage or archiving
- d) periodic updating
- e) output display, transmission and distribution
- f) use
- g) archiving, anonymization or destruction

**Information quality:** a label for desirable attributes of **Information**, including relevance,<sup>1</sup> usefulness and **Representational Faithfulness**<sup>2</sup>

**IS Environment:** all elements of the supporting organizational infrastructure relied upon by the processing domain, including policies, standards, procedures and IT services

**Metadata:** describes the content, context and structure of **Raw Data** before it is turned into **Information** (e.g., description, purpose, origin, used by, owned by, custodian/steward, standard, classification for security/privacy, access privileges, location, version, date/timestamp, retention/disposal requirement, lineage/audit trail, assurance) (see **Meta-information** and **Raw Data**)

**Meta-information:** enables information processing systems to maintain information integrity during processing and for users to understand and use information appropriately; the context for understanding “processed data” (see **Metadata**)

**Operation and Use:** one of the three stages of the system and **Information life cycle** (the others being creation and change); business activity that involves the use of content, **Information**, or systems

**Process:** all activities that transform a collection of inputs (e.g., **Raw Data** or other items from the content domain) into outputs and store them for subsequent use in processing or reporting

**Processing Integrity:** completeness, timeliness, accuracy and validity of system processing in the context of the aim or purpose of the system and its intended users (see **Information Integrity**)

**Raw Data:** data requiring further processing to be useful (see **Information**)

---

<sup>1</sup> According to FASB (2010), relevant financial information is capable of making a difference in the decisions made by users. Information may be capable of making a difference in a decision even if some users choose not to take advantage of it or already are aware of it from other sources. Financial information is capable of making a difference in decisions if it has predictive value, confirmatory value, or both.

<sup>2</sup> COSO (2013) identifies the following determinants of information quality: timely, current, accurate, complete, accessible, protected, verifiable, retained.

**Representational faithfulness (of information):** a depiction connected to the actual phenomena<sup>3</sup> (or the conformity of **Information** to the item to which it corresponds). According to FASB (2010), to be a perfectly faithful representation, a depiction must be complete, neutral, and free from error. In this publication, representational faithfulness of **Information** is determined with reference to whether it is complete, current, accurate and valid. These characteristics must be assessed in the context of the intended or actual use of the **Information** (see **Processing Integrity**)

**Relevance (of Information):** applicability to the purpose for which the **Information** is created; has the capacity to make a difference to users' decisions based on that **Information**

**Risk (of information integrity impairment):** may undermine or threaten one or more of the core attributes of **Information Integrity**; can arise from intentional malicious acts or unintentional errors; and are organized into the three information system and **Information Lifecycle** phases: creation, operation and use, and change

**Risk magnifier:** a factor that magnifies a risk (e.g., complexity, nature, malicious intent, etc.)

**Subject/Subject matter:** set of phenomena (i.e., conditions, events or instances) about which **Information** and accompanying **Meta-information** are provided

**Subject matter information: Information and Meta-information** that portray a subject/subject matter based on the observation, evaluation, measurement and representation of the subject matter (against criteria)<sup>4</sup>

**Threat (to Information Integrity):** arises from internal and external sources; may come from people, technology and the environment; may stem from intentional and unintentional actions (see **Risk**)

---

<sup>3</sup> FASB, *Conceptual Framework for Financial Reporting: Objective of Financial Reporting and Qualitative Characteristics of Decision-Useful Financial Reporting Information* September 2010.

<sup>4</sup> Adapted from *International Auditing and Assurance Standards Board Handbook of International Quality Control, Auditing Review, Other Assurance, and Related Services Pronouncements* Volume 1, 2012.

**Timeliness: Information** available in time to be used for its intended purpose

**Understandability (of Information):** appropriate level of detail or aggregation, labelling and contextual **Information** for the intended use

**Upstream:** the **Creation** and/or previous processing of current information (see **Downstream**)

**Usefulness/Usability (of Information):** sufficient understandability, relevance and integrity for the purpose for which the **Information** is intended

**Validity: Information** that represents what it purports to represent; results from authorized processes, complies with policies, laws and regulations, is properly formatted, authentic, traceable to its source(s) and its ultimate destination, verifiable and free from bias