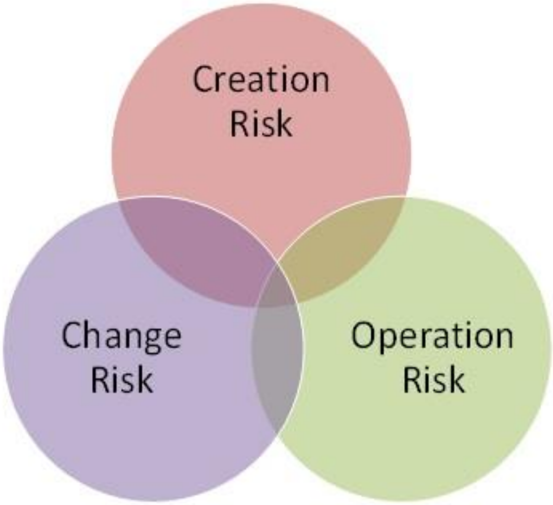
Chapter 2 Information Integrity Risks

Organization of Risks

Risks are threats that can cause information integrity impairments. Risks are found in all three domains and are related to the three main stages of the information and information system lifecycle – Creation, Operation and Use, and Change.1 Due to their sequential relationship these stages can compound risks.

Figure 2.1 Causes of Information Integrity Risks



1

Creation: Definition/Design/Development/Deployment

A key risk associated with the creation stage of information is that the information may be inappropriate for the use for which it is intended – its fitness for purpose. This risk may arise if the attributes of interest of the underlying subject or the environmental attributes and other meta-information may not be observable or measurable. For example, they might be dependent on future events, such as the severity of climate change or may depend on subjective qualitative factors such as people’s tastes in fashion or entertainment. If the uncertainties or subjectivity surrounding the

[1] Nayar, M. And E.G. Flamholtz, “Information Integrity in the Digital Age: A Challenge for the Board” *Management Online Review*, April 2007.

information are not understood, then the information may be misleading or likely to be misunderstood by its intended users. Such risks should be assessed at the definition, design and development phases of information creation to ensure that the information is suitable for its purpose and, in particular that the attribute/characteristic to be reported are not:

- inappropriate representations of the desired information
- incomplete (i.e., missing important attributes)
- out of date (i.e., measured too early or too late)
- inaccurate
- biased
- insufficiently precise for the intended use
- at an inadequate level of aggregation/disaggregation for the intended use
- inconsistent/not replicable (between measurers or between measurements) because of qualitative factors and uncertainty
- inconsistent with laws, norms, policies and other sources

Inadequate **definition** of requirements for information content, processes and IS environments can create insurmountable barriers to information integrity. Definition risks may stem from incomplete or inaccurate understanding of requirements and needs as well as failure to involve the right participants in the requirements determination process.

Risks related to the **design** of information content, processes and IS environments may stem from failure to follow appropriate design methods, failure to involve the right participants in the design process, limitations of the technologies employed, and limitations of human judgment that limit the suitability of a design for a given purpose, incorporate vulnerabilities and flaws in the design,and thereby permit impairments to occur.

Risks related to the **development and deployment** of information content, processes and IS environments may stem from failure to follow appropriate methods to acquire, develop and deploy systems and information, limitations of the technologies employed that result in vulnerabilities and flaws in the systems, failure to involve the right participants in the development and deployment process, and organizational issues that can affect the quality of the outcomes and thereby permit impairments to occur.

Operation and Use

Operation exposes systems and information to errors, malfunctions, malicious attacks, overrides and other circumventions of established procedures, exploitation of vulnerabilities and unforeseen flaws in the design of information content, processes and systems, interruption of established processing sequences and workflows, and entropy (i.e., the natural tendency of all things to deteriorate over time). In this publication, when applied to the process domain, the Operation phase includes the life cycle of particular pieces of information and the risk arising during the following stages of the information processing lifecycle.

- Creation or identification of data
- Observation or measurement
- Documentation or recording
- Input
- Processing, change (including update or synchronization) or aggregation to transform data into information
- Storage or archiving
- Output or retrieval

- Use
- Archiving or destruction

Use risk is the risk that the information will be used for other than its intended purpose, used incorrectly, or not used when it should be. It includes the risk that

a) Someone other than the intended user will make use of the information resulting in a misunderstanding on the part of that user or an erroneous decision. For example, a sale for marketing purposes may not meet the definition of sale defined for tax purposes or financial reporting purposes. Such risks may be addressed by describing the intended user and the intended use of the information in the meta-information provided with the information.

b) An intended user will make use of the information for purposes beyond its intended use or fail to use information for its intended uses resulting in erroneous decision-making or misunderstanding on the part of the user. 2 This may include, inappropriate substitution of available information for unavailable information, inappropriate projection of information to other events/instances, inappropriate combination/transformation/synthesis of information and misinterpretation or misapplication of the information/meta-information. Misinterpretation or misapplication of information could occur if the information supplied is not appropriate for the intended purpose, and/or the meta-information provided is incomplete, erroneous or otherwise misleading. Risks of misinterpretation or misapplication of information by intended users may be addressed by describing the information in related meta-information, designing it to fit its purpose, and ensuring that it possesses information integrity.

[2] This includes failing to use information because it is deemed to be inappropriate; for example, because it is too aggregated or too disaggregated for the intended purpose.

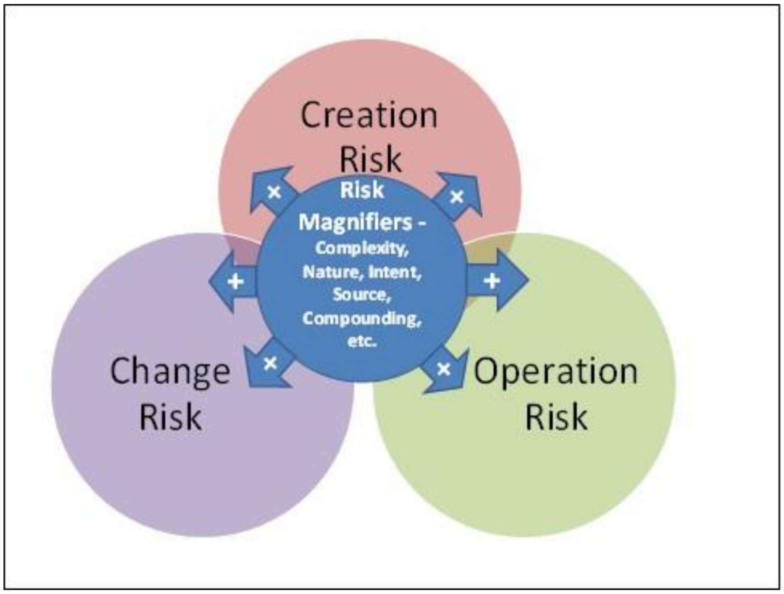
Change

As an entity experiences changes in its organization, business practices, personnel, infrastructure and software, it faces increased risks that systems and processes will deteriorate, that changes will defeat or circumvent existing controls, that current content or information will become irrelevant, or that unauthorized or untested additions or modifications will be made. All of these change-related risks can undermine information integrity. These risks can be addressed by implementing effective change management processes that anticipate, enable and co-ordinate change while preserving information integrity.

Risk Magnifiers

Factors such as complexity, inherent nature of the system, the presence of malicious intent and other factors can magnify the other risks as illustrated by Figure 2.2. These risk magnifiers are not standalone risk categories but rather magnifiers of the risks in the other categories, as discussed below.

Figure 2.2 Magnifiers of Information Integrity Risks


Creation Risk
Risk Magnifiers - Complexity, Nature, Intent, Source, Compounding, etc.
Change Risk
Operation Risk
×
×
+
+
×
×

Complexity

Complexity is usually attributed to the presence of a large number and/or variety of interacting components. Complexity can:

- limit the transparency and understandability of content, process or the information system environment,

- hamper the effectiveness of information system creation, operation and use, and change, and

- increase the challenges of creating effective preventive, detective and corrective controls.

For example, a large number of users of information with conflicting requirements may make it more difficult to define suitable information integrity requirements or to design effective procedures for addressing information integrity risks compared to a less complex setting.

Examples of Complexity Factors That May Magnify Risks

- Multiple data sources can lead to incomplete or conflicting definitions of requirements, incomplete or inconsistent merger of information from the various sources or conflicting changes to processes

- Inconsistencies between many interfaces, systems, and hand-off points can lead to inadequacies in design of processing steps or operations

- Multiple measurement units such as multiple currencies and a variety of units of measure (e.g., metric vs. non-metric measures) can lead to inadequacies in design of processes and related errors in storing and transforming one measure to another

- Special purpose entities, complex financial instruments (e.g. collateralized debt obligations) or non-transparent vehicles can be used to conceal non-compliance or fraud

- Identity theft or masquerading can be used to disguise unauthorized systems changes or transactions

Additional examples of complexity factors and their potential impacts on risks are provided in subsequent sections.

Inherent Nature

The nature or characteristics of the business and system can be risk magnifiers. For example, financial systems may magnify risks of intentional abuse of information during system operation compared to non-financial systems. Similarly, e-commerce systems can magnify risks of information integrity impairments from intentional cyber attacks due to the fact that e-commerce systems are accessible over the World Wide Web, store private and confidential information and process payment information. Companies with frequent changes in operations due to mergers and acquisitions, high turnover in executive management or other reasons may magnify the risks of incomplete or incorrect changes to their systems and information. User developed and maintained systems can magnify risk of information impairments due to the fact that end-users may not have the training, resources or discipline to implement and enforce rigorous system and information creation, operation and use, and change procedures.

Malicious Intent

Each of the categories of risk can arise from intentional or unintentional causes of impairments, as summarized in Table 2.1. An important agenda item for information integrity risk assessments is to avoid assuming that information integrity is well-managed as a starting point for risk assessment or that information processes and systems operate in a benign, non-hostile environment. Making such assumptions at the outset of a risk assessment can bias subsequent analyses and evaluations by making them overly optimistic and lead to an inappropriately low risk profile and implementation of insufficient controls to respond to the risks. For example, the Internet may represent a valuable e-business opportunity for an entity but it also represents a hostile environment for that business due to its openness to threats from unknown and remote attackers.

Table 2.1 Examples of Risks by Type of Intent

Risk	Creation	Operation	Change
Unintentional Error Entropy; human error; acts of nature	Conflicting data definitions lead to errors in reconciliation User requirements omitted or misunderstood Incompatible information needs	Unauthorized alteration during transmission Change in established sequence of activities Interruption of workflow Delay or omission of transmission	Misapplying changes in accounting standards Mistake in uploading new code Delay in payroll table update

Risk	Creation	Operation	Change
	Lacking or out of date policies, standards and expertise User requirements incorrectly implemented Inconsistent data format Combination of incompatible functions	Incorrect classification of information Accidental alteration of information	
Malicious Intent Hacker attack; vandalism; theft; misappropriation of assets; false reporting; bypasses and overrides of required procedures or controls	Out of date processing or environment domain Insecure development practices (e.g. divulges internal system information to unauthorized user) Excessive or inappropriate executive override capability Fraudulent code	Executive override of controls Hacking, viruses Theft of data in transit False information (e.g. stock pump & dump schemes), insider trading, sale of uncollectible debt. Tampering with output or audit logs	Introducing fraudulent or malicious logic during system maintenance Adding unauthorized vendor, employee or other payee during conversion Security patches not applied in a timely manner

Sources of Threats

Threats to information integrity can come from internal or external sources. Internal sources can magnify information integrity risks by overriding or undermining information integrity enablers and controls. External sources can magnify risks through their unpredictability and remoteness.

Cumulative or Compounding Aspects of Risk

In sequential processes, risks may be cumulative. For example, Creation, Operation and Use, and Change are sequential and iterative stages of the information and information system lifecycle. Thus, Creation stage risks may compound Operation and Use stage risks which, in turn, may compound Change stage risks in a repetitive cycle. Similarly, within the information processing lifecycle consisting of Input, Processing, Output and Storage, Input phase risks may compound Processing phase risks which, in turn, may compound Output and Storage phase risks. Therefore, when assessing risks for a particular category or phase, it is important to consider the antecedent categories or phases as well.

Consequences

The evaluation of risk is a study of the likelihood and the consequences of a failure of any one or a combination of information system components. The steps in the risk assessment process are:

1. Identify the IS component(s) associated with information integrity in the domains of content, process or IS environment.

2. Assess the likelihood that the IS component(s) will fail to prevent, detect and correct a significant impairment of information integrity. In assessing the likelihood of failure it will be important to first identify the kinds of things that can go wrong that will contribute to failure of the component (i.e., the vulnerability of the component). The person(s) making the assessment should also consider risk magnifiers such as complexity, nature of the system, and opportunities for malicious acts and their sources.

3. Assess the consequences of the failure if it were to occur.

Typical consequences of failing to prevent, detect and correct significant information integrity impairments are summarized in Table 2.2 below.

Table 2.2 Consequences of Information Integrity Impairments

Categories of Consequence	Typical consequences
Competitive Disadvantage	Delayed time to market Product delay Lost market Revenue loss Reputation loss – damage to stakeholder trust Reliance by third parties Social impact Loss of intellectual capital Theft, disclosure of sensitive, confidential, proprietary information
Business disruption	Loss or corruption of data Inability to meet service demands Customers, users, stakeholders negatively affected

Categories of Consequence	Typical consequences
	Increased or excessive cost to restore availability of viable processing alternatives; replacement of resources, in whole or in part Reliance on key personnel; criticality of the job function to the achievement of business objectives Limited or lack of available labour market/labour pool; inability to replace skills or people Lost investment Productivity reductions Prolonged duration of the recovery Number of workarounds needed to be enacted until normal operations restored
Excessive Costs	Cost of alternative processing; cost of replacement or recovery Cost of workarounds needed Cost of maintaining the old systems or processes Cost of dispute settlements Reorganization, severance, retraining costs Insurance coverage costs and limits Regulatory sanctions and fines
Erroneous Decisions	Reliance on the output for business decisions Unreliable information to management Number of business lines affected
External reporting problems	Unreliable or incomplete processing of information Data not adequately safeguarded from accidental or intentional modification Fraud
Legal/regulatory sanctions	Unreliable information to regulators Privacy breaches Confidentiality breaches