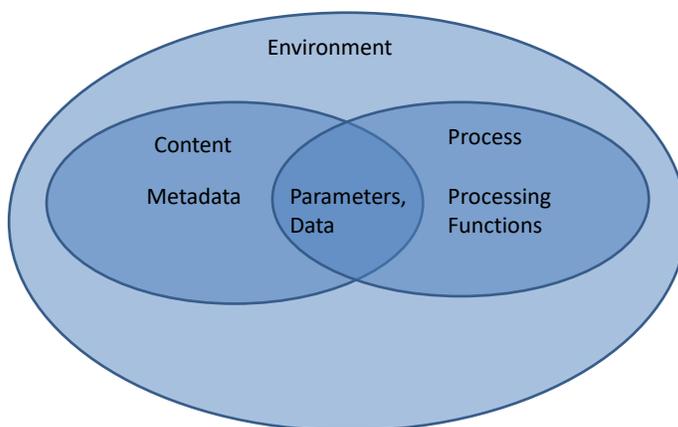


Chapter 8 Content Domain Information Integrity Enablers and Controls

Overview

Content consists of metadata, parameters and data. Processes act on content. Metadata is created and updated by dedicated *content management* process(es) in the environment that are different from those used for information and data processing. Information and data processing functions such as input, processing, output and storage utilize parameters, data and metadata and update the metadata as required.

Figure 8.1
Relationship between Content, Process and IS Environment



Content domain enablers include the inherent characteristics of various types of content, the characteristics of the types of media used, content creation and change procedures, the types of metadata associated with the information and metadata creation and change procedures. All of these, in turn, depend on associated process domain and IS environment domain enablers and controls.

Types of Content

Content domain enablers must be sensitive to the nature of the content which can range from parameters, to raw data, semi-processed data, output reports and structured data such as transactions, unstructured data such as email and contracts.

Content Creation and Change Management Procedures

Content creation and change management procedures (i.e., content definition, design, development and deployment) can contribute to the content's fit for its purpose. Proper labelling, granularity and aggregation based on an understanding of users' information requirements are some of the design features that can contribute to transparency, understandability and usability of content. These features, in turn, can contribute to the completeness, currency, accuracy and validity of information.

As discussed below under the headings *Link to the process* and *Link to the environment*, content in the form of output is the product of a process and both are products of the enablers in the environment that seek to ensure that content fits its purpose and possesses information integrity.

Types of Metadata

Metadata, or information about information, is an important enabler of information integrity. Metadata is data that describes the content, context and structure of information. There are three types of metadata:

- Explicit metadata that is attached to the content
- Explicit metadata that is a central part of the process (e.g. logs) but that is not part of the reported content
- Implicit metadata that provides the context for understanding the content

Metadata can be attached to content (e.g., header and trailer labels on a file), linked to content by hyperlinks (e.g., XBRL taxonomies and linkbases), or reside separately from the content in data

dictionaries, policies and procedures manuals, system documentation, standards, laws and regulations. Some metadata is not explicitly stated but rather is implicit in cultural and linguistic practices, customs and norms.

The description of the content identifies the nature of the information and its purpose (e.g., a stream of sensor data, a set of transactions, a list of accounts receivable). The context information describes the business process(es) to which the information relates, relevant parties to a transaction (i.e. source, intended destination, channel, owner, custodian, etc.) and the duration or instant in time that the information relates to. The information about structure describes the logical and physical organization of information, and the format of and relationships between its elements. Table 8.1 highlights key elements of metadata.

Table 8.1
Key Elements of Metadata

Element Name	Description
Description	Nature of the information.
Purpose	Primary use of the content.
Origin	Identifies the source of the information (e.g. internal, external, etc.) and provides necessary data lineage information.
Used by	Indicates all parties (primary, secondary, etc.) that use this information.
Owned by	Lists the department or individual that is accountable and responsible for the information (e.g. business unit owner).
Custodian/Steward	Individual that is the handler of the information (e.g. the Database Administrator).
Standard	The official convention, which the meta-data adheres to (e.g. Universal Product Code, serialized global trading identification number (SGTIN), etc.)
Classification for security/privacy	Indicates the security/privacy label assigned to the information (e.g. public, internal, confidential, etc.).
Access privileges	Identifies the level of access or authorization credentials required to access the content.

Element Name	Description
	Usually, linked to security/privacy classification of the information.
Location	Identifies the geographic location or department that the information originated from.
Version	Indicates the iteration of document or content to enable version control.
Date/Timestamp	Identifies the date and time the content was generated and/or modified.
Retention/Disposal Requirement	Identifies the duration that the information is to be retained for and indicates when it is to be disposed of.
Lineage/Audit trail	Provides details to allow the tracing of the information back to the source.
Assurance	Indicates the level of verification that the content has undergone.

As can be seen from the items listed above, metadata contributes to the security, availability, understandability, consistency and verifiability of information. There is almost no limit to the amount of information that can be captured about information. The above list is intended to be a set of concise but comprehensive items that can be used to manage information integrity.

Metadata Creation and Change Management Procedures

Metadata creation and change management procedures determine what metadata is required to convey information about the integrity of the information and to support information integrity objectives. Therefore, effective metadata creation and change management procedures are a content domain enabler of information integrity.

As discussed below under the headings *Link to the process* and *Link to the environment*, content in the form of metadata is the product of a process and both are products of the enablers in the environment that seek to ensure that content fits its purpose and possesses information integrity.

Types of Media

Content domain enablers must be sensitive to the media used to process the content which can range from tape/disk storage to CD/DVD/Flash memory and paper. There may be important interactions between content and the type of media that the content resides on that affect information integrity enablers, risks and controls.

Media Selection and Management

Media selection and management can contribute to information integrity by ensuring that the selected media are more reliable and tamper proof than an alternative selection.

Link to Process and IS Environment Domains

The information integrity of content is determined by the process that the content is used in and the IS environment that the process operates in. The process life cycle enablers and controls help ensure that the processing sub-phases are properly initiated by authorized procedures, that all actions affecting content and related metadata are in accordance with assigned privileges and that all actions are logged, that processing errors or malicious acts are prevented or detected and corrected, that the content and metadata are transformed, updated, recorded, backed-up, distributed, stored or disposed of as required.

IS environment domain enablers and controls help to ensure that process and content integrity are given priority, that they fit their purpose, are protected against unauthorized access while being accessible to authorized users, are dependable, consistent, verifiable and assured.