AICPA®

Information Integrity

January 2013

Abstract

The purpose of this white paper is to define what information integrity means and provide context for it to users, preparers and practitioners. This paper is published by the AICPA® Assurance Services Executive Committee's Trust Information Integrity Task Force in conjunction with the Canadian Institute of Chartered Accountants to offer insight into what it means for information to have integrity and how information integrity can be achieved and maintained. The subject matter outlined in this paper is of interest to AICPA members, including both members in public practice and business and industry, those in the accounting profession as a whole, and other participants in the business reporting process, including producers and consumers of business information.

Recognition

Author

Gerald Trites, CICA
Project Director, XBRL Canada

Assurance Services Executive Committee (2011–2012)

William R. Titera, Chair
Dorsey Baskin
Greg Bedard
Suzanne Christensen
Robert Dohrer
Glenn Galfond
Theresa Grafenstine
Charles E. Harris
Christopher W. Kradjan
Mark Mayberry
Leslie Murphy
Beth Schneider
Leslie Thompson
Miklos Vasarhelyi

Trust Information Integrity Task Force

Chris Halterman, Chair
Dennis Bell
Efrim Boritz
Sheri Fedokovitz
Peter Heuzey
Audrey Katcher
Kevin Knight
Chris Kradjan
David Lewis
David L. Palmer
Thomas Patterson

AICPA/CICA Staff

Amy Pawlicki
AICPA Director
Business Reporting, Assurance and Advisory Services & XBRL

Gordon Beal
CICA Director
Guidance and Support

Erin Mackler
AICPA Senior Technical Manager
Business Reporting, Assurance and Advisory Services

Judith Sherinsky
AICPA Senior Technical Manager
Audit and Attest Standards

Introduction

The paper focuses on what it means to have information integrity and how information integrity can be achieved and maintained.

- The purpose of this paper is to define what information integrity means and provide a context for it for users and preparers of information and providers of assurance on such information. The paper focuses on what it means to have information integrity and how information integrity can be achieved and maintained. There is some emphasis on the value added through the verification of information integrity by an independent assurance practitioner.[1]

- Various types of information[2] are increasingly being made available to management, investors, regulators, shareholders and other interested parties by business entities. This information may include excerpts from financial statements such as inventories or accounts receivable, data from the company records such as production volumes and key performance indicators. It is expected that this trend will continue.

- In addition to the metrics published by business entities, numerous metrics also are published by other organizations for a variety of purposes. For example, employment statistics are published by government and non-government entities for use by economic analysts, business, and the general public. In the field of

[1] This paper is written on the assumption that readers in the United States have knowledge of AT section 101 *Attest Engagements* (AICPA, *Professional Standards*) and in Canada, CICA Handbook Section 5025, *Standards for assurance engagements other than audits of financial statements and other historical financial information* and Section 5800, *Special Reports — Introduction.*

[2] Information has been defined as any data that are presented in a context that is meaningful to a user, in contrast to raw data, which are presented without explanation or without information about it (i.e., without meta-information).

sustainability reporting, published metrics include baseline-year emissions data, energy produced/consumed and resource reserves (bbl, tons, etc.). Service organizations routinely produce reports on performance measured against metrics defined in service level agreements and commitments.

- Stakeholders use this information in making decisions, interpreting or using other information and generally increasing their knowledge about the subject matter. To make the best decisions, users need to have confidence in the integrity of the information.

To make the best decisions, users need to have confidence in the integrity of the information.

Scope

Information integrity is defined as the representational faithfulness of the information to the underlying subject of that information and the fitness of the information for its intended use.

- In this paper, information integrity is defined as the representational faithfulness of the information to the underlying subject of that information and the fitness of the information for its intended use.

- Information can be structured (e.g., accounting transactions), partly structured (e.g., object-oriented data bases) or unstructured (e.g., raw data such as a string of digits). For purposes of this paper, information consists of representations regarding one or more events and/or instances that have been created for a specified use. Such events or instances can have numerous attributes and characteristics that may or may not be included in a set of information, depending on the intended use of the information. Some uses may require a small number of attributes to be recorded about a given set of events or instances whereas other uses may require a large number of attributes to be recorded about those same events or instances.[3]

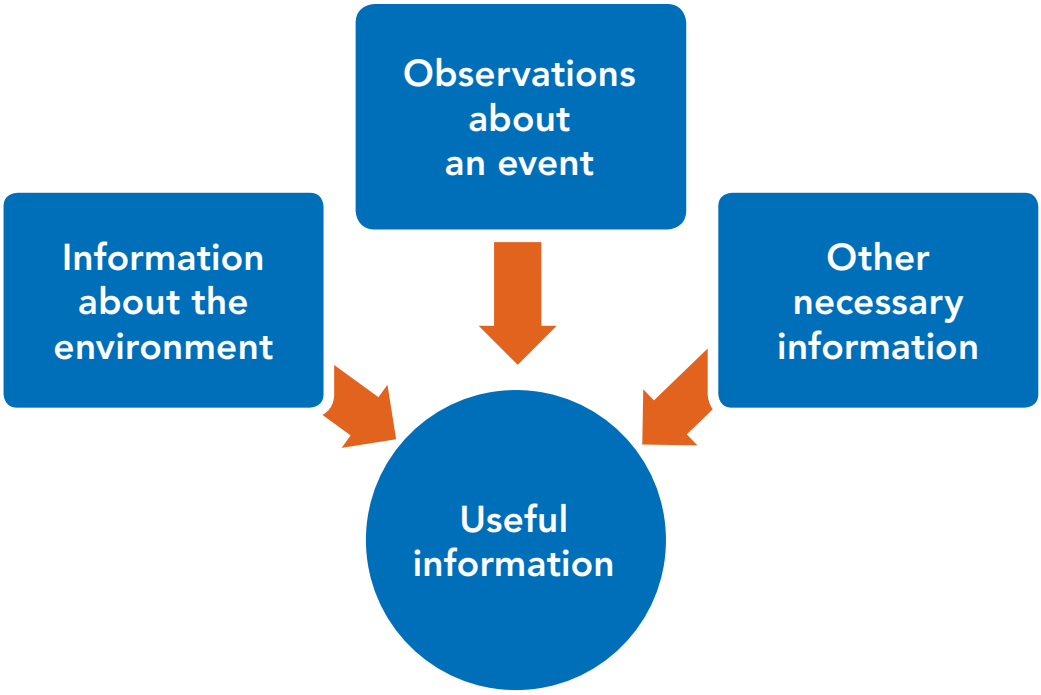
  For the information to be useful, it is important to describe the purpose of the information and other contextual information necessary to make use of the information. This is called meta-information.

- When a practitioner[4] is engaged to perform an attestation engagement on the integrity of information, the information is the subject matter of the engagement and its integrity or representational faithfulness is determined by evaluating how well it represents the subject that it purports to represent. For example, a weather report is the representation of the weather. Therefore, the integrity of the weather report depends on how well it represents the weather.

- In summary, information is prepared for a specified purpose and includes: (1) the observations about the characteristics of the specific events or instances to which it pertains, (2) information about the environment in which the events occurred or the instances existed and (3) other information necessary for the observations to be used for their intended purpose. Information integrity is determined based on both the information's consistency with its meta-information and its representational faithfulness. Therefore, information integrity includes the accuracy, relevance, precision, timeliness and completeness of the information and its meta-information. Information that is accurate, relevant, precise, timely and complete for a particular purpose can be termed to be "fit for purpose."

[3] For example, a log of accounting transactions used to assess the completeness of information transmitted from a branch to headquarters may only require an information identifier and a message digest that can be checked for completeness of transmissions for each item. In contrast, an audit trail used to trace transactions from cradle to grave and vice versa, may need an information identifier, message digest, date stamp, source, destination and intermediate processing steps that were performed on the information.

[4] In the attestation standards, a CPA performing an attestation engagement ordinarily is referred to as a *practitioner.*



- In using information, users need to assess their level of confidence in the integrity of the information. Otherwise, they may place unwarranted reliance on the information. Confidence in information integrity can come from many sources, including:

  A. Additional information supplied by the party responsible for the information, such as a description of the process that produced the information.

  B. The reputation of the responsible party.

  C. Knowledge possessed by the user, whether pre-existing or specifically obtained for the purpose of evaluating the integrity of the information.

  D. Validation of the information by a third party with knowledge sufficient to evaluate the integrity of the information, which may or may not be in the context of a professional engagement.

  E. Obtaining a report from an independent third-party based on procedures performed to evaluate the integrity of the information provided by the responsible party. Such a report would contain an opinion about whether the information is based on or in conformity with specified criteria and would be provided by a CPA or CA reporting under the attestation standards.

An examination report on the integrity of information, provided by an independent CPA or CA, provides the highest level of confidence.

- An examination report on the integrity of information, provided by an independent CPA or CA with the appropriate competencies normally provides the highest level of confidence, because such engagements are conducted with objectivity and supported by work carried out in accordance with relevant professional standards.

- The AICPA's Attestation Standards Section AT 101, *Attest Engagements* (AT 101) enables practitioners to report on subject matter other than historical financial statements. It permits practitioners to report directly on subject matter such as data or information or to report on an assertion about the subject matter. The approach in CICA Handbook Section 5025 is similar in this respect. Several sections of this paper explore the application of these standards. In addition, TSP section 100 Trust *Services Principles, Criteria and Illustrations for Security, Availability, Processing Integrity, Confidentiality and Privacy* (AICPA, *Technical Practice Aids*)[5] provides reporting guidance for situations in which a practitioner is reporting on the effectiveness of controls over the system that processes or stores the information, rather than on the information itself. New attestation standards are unlikely to be necessary in order for a practitioner to report on the integrity of information, but new guidance by the profession will likely be needed.

[5] The paper focuses on what it means to have information integrity and how information integrity can be achieved and maintained.

Understanding the Information Lifecycle

- The process of obtaining or developing information begins with the recognition of the need for particular information. Once this need has been identified, it proceeds through an Information Development Life Cycle (IDLC), which normally includes the following steps:

  A. Information specification

  B. Information design and data definition

  C. Process/system development

  D. Information processing life cycle execution (see phases covered page 8)

  E. Information design revision

  F. Information retirement (destruction or permanent archiving)

- Once the need for information has been recognized, the information requirements are identified and the information and its lifecycle are designed. The design starts with identifying the subject (events or instances of interest) to which the information will pertain; this takes into account the identified information requirements of the users. The design process identifies those attributes of the events or instances that will be observed and reported. This design is crucial in enabling the information to be fit for its purpose. The design also addresses all stages of the information lifecycle through which the recorded observations will pass until it is reported to the user and, at the end of its life, destroyed.

The process of obtaining or developing information begins with the recognition of the need for particular information.

- The information processing lifecycle itself refers to the life of a particular piece of information from the time it becomes identifiable until it is destroyed. Key phases of the life cycle referred are:

  A. Creation or identification of data

  B. Measurement

  C. Documentation or recording

  D. Input

  E. Processing, change or aggregation (to transform data into information)

  F. Storage or archiving

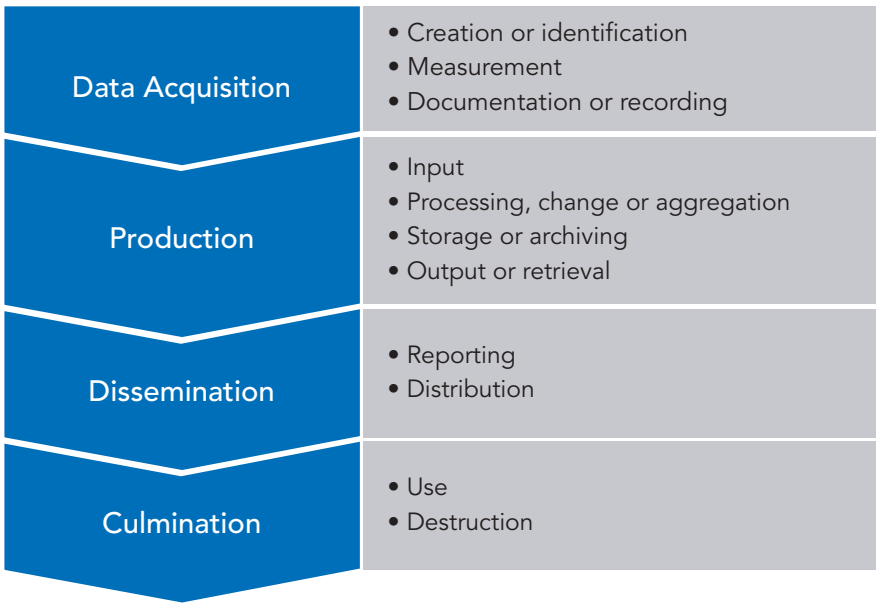
  G. Output or retrieval

  H. Reporting

  I. Distribution

  J. Use

  K. Destruction



- The attributes of each event or instance are affected by the characteristics of its environment, which may change during the period of time in which the event or instance occurs and information is reported. Therefore, understanding the attributes of particular information involves considering how the environment changes during the lifecycle of the information, including the control and processing environments as well as the broader environment in which the event or instance occurs and the information is used. For example, the sales of ice cream at a particular store location will be affected by such factors as temperature, activities in the immediate vicinity, the people in the area, etc. In designing the information for reporting ice cream sales to management, all these characteristics of the environment need to be considered for inclusion in the information in order to place the information in context.

- Some attributes of an event or instance (and environmental characteristics) may be difficult to describe or may even be indescribable (e.g., what the audience of a particular television show finds appealing), or undeterminable (e.g., the intent of a borrower to properly maintain assets pledged as collateral). Yet, these attributes exist and may have an effect on the nature and interpretation of a portion or aspect of the information. For example, the likability attribute of a particular actor in the cast of a television show may have an effect on how people receive a show, directly affecting viewership. If the likability of the actor changes, there may be a direct effect on the viewership, however, this change may not be easily measured or described. The design of information about the television show needs to take into account the effect of such attributes on the fitness for purpose of the information and consider whether the omission of such attributes would make the information misleading.
- Attributes may be quantifiable or qualitative. A quantifiable attribute or environmental characteristic is measurable at some point in the past or present, whereas, qualitative information is difficult to measure. In designing qualitative information, there should be consideration given as to whether the information and meta-information are sufficiently objective to enable the risk that the information will be misunderstood to be reduced to an acceptable level.
- If an attribute will be measurable in the future, the attribute of the event or instance is probably contingent on the occurrence of one or more future events. In turn, there may be information regarding these future events that may be describable, quantifiable or measureable (e.g., based on a known probability) and that should be included in the design of the information.
- If the measurability of an item depends on the occurrence of a future event, it can become measureable at a date or period that is certain or one that is uncertain. For example, the number of future sales returns within a 30-day return period relates to a certain period, while the date of collection on an account receivable subject to bankruptcy proceedings is most likely to be uncertain.
- The objectivity or subjectivity of an item can have an effect on the ease with which it can be measured. Both types of information are likely able to be measured, but the more subjective an item is, generally the more difficult it is to measure and, at the extreme, measurement may well be impossible.
- Every item of information has meta-information associated with it such as the environmental characteristics noted above, which permit the user to understand and interpret the information. Meta-information is defined as information about information; it describes what the information is and contributes to an understanding of the event or instance and its attributes. For example, an amount of 35,300 is meaningless because we do not know what the number represents. It could be dollars or miles or numbers of automobiles. If we add a dollar sign, we know that it is a monetary measure, but we still don't know what the item is. If a label "Inventory" is added, we have

Meta-information is defined as information about information; it describes what the information is and contributes to an understanding of the event or instance and its attributes.

Meta-information provides additional information about an item and places it in context, making it fit-for-purpose.

more information but still not enough to be very useful. However, adding a description — for example, Inventory of Finished Goods for Jones Corp as at Dec. 31, 20X1, valued under U.S. GAAP at the lower of cost and net realizable value — provides a reasonable amount of information, including ownership, date and valuation. All of the information that was added is meta-information.

- Meta-information provides additional information about an item and places it in context, making it fit-for-purpose. Such context also is essential to be able to perform an attestation engagement on the information. In the aforementioned example, an examination engagement could be performed on whether the inventory is fairly stated in conformity with generally accepted accounting principles (GAAP). In this case, GAAP provides suitable criteria for evaluating the inventory information. Therefore, suitable criteria used in an attestation engagement are part of the meta-information associated with the subject matter.

- A practitioner engaged to perform an attestation engagement on the integrity of information needs to consider the completeness of the information and the accompanying meta-information when evaluating the integrity of information. There is a range of meta-information that might be available, from very complete to minimal, perhaps just a basic definition or label. In the latter cases, where the meta-information is minimal, the criteria also will be minimal, and the practitioner may decide that the criteria, like the information, are not complete enough to carry out the engagement.

- When information is extracted from its original form by a user, it may be placed into a different context, which could cause the users of the information to misinterpret or misunderstand it. While users have always been able to take line items out of financial statements and present them in some other context, changes in technology have meant that the portability of information has increased. Accordingly, de-contextualizing and re-contextualizing electronic information has become much easier and more common.

- The portability of information raises the following issues:

  A. Changing the context in which the information is presented may mean that:

     1. It may be difficult for users to determine what the information is meant to convey.

     2. Important meta-information needed to understand the information may not be carried with the information and may not be accessible to the users.

     3. The criteria used to evaluate the integrity of information in the original context may not be appropriate in the new context. An example is removing the disclosure from a financial statement that it was prepared in accordance with an "other comprehensive basis of accounting." Any user who does not know the original context could assume the financial statements were prepared in accordance with GAAP and would be misled.

B. The information could travel through different systems, thus jeopardizing its integrity because of variability in the quality of controls among systems. The use of modern tagging techniques — such as those found in XML or XBRL — can help by attaching the contextual meta-information — such as underlying standards — to the information in order that this meta-information can move along with the information. When the meta-information involves standards such as IFRS or GAAP, or frameworks such as COSO, the meta-information that moves with the information may of necessity be confined to links or references to the applicable sections or paragraphs of those standards or frameworks.

- The relationship of information to a point in time or a period of time also is important context to the use of information. Information that was relevant during one period may become irrelevant during a different period because its context is not appropriate for the use of the information in the different period. For example, the sale of punch cards was useful in the past as a predictor of computer usage; however, it is no longer valid for that purpose today. The usefulness of information changes over time and requires the responsible party to continually consider the subject matter and the context in order to evaluate relevance.

The information could travel through different systems, thus jeopardizing its integrity because of variability in the quality of controls among systems.

Information Integrity Risk

- There are various risks associated with the design, creation and use of information as well as when performing an attestation engagement on its integrity. These risks are discussed under the headings of subject matter risk, use risk, information design risk and information lifecycle risk. The risks can have an effect on the information integrity, increasing the possibility of material misstatements of the information or the risk of misunderstanding during its use. These risks need to be considered when performing an attestation engagement.

- ***Subject matter risk*** The third general standard for attestation engagements is: *The practitioner must have reason to believe that the subject matter is capable of evaluation against criteria that are suitable and available to users.* Subject matter risk is the risk that suitable criteria cannot be developed for the particular

events or instances and information about the events or instances is inappropriate for the use for which it is intended — its fitness for purpose. It includes the following elements:

A. The attributes of interest related to the event or instance 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 collectability of an account receivable. They also might be qualitative factors that are too subjective to be observed or measured.

B. The information that can be supplied is misleading or is likely to be misunderstood by its intended recipient.

- ***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. 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. This includes:

1. Selection[6] of inappropriate information or omission of appropriate information for use in the decision-making process

   - Inappropriate substitution of available information for unavailable information

   - Inappropriate projection of information to other events/instances

   - Inappropriate combination/ transformation/synthesis of information

2. Misinterpretation or misapplication of the information/meta-information

3. Inconsistencies in the decision-making process both by a user and between users

4. Inconsistency/misunderstanding between the intent of the information supplier and that of the information user

B. Someone other than the intended user will make use of the information resulting in a misunderstanding on the part of the user or an erroneous decision.

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.

Inappropriate application of meta-information would occur, for example, when the information supplied is given excessive weight in the decision-making process or the information does not contain all the meta-information required for the intended use or simply is not well understood by the user (e.g., use of the information and disclosures written in German by someone with limited knowledge of the German language).

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.

[6] 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.

Some risks can be addressed by effective controls whereas others may need to be addressed by other risk mitigation strategies such as avoidance.

Risks of misinterpretation or misapplication of information may be addressed by describing the intended user and the intended use of the information in related meta-information and in assurance reports on the integrity of the information. Information integrity risk may be addressed by applying effective controls over and performing assurance procedures on the information and related meta-information to ensure that they possess information integrity.

- ***Information design risk*** consists of those risks of misstatement that arise from the failure of the information design to address subject matter and use risks, as well as the risks inherent in the activities that occur throughout the lifecycle of the information. It includes the risk that.

  A. The attribute/characteristic to be reported:

     1. Is an inappropriate representation of the desired information
     2. Is out of date (measured too early or too late)
     3. Is inaccurate
     4. Contains bias
     5. Has insufficient precision for the intended use
     6. Is at an inadequate level of aggregation/disaggregation
     7. Is inconsistent/not be replicable (between measurers or between measurements) because of qualitative factors and uncertainty
     8. Is inconsistent with norms or other sources

  B. The processing of the information from measurement to reporting introduces errors in the information

  C. The storage of the information introduces errors in the information

  D. The retrieval of the information introduces errors in the information

- **Information processing lifecycle risk** consists of those risks that are introduced during the life cycle of particular pieces of information.

  A. Creation or identification of data

  B. Measurement

  C. Documentation or recording

  D. Input

  E. Processing, change or aggregation (to transform data into information)

  F. Storage or archiving

  G. Output or retrieval

  H. Use

  I. Destruction

  These risks can be mitigated by controls established during the design process, but never can be completely prevented.

- All of the risks discussed above show that the integrity of information depends on the integrity of the meta-information. These risks and their nature need to be taken into account when reporting on information. Some of these risks can be addressed by effective controls whereas others may need to be addressed by other risk mitigation strategies such as avoidance. For example, risks to information integrity during the information life cycle can be addressed by effective environmental and processing controls. However, if the subject matter is not capable of evaluation against suitable, available criteria, then a practitioner can and should avoid the information integrity engagement risk by not taking on the engagement.

Criteria for Information Integrity Assurance

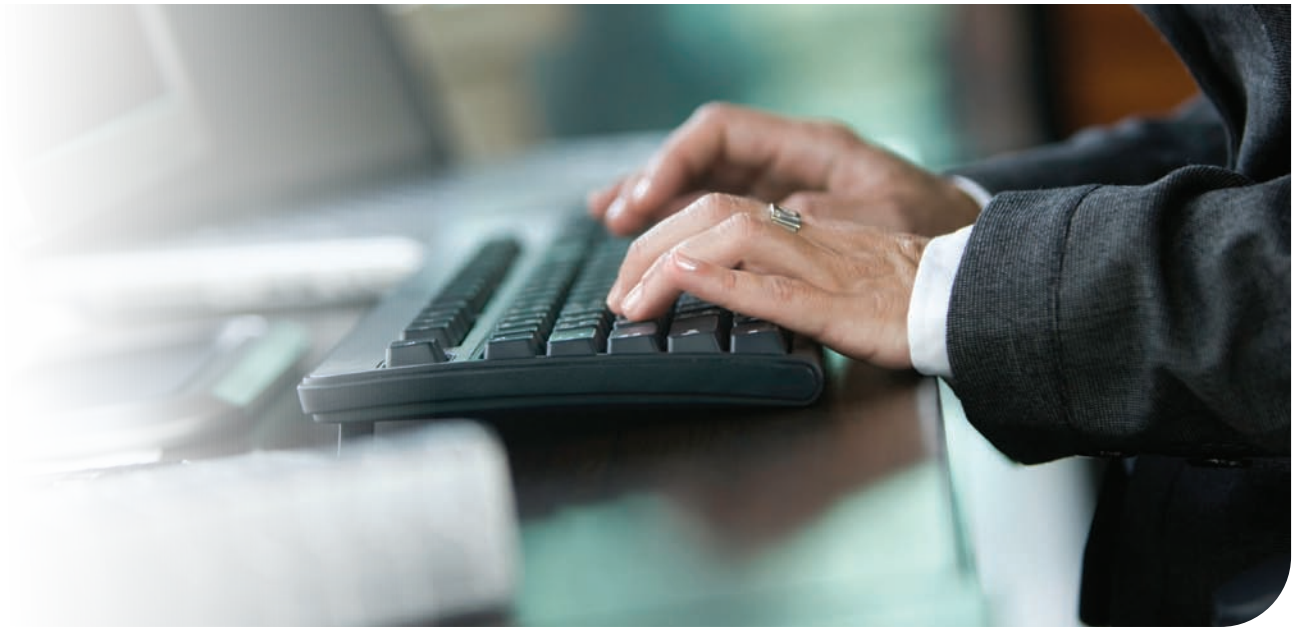
- Within the professional standards, opinions related to the integrity of information are arrived at by measuring or evaluating the information reported against suitable criteria. Since the criteria are closely related to the meta-information, it follows that the identification of criteria requires an analysis of the meta-information necessary to understand the subject matter.

- Information that contains complete meta-information would provide a greater array of possible criteria for evaluating information integrity or reporting on information integrity. For example, if the meta-information states that the information is prepared in accordance with generally accepted accounting principles, then this could be the criteria used for evaluating the information.

- Under AT 101.24, criteria must be suitable, which means they must be objective, measurable, complete and relevant. Accordingly, the criteria must be identifiable and capable of consistent evaluation; consistent not only between periods but between entities or similar circumstances. In addition, it is important that the criteria can be subjected to procedures for gathering sufficient appropriate evidence to support the opinion or conclusion provided in the practitioner's report. Moreover, metrics need to be selected that address the risks that were identified.

Under AT 101.24, criteria must be suitable, which means they must be objective, measurable, complete and relevant.

- TSP section 100 *Trust Services Principles, Criteria and Illustrations for Security, Availability, Processing Integrity, Confidentiality and Privacy* (AICPA, *Technical Practice Aids*) sets out the criteria to be used in reporting on information systems. The criteria are met by controls in an information system accordingly, the document contains illustrative controls for the criteria. Since that document addresses reporting on systems, it can be used for reporting on the systems containing information that is the subject matter of an attestation engagement.



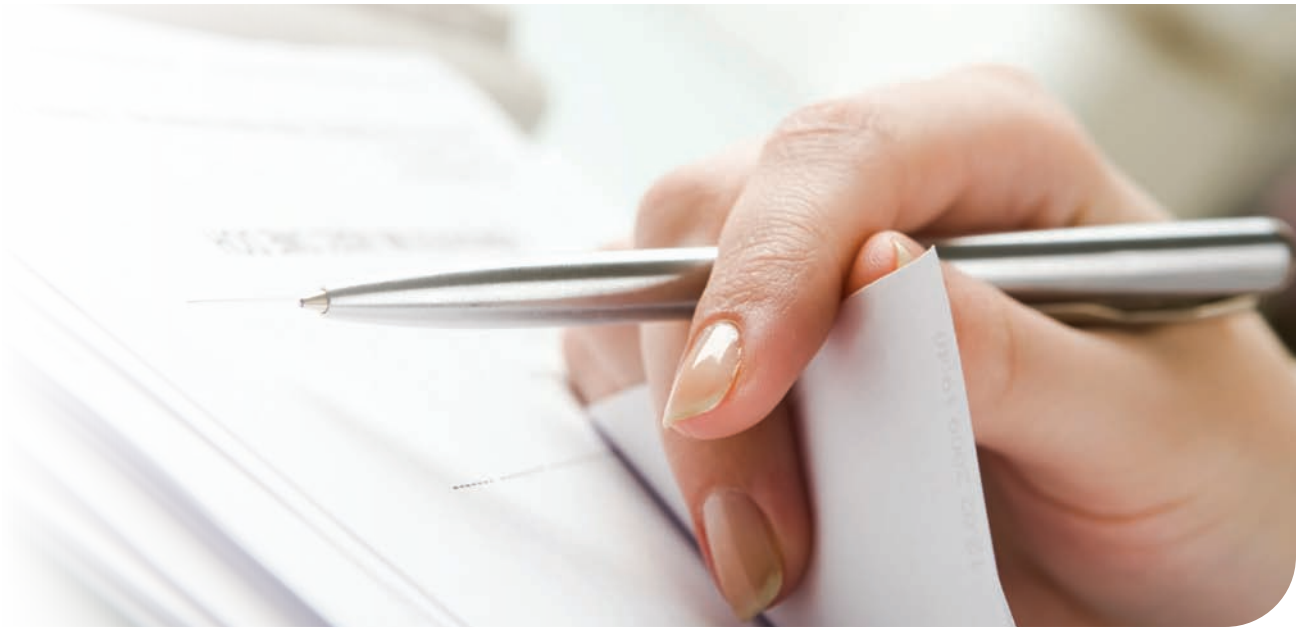
Materiality

- In considering the integrity of information other than financial statements, the question of materiality arises — how is it measured in the context of information other than financial statements? The concept of materiality is fundamentally the same in any attestation engagement. An item is considered to be material if omitting it or misstating it could influence the decisions that users make on the basis of the information. It is the application of that concept that presents issues.
- Measures of materiality vary for financial statements; for example it might be 5% of net income or 2% of total assets. For other financial items expressed in currency, the magnitude of materiality often is in the same range. For example, if an opinion is being expressed on sales, the materiality used by the auditor could be somewhere in the 2% range. It would follow that when an engagement is performed on smaller bits of data, say individual data elements or individual transactions, then the same principles would be followed. The exact percentage to be used always is a matter of professional judgment.
- A more difficult aspect of materiality is that it is not only quantitative, but also qualitative. Some items may be quantitatively immaterial, but qualitatively material. For example, a small error in record keeping is detected by the auditor. The amount is a fraction of quantitative

materiality but has the effect of showing a result that just meets analysts' expectations/management's forecast. This error would likely be qualitatively material. Like quantitative materiality, qualitative materiality is a matter of professional judgment.

- Because of the difficulty of determining materiality for information in attestation engagements, there is a good case for disclosure of materiality in the attestation reports that results from such engagements. Without this information, users of such reports would be at a disadvantage because they would have difficulty knowing how materiality was determined in the attestation engagement. For financial statement audits, the methods of determining materiality are well-established. However, attestation engagements on other information are a new area and the understanding of users could be enhanced with information about materiality.

A more difficult aspect of materiality is that it is not only quantitative, but also qualitative.



Report Delivery

Properly tagged electronic reports have the additional advantage that they can be conveyed from machine-to-machine and platform-to-platform and may be read using electronic means.

- Information might be presented on a website, extracted by a user and reused in another context. It might be included in an analyst's report or downloaded into a user's system and then employed in various ways. Users extracting a single information item or even a performance indicator will not necessarily know that there is an attestation report associated with the information
- There is a need for some method of informing users that there is a report on the information. This suggests a need for electronic reporting.
- There are several ways reports can be delivered electronically. They include:
  - A. Providing a URL (Uniform Resource Locator) for the location of a report
  - B. Tagging the information with a report or a URL reference to a report
  - C. Using secure electronic publication
- Properly tagged electronic reports have the additional advantage that they can be conveyed from machine-to-machine and platform-to-platform and may be read using electronic means. When a URL is used for a report, it should be properly secured.

- In some cases, the practitioners may be interested in knowing the report is not being misused or misrepresented. The users of the report may also have an interest in ensuring that the report presented is the same as the one the practitioner issued. In such cases, the practitioners should sign the report using secure electronic publication methods including a combination of encryption and digital certificates that would verify that the practitioner actually issued the report.
- The use of secure electronic publication also helps to establish:

    1. Authorization — The publication of the report was properly authorized; through time-stamping it can be determined that any signature used was appropriate at the time, even if the signer has since changed roles or left the organization
    2. Authentication — The identity of the issuer and the information in the report reflect the actual issuer and the actual assertions made by the issuer
    3. Integrity — The report and information have not been changed in an unauthorized manner since they were initially published
    4. Non-repudiation — The issuer cannot deny they issued the report and the recipient cannot deny that they received the report

The users of the report may also have an interest in ensuring that the report presented is the same as the one the practitioner issued.

Appendix A — Example of Independent Assurance Report

To the Stakeholders of Example

We have examined (the information) the information identified in items 1-5 below, which is contained in Example Company's Annual Sustainability Report for the year ended Dec. 31, 20XX (sustainability report).

Information Contained in the Purchasing Section of the Sustainability Report

A. Product purchases and average price per pound

B. Environmentally friendly purchases and such purchases as a percentage of total purchases

C. Fair trade certified green purchases and such purchases as a percentage of total purchases

D. Certified organic product purchases and such purchases as a percentage of total purchases

E. Amount of commitment to investment in farmer loans and number of farmers

Information Contained in the Farmer Support Section of the Sustainability Report

Example Co.'s management is responsible for the information. Our responsibility is to express an opinion on the information identified in items 1-5 based on our examination. Criteria used to evaluate the information identified in items 1-5 is included in the same section of the sustainability report in which the item is presented.

Our examination was conducted in accordance with attestation standards established by the (American Institute of CPAs/Canadian Institute of Chartered Accountants), and accordingly, included examining, on a test basis, evidence supporting the Information and performing such other procedures as we considered necessary in the circumstances. Those procedures are described in more detail in the paragraph below. We believe that our examination provides a reasonable basis for our opinion.

Our evidence — gathering procedures included, among other activities, the following:

- Testing the effectiveness of the internal reporting system used to collect and compile the information included in the report

- Performing specific procedures, on a sample basis, to validate the information, on site at company buying operations in Lausanne, Switzerland, and corporate headquarters in Seattle

- Interviewing partners (employees) responsible for data collection and reporting
- Reviewing relevant documentation, including corporate policies, management and reporting structures
- Performing tests, on a sample basis, of documentation and systems used to collect, analyze and compile the information that is included in the report
- Confirming certain of the Information to third-party confirmations and reports

In our opinion, the Information for the fiscal year ended Dec. 31, 20XX is fairly presented, in all material respects, based on the criteria indicated above.

(Signature)

City, State
Date

Appendix B — Definitions

Change — The replacement of a pre-existing organizational element, business practice, infrastructure or software with a revised version; also, includes departure or replacement of personnel.

Complexity — The presence of a large number and/or variety of interacting components.

Content — All types of data that are used to generate information including, raw data, sensor data, semi-processed information, meta-data and parameters.

Contextual Information — See information.

Data — A recorded set of qualitative and quantitative measurements of the characteristics/attributes of events and instances. Data may be presented as specific quantities or as narrative descriptions.

Data Quality — A label for a variety of concepts describing desirable attributes of data ranging from relevance and usefulness to integrity; at a minimum, data quality refers to the level of completeness and accuracy of data captured and processed for a specific purpose.

Enabler — Component, feature or practice associated with the content, process, or environment domain that contributes to information integrity.

Environment — All elements of the supporting organizational infrastructure that are relied upon by the processing domain, including policies, standards, procedures and IT services.

Event/Instance — An event is a category of occurrences that is to be captured by a system if business rules identify the event as a type that is to be captured; an event instance is an actual and particular occurrence of the event type that is to be captured.

Information Activity vs. Process — A process is a collection of activities; see process.

Information — Any data that are presented in a context that is meaningful to a user, in contrast to raw data, which are presented without explanation or without information about it (i.e., without meta-data or meta-information.)

Information Assurance — It is 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 — A body of 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 quality — A label for desirable attributes of information achieves its intended purpose, including relevance, usefulness and representational faithfulness. COSO (2011) identifies the following attributes that contribute to the quality of information: sufficient; timely; current; correct; accessible; protected; verifiable; and retained.

Information Integrity Impairment Risk — See Risk.

Information Integrity — It is the representational faithfulness of information to the underlying subject of that information and the fitness of the information for its intended use.

Information Life Cycle — The process from specification of information to its retirement.

A. Information specification

B. Information design and data definition

C. Process/system development

D. Information processing life cycle (see information processing lifecycle below)

E. Information design revision

F. Information retirement (destruction or permanent archiving)

Information Processing Life Cycle — The process from creation of information to its ultimate destruction (see information lifecycle above).

A. Creation or identification of data

B. Measurement

C. Documentation or recording

D. Input

E. Processing, change or aggregation (to transform data into information)

F. Storage or archiving

G. Output or retrieval

H. Reporting

I. Distribution

J. Use

K. Destruction

Meta-Data — Data about data. More specifically, meta-data are data that describe the content, context and structure of data. See also meta-information.

Meta-Information — A set of information that is necessary for the information processing systems to maintain information integrity during processing and for users to understand information and use it appropriately. See also meta-data.

Process — It describes all activities used to 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.

Recording — The capture of information.

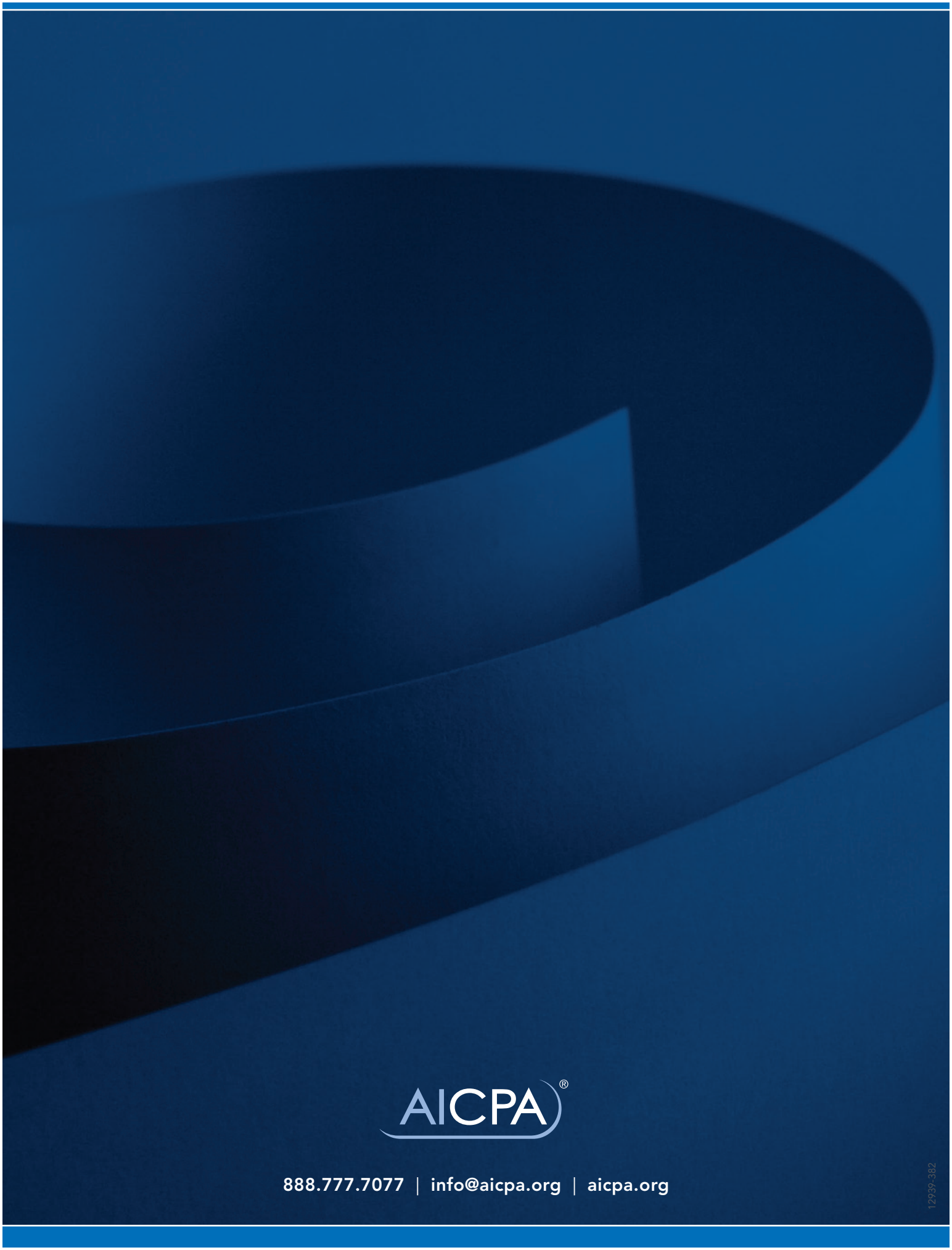
Risk (of Information Integrity Impairment) — It is a factor that may undermine or threaten one of the core attributes of information integrity. Risks can arise from intentional malicious acts or unintentional errors.

Risk Magnifier — A factor that magnifies a risk (e.g., complexity, nature, malicious intent, etc.).

Subject Matter — It is the information about a subject, which consists of an event/instance and accompanying meta-information

Threat (to Information Integrity) — See risk.

New York, NY 10036-8775



888.777.7077 | info@aicpa.org | aicpa.org

12939-382