Integrity: definition, subdivision, challenge

Leon Strous
Gistel 20
5707 GV Helmond
The Netherlands
telephone: +31 20 5242748 / +31 492 548636
fax: +31 492 548636
e-mail: strous@iaehv.nl

Abstract

This discussion paper gives the definitions of integrity and internal control as they are used by IFIP TC-11 Working Group 11.5. A subdivision of areas where integrity requirements and measures are in place, is presented. The paper concludes with a challenging statement to start the panel session of the working conference.

Keywords

Integrity, internal control, definitions, subdivision, challenge, standards

1 INTRODUCTION

This paper is a discussion paper to start the panel session of the IFIP TC-11 Working Group 11.5 First Working Conference on Integrity and Internal Control in Information Systems (4-5 December, Zürich, Switzerland). The paper is the result of many discussions with and contributions by members of the working group. In chapter 2. the definitions of integrity and internal control as they are used by this working group are presented. In chapter 3. a subdivision of areas where integrity requirements play a role, is given. Chapter 4. contains a challenging statement to start the discussion between the conference participants and the panel members. The annex is a collection of several definitions found in literature.

2 DEFINITION

There are as many definitions of integrity as there are books and guidelines on security and audit, maybe even more. They all differ more or less. We will not try to find the ultimate definition, because there will always be someone who doesn't

Integrity and Internal Control in Information Systems Volume 1
S. Jajodia, W. List, G. McGregor & L. Strous (Eds)

agree. The definition we present here is the one we use within the working group as a basis for our activities. We look at integrity as a broad concept and place it in a broad perspective. The broad concept will be illustrated in this paragraph by the definition, the broad perspective will be illustrated in the next paragraph by the subdivision of areas for integrity requirements.

A very interesting statement can be found in "The NIST Handbook: An introduction to computer security" (NIST 1995; for the definition see Annex 1), where they start with giving a definition of integrity used by lays (which is the term used by NIST for persons that are non IT security experts; working group 11.5 prefers the term users (which includes managers) as opposed to experts on IT and on security, audit and control). Although the NIST definition is referring to information integrity, which doesn't include for example system integrity, it is a broad definition. The interesting thing is that they proceed with narrowing it down when presenting a definition by security experts.

Since we believe that it is time to effect a paradigm shift from the IT (security) experts view towards the user's view of security, our definition is closer to the "lay" definition than that of the security experts. Based upon and influenced by many definitions in standards, handbooks and guidelines we have come to the following definition as a basis for the working groups activities:

"*Integrity is a quality aspect.* We have made a distinction between data integrity, integrity of information, integrity of systems and integrity of persons. More in detail, integrity implies that:

a. when referred to information:
   - information is timely - it is there when required;
   - information is current - it represents the real world at the time required;
   - information is accurate - it is sufficiently right at the time of use for the purpose it is used for;
   - information is complete; the information needed is all there and what is not there and should be, is known;
b. when referred to data (stored or transmitted):
   - data are accurate - no accidental or deliberate changes have been / can be made without this being noticed;
   - data are complete - no accidental or deliberate deletions or additions have been made without this being noticed, for the period for which the data is required to be kept;
c. when referred to systems:
   - a system processes the data provided in accordance with business requirements at all times, free from deliberate or accidental manipulation of the system.
d. when referred to persons:
   - people are of sound moral principle; they are upright, honest and sincere and have the desire to do the right thing, to profess and live up to a set of values and expectations."

The main issue is information integrity. Information is what the users (including the line managers) need to perform their tasks and control the business processes. **Integrity of systems, data and persons are all prerequisites to achieve integrity of information.**

Definitions of internal control are less common then integrity definitions. Most of them can be found in accounting literature. The working group uses the following definition:
"Internal control is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- effectiveness and efficiency of operations;
- reliability of information processing and reporting;
- compliance with applicable law and regulations."

This definition is to a large extent derived from the report *Internal control - Integrated Framework (COSO, 1992).* Only with respect to the second category, an adjustment has been made (originally it read: reliability of financial reporting).

The definition reflects certain fundamental concepts:

- internal control is a process;
- internal control is effected by people, supported by automation as required;
- internal control can be expected to provide only reasonable assurance.

The relationship between integrity and internal control is illustrated by one of the conclusions in the working paper "Integrity in information systems" (List/Melville, 1994):

> "It is unacceptable in the context of Internal Control theory to rely on assumptions that cannot be justified. System designers and users must therefore ensure that the capability to justify the assumption of integrity of information is provided by the systems."

More specifically, this means that all measures, whether technical or procedural, that preserve integrity, whether for data, information, systems or persons, must be constructed in such a way that their operation can be demonstrated to be correct.

3 SUBDIVISION

The working group places integrity in a broad perspective. To be able to identify where measures are appropriate, we divide the information processing environment in several areas. We prefer to speak about information processing environment rather than information technology environment in order to illustrate that this environment includes also procedures and people. This is illustrated by the following figure, that has been derived from a figure used in a publication by the Royal Dutch Institute of Chartered Accountants (NIVRA). Although the figure

originates from a centralized (mainframe) information processing environment, we believe that by referring to functions rather than to departments or organizations, the figure is also applicable to decentralized or even distributed information processing environments and the answer to the question where and by whom these functions are performed, depends on the specific situation for a company or organization.

The figure is in the first place meant as a model for automated information processing systems, but if the areas of the technical infrastructure (operating system, dbms, etc.) are removed, the model is also applicable for manual information processing systems.

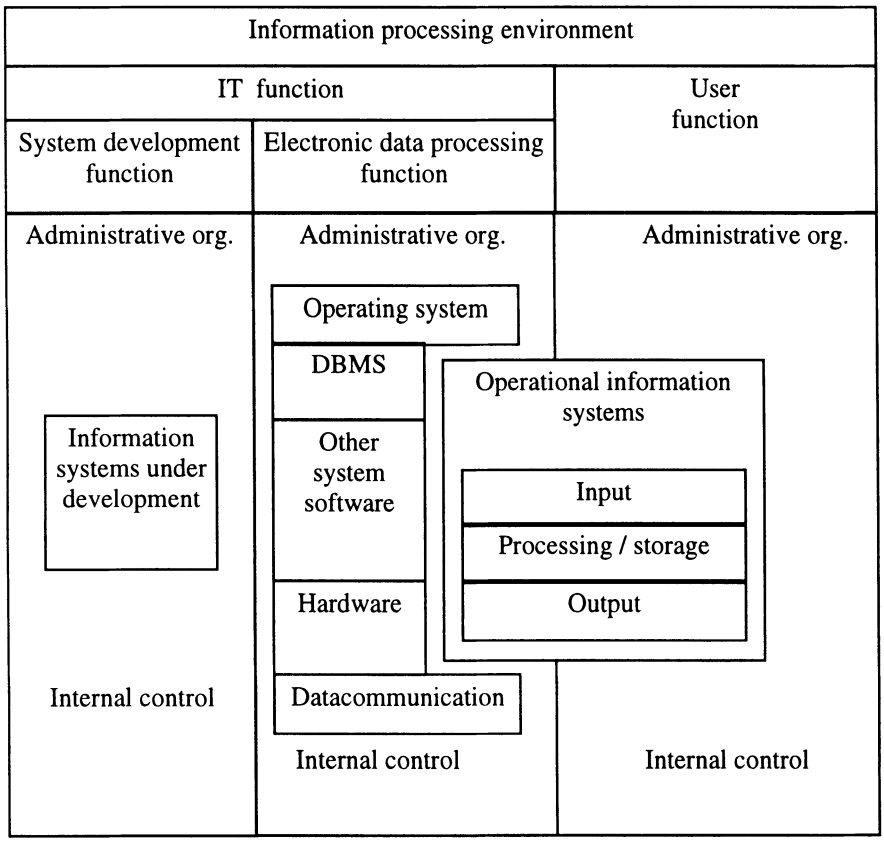

Figure 1. Information processing environment

The broad perspective means that all the different areas of this figure have to be taken into consideration when deciding for a specific situation if and where integrity requirements are in place and where measures can be taken to meet these

requirements. It should be noted that sometimes it may well be possible to compensate missing measures in one area by additional measures in another.

This leads us to the following subdivision of areas where integrity requirements and measures have to be assessed. This subdivision is meant to be of assistance in identifying where and what requirements and measures are necessary and possible to assure the integrity of information.

Subdivision:

E.00 Environment
E.01 Overall procedure / cohesive combination of procedures
A.00 IT function
A.01 Technical measures, e.g. separation of environments
A.02 Procedural, e.g. supervision
AS.01 System development function
AS.02 Technical, e.g. development tools
AS.03 Procedural, e.g. change management
AD.01 Electronic data processing function
AD.02 Procedural measures in the organization
AD.03 Technical measures in:
AD.04 Operating system
AD.05 Database management system
AD.06 Other system software
AD.07 Hardware
AD.08 Datacommunication
AD.09 Application software
U.00 User function
U.01 Technical, programmed controls in software
U.02 Procedural controls concerning input, processing / storage, output

4 CHALLENGE

Working group 11.5 considers it one of it's main activities to make an inventory (or to identify) whether sufficient attention is paid to all the areas in the above subdivision by researchers and developers of solutions, systems, products and standards. Second, it is a task to identify whether the requirements demanded by managers and accountants / auditors form a coherent set and cover all areas.

At this point we would like to challenge the panel members with the following statement:

> **Current security, audit, evaluation and software engineering standards cover integrity only to a limited extent, if at all. This means they cover only a narrow definition, one or only a few parts of the subdivision of the information processing environment (as given in chapter 3) and pay only a little attention to it.**

5 REFERENCES

Biene-Hershey, Margaret van (1996) IT Auditing, an object-oriented approach, Delwel, Den Haag / The Netherlands

BSI (1995) Code of Practice for Information Security Management, BS7799

COSO (1992) Commission of Sponsoring Organizations of the Treadway Commission, Internal control - Integrated Framework

ISACA (1996) Control Objectives for Information and related Technology: COBIT

ISO (1996) Banking, securities and other financial services - Information security guidelines, ISO TR 13569

ISO (1996) Guidelines for the Management of Information Techonology Security: GMITS, ISO DTR 13335-1

ISO (1996) Information technology - Vocabulary. Part 8: Security, ISO DIS 2382-8

List, William and Melville, Rob (1994) Integrity in Information Systems, City University, London, UK

NIST (1995) An introduction to computer security: The NIST Handbook, final draft

NIVRA (1982) Automatisering en Controle deel IVMededelingen door de accountant met betrekking tot de betrouwbaarheid en continuïteit van geautomatiseerde gegevensverwerking, NIVRA Geschrift 26, Amsterdam, The Netherlands

OECD (1992) Guidelines for the security of information systems

Russell, Deborah and Gangemi Sr., G.T. (1991) Computer Security Basics, O'Reilly & Associates, Sebastopol, California, USA

ANNEX 1. COLLECTION OF DEFINITIONS

- Integrity: in lay usage, information has integrity when it is timely, accurate, complete and consistent. However, computers are unable to provide or protect all of these qualities. Therefore, in the computer security field, integrity is often discussed more narrowly as having two facets: data integrity and system integrity. Data integrity is a requirement that information and programs are changed only in a specified and authorized manner. System integrity is a requirement that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. The definition of integrity has been, and continues to be, subject of much debate among computer security experts. *(An introduction to computer security: The NIST Handbook, final draft, March 16, 1995)*
- Integrity means the characteristic of data and information being accurate and complete and the preservation of accuracy and completeness. *(Guidelines for the security of information systems, OECD, 1992)*
- Integrity: relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations. *(Control Objectives for Information and related Technology: COBIT, Information Systems Audit and Control Association: ISACA, April 1996)*
- Integrity: element of information security. Information security: protection of information for b) integrity: safeguarding the accuracy and completeness of information and computer software. *(Code of Practice for Information Security Management, BS7799, BSI, 1995)*
- Integrity: a state in which data is being maintained according to explicitly defined standards for completeness, correctness and timeliness. *(IT Auditing, an object-oriented approach. Margaret van Biene-Hershey, 1996, Delwel)*
- A secure computer must maintain the continuing integrity of the information stored in it. Accuracy or integrity means that the system must not corrupt the information or allow any unauthorized malicious or accidental changes to it. *(Computer Security Basics, Deborah Russell and G.T. Gangemi Sr., O'Reilly & Associates., 1991)*
- Integrity: data integrity: the property that data has not been altered or destroyed in an unauthorized manner. system integrity: the property that a system performs its intended function in an unimpaired manner, free from deliberate or accidental unauthorized manipulation of the system. *(Guidelines for the Management of Information Techonology Security: GMITS, ISO DTR 13335-1, July 1996)*
- Integrity: quality of information or a process which is free from error, whether induced accidentally or intentionally. Software integrity: confidence that the software being used performs only the functions for which it was purchased or developed. *(Banking, securities and other financial services - Information security guidelines, ISO TR 13569, November 1996)*
- Data integrity: the property of data whose accuracy and consistency are preserved, regardless of changes made. System integrity: the quality of a data

processing system fulfilling its operational purpose while both preventing unauthorized users from making modifications to or use of resources and preventing authorized users from making improper modifications to or improper use of resources. *(Information technology - Vocabulary. Part 8: Security, ISO DIS 2382-8, December 1996).*

- Information is sufficiently right at the time of use for the purpose to which the user wishes to put the output. *(Integrity in Information Systems, List / Melville, October 1994)*

- Internal control is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: - effectiveness and efficiency of operations; - reliability of financial reporting; - compliance with applicable law and regulations. *(Internal control - Integrated Framework (Committee of Sponsoring Organizations of the Treadway Commission (COSO), September 1992)*
- Internal control is actions taken by management to plan, organize and direct the performance of sufficient actions so as to provide reasonable assurance that the following objectives will be achieved: - the accomplishment of established objectives and goals for operations and programmes; - the economical and efficient use of resources; - the safeguarding of assets; - reliability and integrity of information; - compliance with policies, plans, procedures, laws and regulations. *(Institute of Internal Auditors: IIA)*