Chapter 3 Content Domain Risks

Overview

Example risk statement – The content does not possess the necessary attributes of information integrity to the degree required to effectively support business decisions and related activities.

Content domain risks can arise from:

- flaws in the creation, use and change of the content
- flaws in the creation and management of metadata related to the content
- the process and environment domains that affect the content.

Content domain risks are magnified by complexity, the inherent nature of the content and media used for the content and the presence of malicious intent.

Type of Content

Content can be raw data, semi-processed information, reports and other outputs such as cheques and parameters that control processing and information flows. Also metadata could have a different risk profile from the data that it describes. Incomplete, out of date, incorrect or invalid metadata can lead to information integrity impairments of the content to which the metadata applies. For example, financial statements that are tagged with the incorrect XBRL XML tag will be incorrectly treated by applications that import such data.

Type of Media

The type of media used to record, store and transfer data can affect risk. Content may be provided on tape/disk, CD/DVD/Flash memory, on a display screen, via wireline or wireless signals, and paper. Each of these media is subject to particular risks. Flaws in the creation, use and change of the media can create information integrity risks. In this publication, the emphasis is on reports and other outputs in a finished form that are intended to be used to support decisions and related activities such as performance monitoring. Although the concepts discussed in this section and

illustrated in the tables developed for final form information apply to other types of content the actual tables are limited to final form information. Incomplete, out of date, incorrect or invalid content can lead to the types of consequences enumerated in Table 3.1.

Link to Process Domain

Flaws in the creation, operation and change of a process can result in inappropriate processes or a process that lacks appropriate information integrity enablers and controls. This in turn can make content and related metadata increasingly vulnerable to information integrity impairments.

Link to IS Environment Domain

Flaws in the creation, operation and change of the IS environment can result in an environment that does not have appropriate information integrity enablers and controls. This in turn can create information integrity impairments risks for processes that depend on the environment, the metadata that depend on those processes and the content that depends on all of them.

Risk Magnifiers

Complexity

Complexity factors that may magnify risks in the content domain include:

- Multiple data sources or interfaces with other information systems, outsourcing suppliers and business partners with access to content may complicate information transfers and permit flowthrough of errors from other subsystems through the interfaces.
- Multiple types of entry devices and subsystems increase difficulties of defining data capture steps and ensuring completeness and accuracy of inputs.
- Multiple output and storage devices or media may increase difficulty of understanding the universe of information to be controlled.
- Lack of clarity/transparency/understandability of content increases the risk of misuse and the difficulty of maintaining information integrity.
- A central IT infrastructure that is not tuned to the specific needs of its users but attempts to cater to some common denominator may not address the varying information integrity

needs of multiple business units.

- The existence of several potentially conflicting purposes of content may create difficulties in identifying a primary purpose of content and linking it to specific users, owners, custodians, etc. and this may make it difficult to determine whose requirements rule.

- Inadequate knowledge of external parties' (e.g. suppliers, customers,. outsourcers, etc.) procedures/processes may impede correct creation of content.

- Variety of data formats and numerous standards may make it difficult to achieve consistency in content design.

- Policies, statutes and regulations that vary across business segments and geographic locations may make it difficult to define and design information integrity standards and access privileges to meet all requirements.

- Many users of content may be updating it constantly, creating rollback problems in case of error or system failure.

- There may be varying time clocks for operations in different time zones making it difficult to synchronize information across the enterprise.

- Disposal requirements of some users may conflict with retention requirements of other users for audit or regulatory purposes.

- Tracking lineage may require end-to-end understanding of process, including manual, web-based and other applications.

- Assurance needs of multiple users increases the risk of failing to fully satisfy information integrity requirements of all users of the content.

Inherent Nature of Content

As noted earlier, the type of media used to store or transfer information can affect the level of risk. For example, wireless media, such as a wireless hard drive, can magnify certain data security and availability risks.

Another magnifier of risk is the nature of the content itself. For example, transmitting credit card data is riskier than transmitting the ingredients of donuts sold by a fast food chain. The former can be used for financial gain, while the latter is publicly available information. Another example would be content captured via web-based marketing or sales initiatives, where there is a high risk

of “fraud”. This is where the organization provides access to content if the user gives their information. The user may give incorrect information to avoid being contacted by the organization.

The dynamic nature of some types of content can pose challenges to information integrity. For example, as time passes, customer data (e.g. marital status, addresses, etc.) can change frequently without notice being given to the entity. Beyond this, content retained by an organization regarding its customer, clients, etc. may cease to be relevant when interacting with that individual. For example, a book retailer needs to assess what part of the customer’s transaction history is relevant in predicting what they buy now – a person with children will likely have different preferences than when they were single. Also, content may be sensitive to interpretation errors (language, culture of originator, operator, user, etc.)

Flaws in the creation, use and change of the metadata associated with data can increase vulnerability to information integrity risks.

Malicious Intent

Content can be impacted by unintentional flaws in the process or the environment that impair the information integrity of the content.

Content may also be impacted by intentional malicious acts of tampering with and destruction of content (or the process or the environment).

Table 3.1 illustrates some of the risks by category.

Table 3.1 Examples of Content Domain Risks by Category

		Illustrative Content Domain Risks Organized by Stage of the Information Lifecycle		
Content Category		**Creation**	**Operation**	**Change**
Type of Data	Raw Data	Lack of clarity or consensus in the definition of requirements Unsuitability of design of raw data for the intended use or user Unusability of raw data format Unsuitability of raw data to support business requirements Business, legal and regulatory requirements not identified or not met	Missing or lost raw data. Incomplete or delayed error correction Delayed receipt of raw data Unreliable acquisition of raw data Data management/ custodianship failing Obsolete raw data not appropriately destroyed or removed Compromised integrity of storage sources of raw data Raw data not available or retrievable when needed Unauthorised alteration of raw data Inability to recover or restore raw data in the event of a disaster	Changes in specifications, format or structure of raw data, processes or system environment not reflected in the requirements, design or operation of raw data
	Semi-processed content	Lack of clarity or consensus in the definition of requirements Unsuitability of design of semi-processed content for the intended use or user Unsuitability of semi-processed content to support business requirements Business, legal and regulatory requirements not identified or not met	As above, plus: Incorrect or incomplete aggregation, manipulation, computation, or presentation of semi-processed content Content deterioration when next processing step is removed by time or space from the previous step. Intervention or rework of data	As above

		Illustrative Content Domain Risks Organized by Stage of the Information Lifecycle		
Content Category		**Creation**	**Operation**	**Change**
	Structured content (such as transactions)	Lack of clarity or consensus in the definition of structured content requirements Unusability of structured content format Unsuitability of structured content to support business requirements Business, legal and regulatory requirements not identified or not met Compromised integrity of structured content	As above, plus: Incorrect or incomplete aggregation, manipulation, computation, or presentation of structured content Inappropriate presentation of structured content	As above, plus:
	Unstructured content (such as email and contracts)	Lack of clarity or consensus in the definition of requirements Unusability of unstructured content format Unsuitability of unstructured content to support business requirements Business, legal and regulatory requirements not identified or not met Compromised integrity of critical unstructured content Metadata related to content creation not defined or not enforced Content design does not facilitate spotting errors or omissions in content	As above Duplication leading to confusion in official record Discovery or search compromised Failure to appropriately destroy or remove leading to regulatory no-compliance or legal risk Data storage practices increasing risk of data leakage or loss to the organization	As above Untracked changes leading to confusion of intent or inability to determine final record Content additions, modifications or abandonment not synchronized with metadata changes.

		Illustrative Content Domain Risks Organized by Stage of the Information Lifecycle		
Content Category		**Creation**	**Operation**	**Change**
	Processed Output	Metadata related to content creation, modification or use not defined Content design does not facilitate spotting errors or omissions in content	Incomplete data entry, transmission, processing or output Destroyed or overwritten output Metadata related to content creation, modification or use not enforced Garbled/corrupted transmission Duplicated input, transmission, processing or output Missing or lost processed content Incomplete or delayed error correction Delayed receipt of processed content Data management/ custodianship failing Obsolete processed content not appropriately destroyed or removed Storage sources of processed content not safeguarded Processed content not available or retrievable when needed Unauthorised alteration of processed content Inability to recover or restore processed content in the event of a disaster Processed content deterioration	Content additions, modifications or abandonment not synchronized with metadata changes

		Illustrative Content Domain Risks Organized by Stage of the Information Lifecycle		
Content Category		**Creation**	**Operation**	**Change**
			over time. Intervention or rework of data	
Type of Metadata	Description	Description of content may be incomplete or incorrect due to limited understanding of the enterprise wide use of the information The description of the information may limit its use	Description may limit retrieval of the information or may expose it to insufficient protection	Description may not be updated as frequently as the systems and information
	Purpose	An incomplete definition of content's purposes and requirements will lead to erroneous use of the content or potential abuses of the content and incomplete specifications for other metadata Content may not be suitable for its purpose Granularity of the content may not meet user needs Design flaws are more likely when the purpose of content is not fully understood by the designer Content purpose alternatives not fully explored or identified	Content meant for one purpose may be incorrectly used or applied to other unintended purposes leading to inappropriate disclosure of information or decision errors	Changes to content may render it unsuitable for its original purpose Content may not be appropriately or completely changed to suit revised purpose
	Origin – internal, external	Definition of sources and owners may become incomplete and incorrect Data conversion process not adequately documented	Operations may not be fully under the oversight of a single user (e.g., in a B2B supply chain) leading to errors or frauds caused by the weakest operational link External data may not be complete	Source of content may change but downstream users may not be made aware of this change and its potential impact on the integrity of the content External content providers not

		Illustrative Content Domain Risks Organized by Stage of the Information Lifecycle		
Content Category		**Creation**	**Operation**	**Change**
		Externally provided content may not comply with stated requirements Externally provided content may not be in the proper format Design may omit external sources of information and thus fail to assess the integrity of content provided by both internal and external parties Inadequate design of content conversion process to maintain integrity of source content	or accurate Data conversion errors in details or summary figures Compromised integrity of content at the source of the content, interface between systems or conversion process	advised of needed content changes to suit amended processing
	Used by	Failure to define all users may make it difficult to assess the impact of a flaw, error or fraud Synchronization requirements between parties not defined, incomplete or incorrect Failure to take into account users with different roles (e.g., internal, contract, external, security, etc.) may lead to design of content that does not meet the needs of disparate users	Content used or manipulated by unauthorised users or processes Overrides can permit access to unauthorized users Authorized but unknown users can submit invalid/fraudulent content Processing errors not identified or rectified on a timely basis Error correction procedures not effective	Users may be added or deleted but the metadata may not be amended to record this change
	Owner	Failure to define an owner may make it difficult to implement accountability. Incorrect ownership identified. Shared responsibility between owner, users, and custodian may create accountability problems	Owner may not be able to maintain operational oversight of the content Owner not aware of the use or manipulation of content	Changes in ownership due to organizational structure may not be reflected in the metadata

		Illustrative Content Domain Risks Organized by Stage of the Information Lifecycle		
Content Category		**Creation**	**Operation**	**Change**
		Identified owner is unable to effectively exercise accountability Owner's role and responsibilities not defined, communicated or implemented		
	Custodian/ Steward	Failure to define a custodian of the content may lead to abdication of responsibilities for content monitoring and correction Failure to design the custodian's/ steward's duties with respect to the content may lead to ineffective monitoring and error correction Failure to design the custodian's/ steward's duties with respect to the content may lead to loss, destruction, or corruption of content	Errors and omissions by the custodian may permit errors and abuses of the content	The custodian/steward may change but the metadata may not record the change giving a false impression that stewardship continues as before The custodian/ steward may not be advised of a change to the metadata, thereby failing to initiate appropriate custodianship changes
	Standard	Failure to define a set of standards may lead to selection of weaker standards or no standards being used in design of content Lack of effective standards by which to gauge content suitability Standard may not be adhered to during design, development of the content detracting from effective use of content for its intended purpose	Failure to monitor and enforce compliance with standards may lead to inconsistent adoption	Standards may change or may no longer fit changed circumstances, but these changes may not be communicated to content designers or users

		Illustrative Content Domain Risks Organized by Stage of the Information Lifecycle		
Content Category		**Creation**	**Operation**	**Change**
	Classification for security	Content not classified Failure to consider the most stringent user's needs may permit too broad access to content and may fail to comply with policies, regulations or statues Design of security features not consistent with content security classification Failure to use a sufficiently robust and detailed classification may give an illusion of security while permitting exploitable gaps	Operation of security features not consistent applied in accordance with security classification	Value of content may change but its security classification may not be updated leading to a mismatch between the classification of the content and users' access to the content Changed security features may no longer be effective to provide content security
	Access privileges	Failure to define appropriate access privileges may make content vulnerable to unauthorized access to information, theft, disclosure and tampering Failure to design effective access credentials that prohibit as well as permit access may cause users to work around the intended access privileges May fail to specify who cannot access thus permitting incompatible functions to be performed	Access privileges not enforced consistently or continuously Systems failures or emergencies may permit access to content beyond that normally permitted	Access privileges may be inappropriately amended or not updated on a timely basis Changes that are implemented to other systems or processes undermine existing controls
	Location	Failure to identify access points and content storage locations Location-specific requirements	Systems fail to move content in an effective, trusted and reliable to the intended user	Location of data may change due to a re-organization but metadata may not be not updated to reflect this

		Illustrative Content Domain Risks Organized by Stage of the Information Lifecycle		
Content Category		**Creation**	**Operation**	**Change**
		for availability, continuity, confidentiality and protection of content not defined Failure to design access paths that permit effective, trusted and reliable access and use of content		
	Version management	Failure to define an enterprise wide versioning system to maintain the version of content Failure to design manual and automated version management procedures to ensure the integrity of the versioning	Failure to check for version in each manual and automated process that handles content may lead to omissions, duplications and other errors System delivers the wrong version	Content may be updated frequently but version may not be updated resulting in non-current version information and inconsistent use of content
	Date/ Timestamp	Failure to identify synchronization requirements and a protocol for synchronizing time across multiple time clocks and time zones. Failure to design effective procedures to ensure the accuracy and reliability of date/timestamp or to prevent multiple date/timestamps for the same content.	Date/Timestamp may be overridden. Date/Timestamp procedures do not operate reliably and continuously as designed Content may be updated but its date/timestamp may not be updated	Data conversion procedures related to the implementation of system or process changes may alter, corrupt or delete time stamp
	Retention/ Disposal Requirements	Failure to identify all retentions and disposal requirements for content Failure to design effective manual and automated procedures to enact retention / disposal requirements Failure to deploy effective	Retention / disposal procedures do not operated reliably and continuously as designed resulting in outdated content being used inappropriately	Retention requirements may change due to legal changes but metadata may not be updated leading to potential liability Failure to check retention/disposal requirements for content when hardware and media are reassigned, recycled or disposed

		Illustrative Content Domain Risks Organized by Stage of the Information Lifecycle		
Content Category		**Creation**	**Operation**	**Change**
		manual and automated procedures to enact retention / disposal requirements		
	Lineage/ Audit trail	Lack of definition of requirements of important points in the audit trail Difficult to trace content processing through the audit trail Failure to capture audit trail information in all processing steps	If operations fail then lineage tracking may also fail at the same time Gaps in the audit trail The audit trail may be tampered with or overwritten if it is not protected	New uses may be added to content but audit trail not effectively amended Content as an intermediate input may not be recorded, leaving a gap in the audit trail
	Assurance	Assurance needs of more stringent users not effectively defined Assurance procedures not enacted to satisfy the assurance requirements Assurance reports may be too general to provide specific assurance on content used for specific decisions	Assurance procedures do not operate reliably and continuously as designed Assurance process may fall prey to sampling and non-sampling risks (i.e., drawing a wrong conclusion because sample is not representative of the population or because an assurance procedure is performed incorrectly, respectively)	Assurance that was applicable to a previous period may not be applicable to the current period but the metadata may not be updated to reflect this
Type of Media	Offline media (e.g. CDs, DVDs, tapes, etc.)	Media characteristics not suitable or appropriate for the intended use or user. For example: Media (e.g. CD, tape, etc.) is not suited for rate/volume of transactions generated Media is not suited to capture transactions in real time	Content is inaccessible due to media's susceptibility to environmental risks (magnetic waves, humidity, etc.) Where media is re-used for backup purposes, incorrect "unit" (e.g. tape) is erased Content cannot be accessed due to poor labelling/inability to identify	Media fails to capture content due to changes in upstream job scheduling/ processing Changes in specifications, format or structure of content, processes of system environment not reflected in the requirements or design of media

		Illustrative Content Domain Risks Organized by Stage of the Information Lifecycle		
Content Category		**Creation**	**Operation**	**Change**
		Media lacks access management features to prevent unauthorized changes to data Lack of clarity or consensus in the definition of media requirements Unusability of media for content format Labelling or version identification standards are poorly designed Job schedules and processing logic (i.e. that record data on media) are poorly designed	media Inappropriate media used for presentation of content Media is lost or stolen Media deteriorated Archived media cannot be restored due to changes in infrastructure	
	Online media (e.g. servers, Network Storage Devices, etc.)	Media (e.g. server, NAS, etc.) is not adequate for the storage demands of the system Storage device is poorly integrated into the system Stored data and information not effectively organized	Electronic data stored on storage is not organized Data not readily retrievable when needed	Changes to the storage devices are not properly planned, tested or implemented
	Display Screen	Display of images is defined for older versions of software Screen design does not facilitate spotting errors or omissions in content Output does not display on all browsers (e.g. Firefox) Poor user manuals, poor training Content from screen can be viewed by unauthorized users	Images is displayed in an unreadable format	Formatting changes in HTML script prevent the images from being viewed

		Illustrative Content Domain Risks Organized by Stage of the Information Lifecycle		
Content Category		**Creation**	**Operation**	**Change**
	Paper	Paper, as a storage medium, is not suited for long term storage (i.e. prone to biodegradation) or harsh environmental conditions (e.g. humidity, fire, etc.) Paper cannot be easily "mirrored" as electronic formats of data can be Labelling or version identification standards are poorly designed Fonts and colours schemes (e.g. RGB vs CMYK) used are not supported in printing technology resulting in presentations that are useable on screen, but are unusable when printed	Content is inaccessible due to paper's susceptibility to environmental risks (humidity, biodegradation, etc.) Content cannot be accessed due to poor filing standards Organization does not maintain filing standards Information is inaccessible for employees who are not physically located near the information	System changes are not reflected in output process resulting in print jobs outputted to incorrect paper sizes
Link to the Process that the Content is used in		Omission of required processing steps may result in incomplete, delayed or incorrect content Flaws in interface design/poor integration of multiple systems/subsystems Errors in design of processing steps may permit errors in content such as lost or delayed content, garbled transmission and errors	Errors and delays in execution of processes may lead to errors in content Errors in one phase may flow through to other phases and ultimately into the content	The process may change but this change may not be assessed for its impact on the content Conversion of data to new format or medium may result in omissions of previous data or insertion of unauthorized new data
Link to the Environment that the Content is used in		Requirements definition errors during system development may affect processing integrity	Operations errors during system processing may affect processing integrity	The environment may change but the change may not be assessed for its impact on system

	Illustrative Content Domain Risks Organized by Stage of the Information Lifecycle		
Content Category	**Creation**	**Operation**	**Change**
	Design errors during system development may affect processing integrity and content integrity. For example, the wrong level of granularity or aggregation may detract from clarity/transparent of information and lead to its misuse	Errors may flow from one subsystem to another	processing or content Regulatory changes may require changes in information requirements or processing methods