Criteria for Assessing and Reporting on Data/Information Integrity

Efrim Boritz, University of Waterloo

jeboritz@uwaterloo.ca

Speaker Background

J. Efrim Boritz, PhD, FCPA, CISA

- **Chartered Professional Accountants Chair in Accounting University of Waterloo**
- **Director of the University of Waterloo Centre for Information Integrity and Information Systems Assurance**
- **Member of CPA Canada Assurance Innovation Committee**
- **Member of the AICPA working group on Data Integrity**

Information

- Financial statement information - integrity governed by GAAP/GAAS

- But what about Financial non-GAAP and non-Financial - ????

- Trends in <u>voluntary</u> expanded reporting
  - Key Performance Indicators (KPIs)
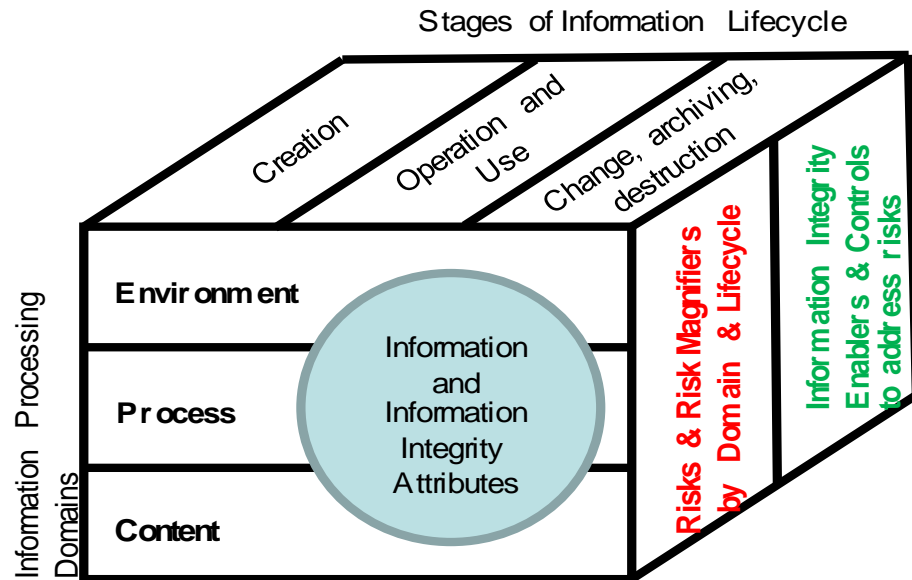 - Framework based: Environment, Sustainability, Governance (ESG); GRI; IR; etc.

- Trends in <u>mandatory</u> reporting to governments and public
  - Production related (regulatory capital, loans gjven, newspaper circulation)
  - Labour related (gender representation, pay equity)
  - Environment related (water consumption, carbon emissions)
  - Social policy related (human rights, diversity)
  - Bribery and corruption
  - Etc.

- **There is much activity internationally around criteria and assurance practices that will govern the integrity of Financial non-GAAP and non-Financial information!**

Overview of Presentation

- Introduction
- Information Integrity Framework
  - Information Lifecyle
  - Information Integrity Definition
  - Domains of Information Processing
  - Risks, Enablers and Controls
- Assurance on Integrity Data/Information
- Producing a Description of Data/Information
  - Principles and Criteria for Preparing a Description
- Assurance Procedures
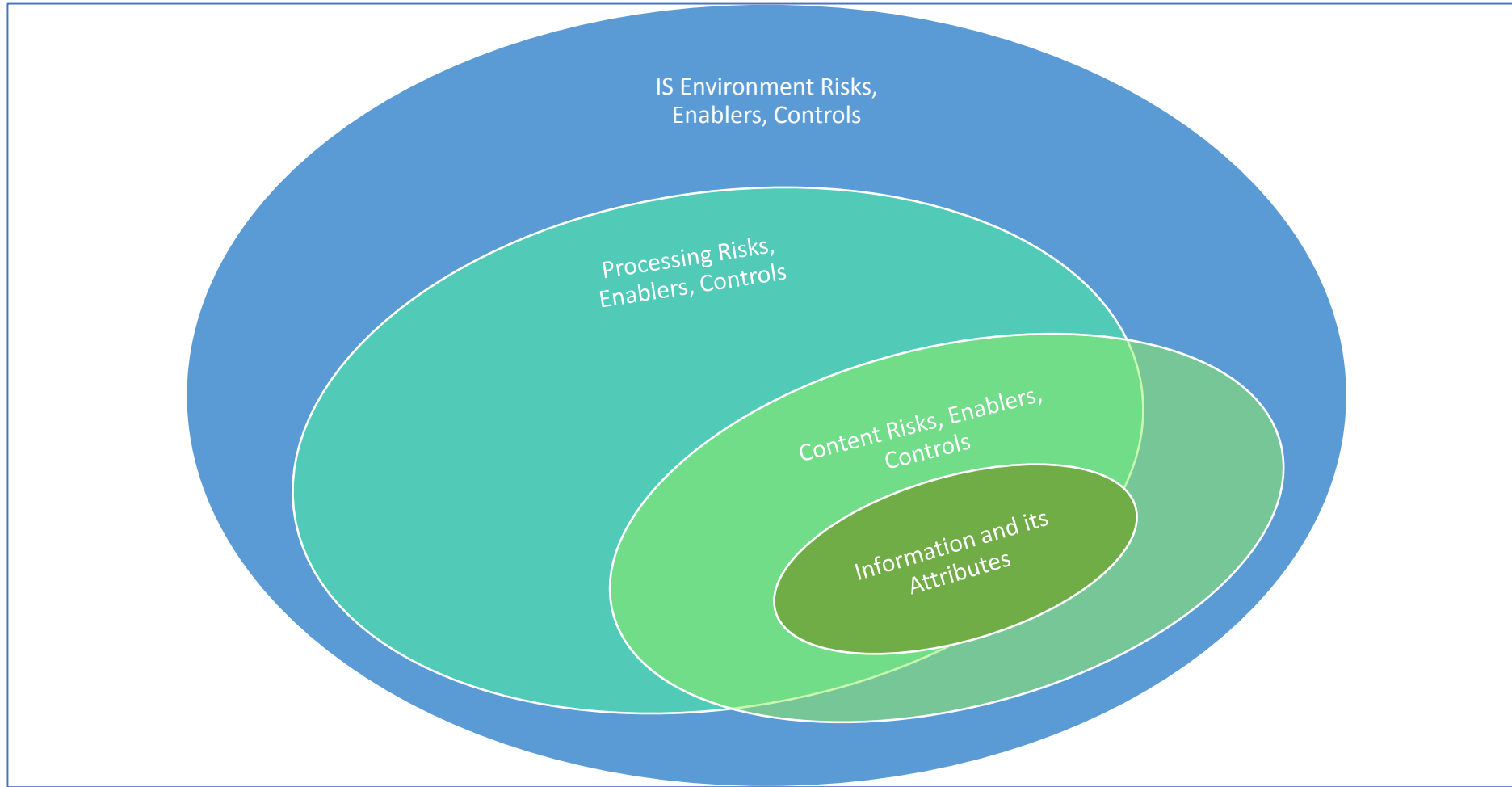
Information Integrity Framework

Stages of Information Lifecycle

Creation · Operation and Use · Change, archiving, destruction

Information Processing Domains

Environment · Process · Content

Information and Information Integrity Attributes

Risks & Risk Magnifiers by Domain & Lifecycle

Information Integrity Enablers & Controls to address risks

- **information and the attributes of its integrity**

- **the information lifecycle**

- **Information processing domains (environment, process and content)**

- **information integrity risks and risk magnifiers**

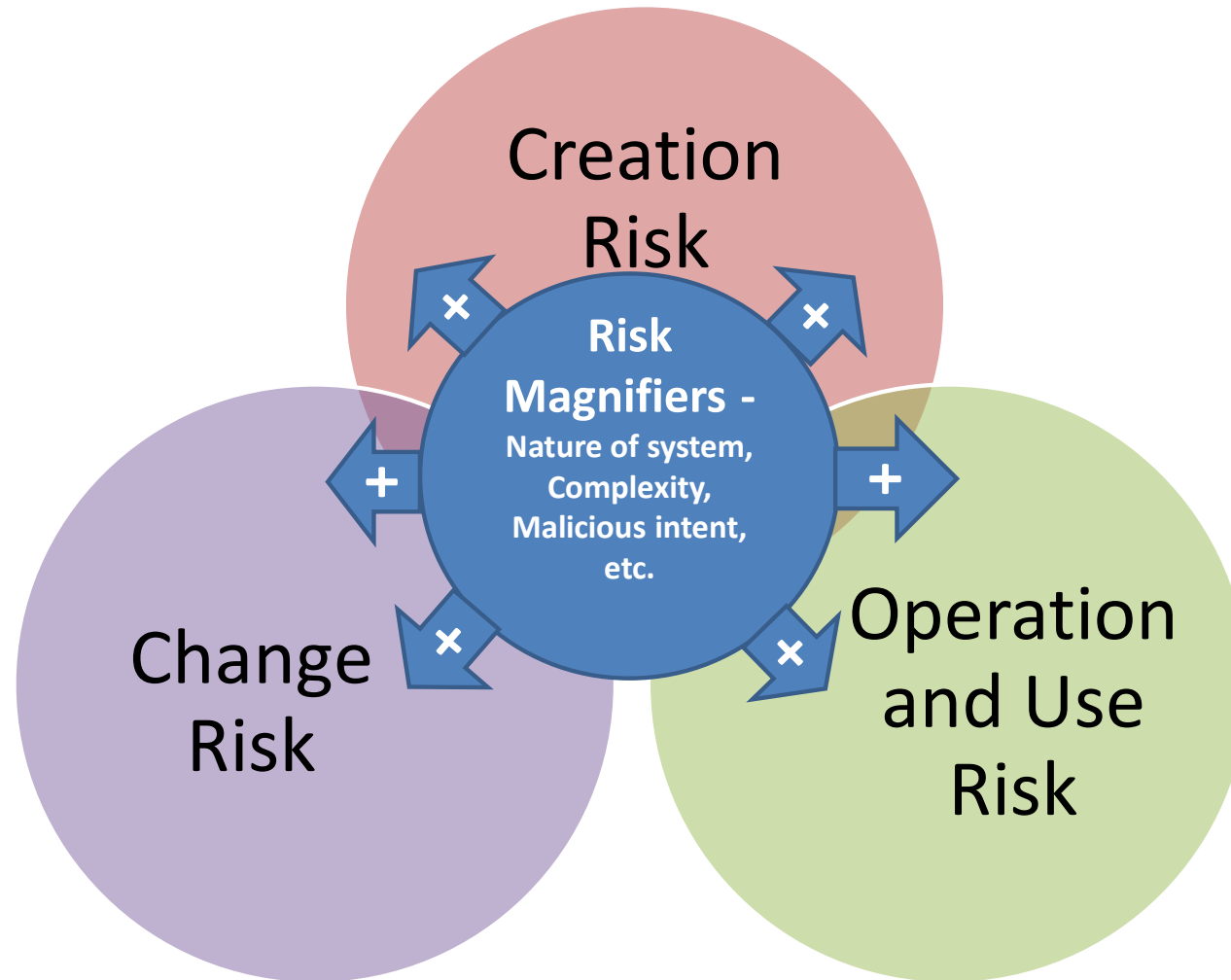- **information integrity enablers and controls designed to address risks.**

UW CISA

Information Integrity = Representational Faithfulness
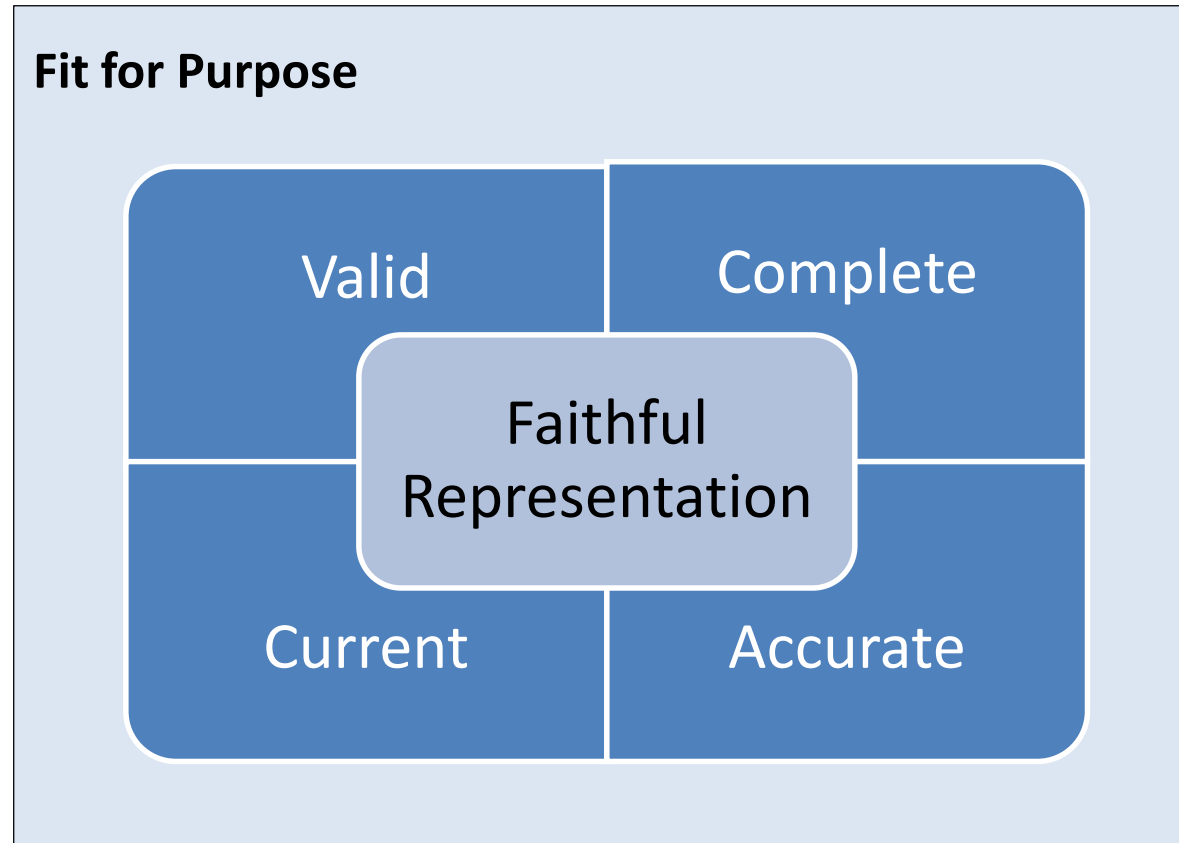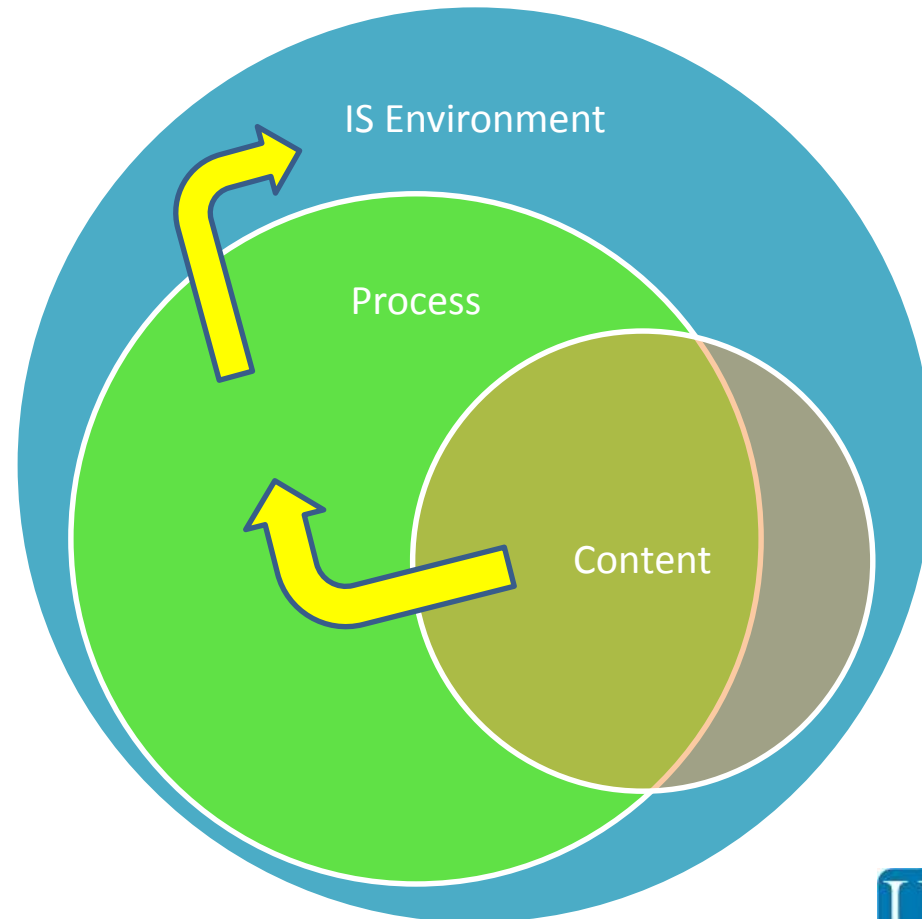
Information Integrity Risks, Enablers and Controls

IS Environment Risks, Enablers, Controls

Processing Risks, Enablers, Controls

Content Risks, Enablers, Controls
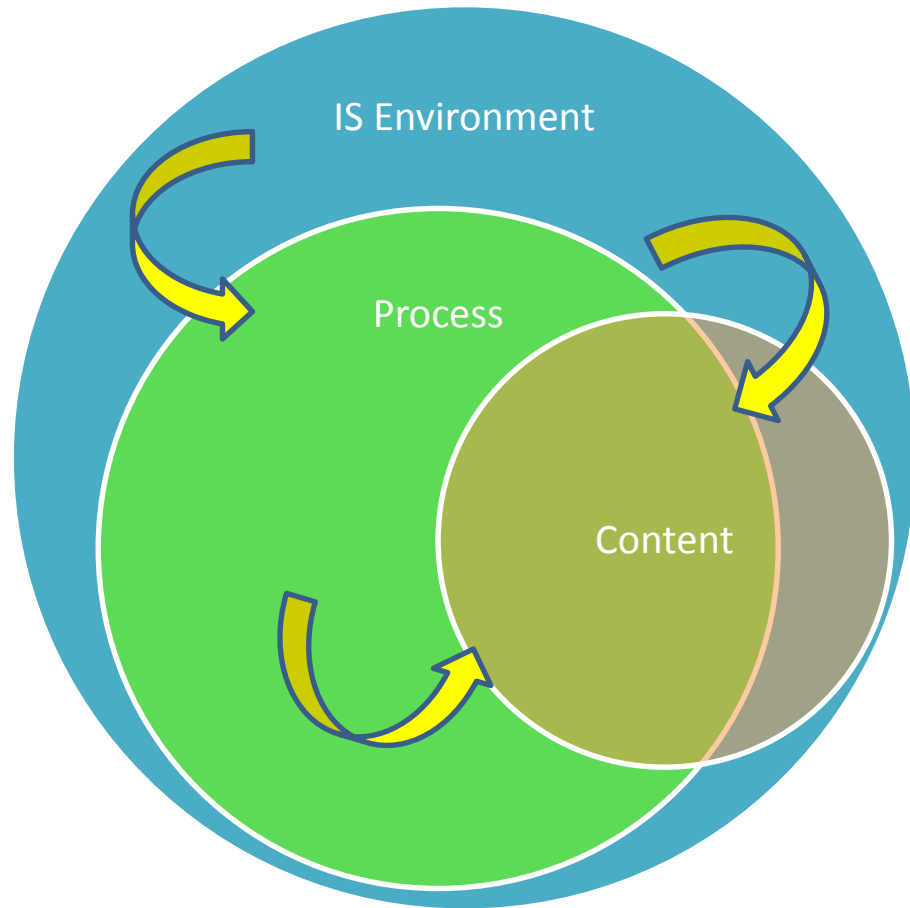
Information and its Attributes

UW CISA

Information Integrity Risks

Information Integrity Enablers, Controls and Impairments

Information Integrity Enablers and Controls

Domains/Risks	Enablers	Controls
Content Creation, Operation and Change Risks	• Selection of Media; • Creation, Change, Management of Data and Metadata	• Evaluate Media • Controls over Creation, Change, and Management of Data and Metadata
Process Creation, Operation and Change Risks	• Input, Processing, Output and Storage Features	• Controls over Input, Processing, Output and Storage
Environment Creation, Operation and Change Risks	• Information governance practices • Information creation practices to get fit for purpose • Security practices to protect the information against unauthorized creation, change and destruction • Availability processes to ensure the information is available to and accessible by authorized users • Dependability practices to ensure predictable ops • Standards to ensure consistency of info production • Verifiability features (audit trails) to enable verification • Assurance services to add credibility to assertions about information integrity.	• Controls over governance practices • Controls over fit for purpose • Controls over security • Controls over availability • Controls over dependability • Controls over compliance with stds • Controls over existence and effectiveness of audit trails • Controls over quality of assurance services on assertions about information integrity.

Assurance on the Integrity of Data/Information

A data/information integrity attestation engagement is performed in accordance with assurance/attestation standards

- Canada – CSAE 3000/3001

- International - ISAE 3000; IAASB Consultancy Paper on Extended External Reporting (EER) Feb 2019; IR; many others

- US - AT-C section 105, Concepts Common to All Attestation Engagements

- Other initiatives – UK; France; Spain; other EU; etc.

Criteria for Describing Data/Information 1

A data/information integrity attestation engagement requires

- Criteria

    - Attributes of suitable criteria are:*

        a. Relevance. Criteria are relevant to the subject matter.

        b. Objectivity. Criteria are free from bias.

        c. Measurability. Criteria permit reasonably consistent measurements, qualitative or quantitative, of subject matter.

        d. Completeness. Criteria are complete when subject matter prepared in accordance with them does not omit relevant factors that could reasonably be expected to affect decisions of the intended users made on the basis of that subject matter.

* EER: a) Relevance; b) Completeness; c) Reliability; d) Neutrality; and e) Understandability.

Criteria for Describing Data/Information 2

For a set of data/information to have integrity, there has to be:

a. A definition/description of the data/information that identifies the:

    a. relationship between members of the set,

    b. the factors that determine inclusion or exclusion possible members of the set,

    c. elements of data/information related to each member of the set and

    d. characteristics of those elements.

b. Consistency between the data/information and the definition/description.

Data/Information is consistent with its definition/description if…

- Each member of the set of data is appropriately included in the population of the events or instances represented by the set of data.

- No events or instances that should be included in the population are omitted from the set of data.

- No events or instances that should not be included in the population are included in the set of data.

- The elements of each member of the set of data/information are
  - complete
  - accurate
  - valid
  - current
  based on the definition and intended use.

UW CISA

Criteria for Evaluating Data/Information Integrity

1: The description of the set of data/information includes the intended use of the data/information.

2: The description of the set of the data/information includes the following:
- **a. The population of events or instances included in the data/information**
- **b. The nature of each element (field) of the data (that is, the event or instance to which the data element relates)**
- **c. The sources of the the data/information**
- **d. The units of measurement of the data/information elements**
- **e. The accuracy, correctness, or precision of measurement**
- **f. The uncertainty or confidence interval inherent in each the data/information element and in their population**
- **g. The time periods over which the the data/information was measured or the time during which the events occurred**
- **h. The factors in addition to date or period of time that determined the inclusion or exclusion of items**

3: The description of the set of the data/information is complete and accurate.

4: The description of the data/information identifies any information that has not been included but is necessary to understand the data/information elements and the population for the intended purpose.

5: The description is provided with the set of the data/information or is otherwise available to users.

6: The data/information is consistent with its description.

Assurance Procedures 1

- Preconditions to accepting engagement

- Planning

- Risk Assessment

- Analytical review

- Detailed testing

- Reporting

Assurance Procedures 2

- Preconditions to accepting engagement
  - Subject matter suitable
  - Criteria exist and are available to intended users
  - Expertise available
  - Ethical requirements met
  - Evidence can be obtained
  - Likelihood of completion

- Planning
  - Scope
  - Materiality
  - Need for Specialists
  - Data sources

Assurance Procedures 3

- Risk Assessment
  - Inherent risk
  - Control risk (environment, process, content)
- Analytical review
  - Relationships – time series; cross-sectional
- Detailed testing through
  - Inspection
  - Confirmation
  - Tracing
  - Vouching
  - Recalculation
  - etc.

Assurance Procedures 4

- Reporting
  - On an assertion by the responsible party vs. directly on the data/information
  - Point in time vs. Period of time
- Description of Data/Information
- Description of Criteria Used
- Format
  - Binary; Non-Binary – graded; maturity level; etc.
  - Short form
  - Long form; factors considered; tests conducted; findings
- Inherent limitations

- Signature

UW CISA

Questions? Comments?