ISACA®
Servire i professionisti dell'IT Governance
Rome Chapter

Dipartimento di Informatica
Facoltà di Scienze M.F.N.
Università di Roma "La Sapienza"

COBIT

CASE STUDY

COBIT come strumento di miglioramento dei processi IT: l'esempio della "Data Governance"

Università degli Studi di Roma – Facoltà di Ingegneria
16 febbraio 2008

NOTE SUL RELATORE :

Enrico Viola - viola@eclat-web.com

- **CISA**
- **Membro del JTC1-SC7 dell'ISO**
- **Co-editor nella norma ISO-IEC 25012**
  Software Engineering – Software product Quality Requirements and Evaluation (SQuaRE) - Data Quality Model
- **Amministratore unico di ECLAT srl**

PROBLEMA :

Impostare un programma di miglioramento per il processo di "DATA GOVERNANCE"

OBIETTIVO:

Raggiungere un livello di maturità del processo tale da aderire alla seguente definizione:

*"**Defined Process**—Procedures have been standardised and documented, and communicated through training. It is mandated that these processes should be followed; however, it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalisation of existing practices."*

VINCOLI :

- Utilizzare un framework per supportare il miglioramento dei processi, riusando competenze, tecniche, attività, strumenti presenti nell'organizzazione
- Limitare al minimo la richiesta di nuove risorse

STRUMENTO SCELTO:

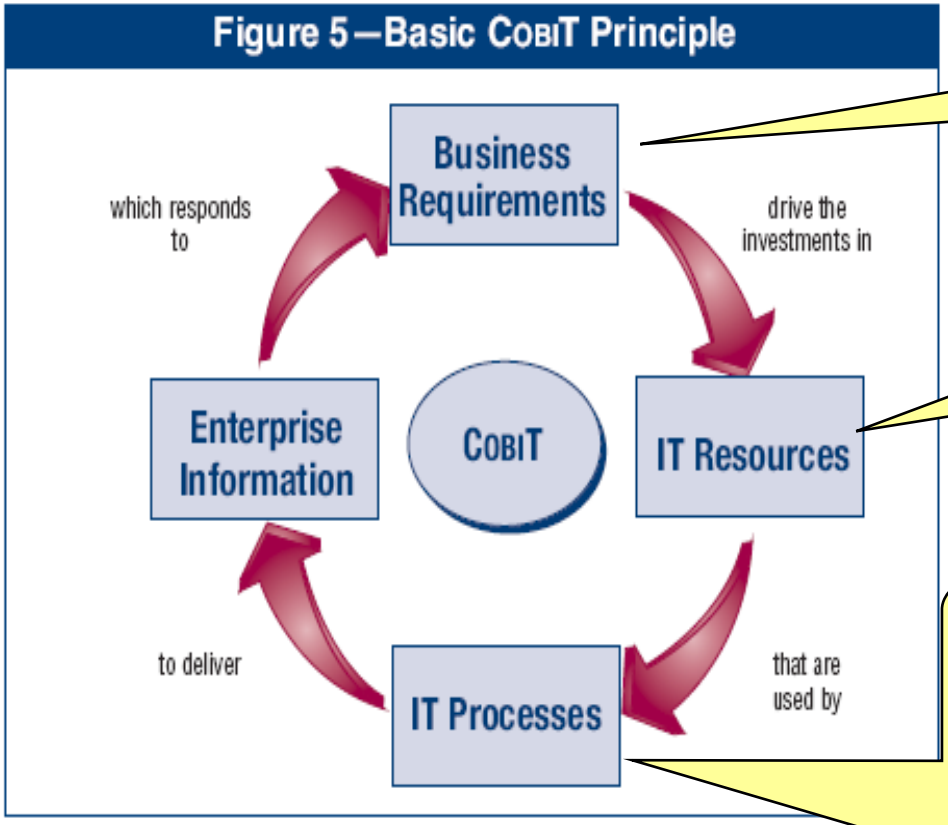
Sulla base di una analisi di mercato la scelta è stata COBIT

PREMESSE:

- COBIT nasce come strumento di audit per i processi IT
- le persone esperte di audit non sono abitualmente coinvolte nell'attività di miglioramento dei processi
- l'organizzazione ha già definito alcuni processi "standard"

Il processo che governa le responsabilità relative alla gestione dell'informazione

(un efficace processo di Data Governance migliora la qualità dei dati)



Disporre di informazioni di qualità per le decisioni di business

Priorità di investimento

DATA GOVERNANCE
P02–Define the Information Architecture
+
D11-Manage Data
+
Data Quality

PO2 Define the Information Architecture

Control over the IT process of

Define the information architecture

that satisfies the business requirement for IT of

being agile in responding to requirements, to provide reliable and consistent information and to seamlessly integrate applications into business processes

by focusing on

the establishment of an ***enterprise data model*** that incorporates a data classification scheme to ensure the integrity and consistency of all data

is achieved by

- Assuring the ***accuracy*** of the information architecture and data model
- Assigning ***data ownership***
- Classifying information using an agreed-upon ***classification scheme***

and is measured by

- Percent of redundant/duplicate data elements
- Percent of applications not complying with the information architecture methodology used by the enterprise
- Frequency of data validation activities

PO2 – Control Objectives

PO2.1 Enterprise Information Architecture Model

Establish and maintain an ***enterprise information model*** to enable applications development and decision-supporting activities, consistent with IT plans as described in PO1. The model should facilitate the optimal creation, use and sharing of information by the business in a way that maintains integrity and is flexible, functional, cost-effective, timely, secure and resilient to failure.

PO2.2 Enterprise Data Dictionary and Data Syntax Rules

Maintain an ***enterprise data dictionary*** that incorporates the organisation's data syntax rules. This dictionary should enable the sharing of data elements amongst applications and systems, promote a common understanding of data amongst IT and business users, and prevent incompatible data elements from being created.

PO2.3 Data Classification Scheme

Establish a ***classification scheme*** that applies throughout the enterprise, based on the criticality and sensitivity (e.g., public, confidential, top secret) of enterprise data. This scheme should include details about data ownership; definition of appropriate security levels and protection controls; and a brief description of data retention and destruction requirements, criticality and sensitivity. It should be used as the basis for applying controls such as access controls, archiving or encryption.

PO2.4 Integrity Management

Define and implement procedures to ensure the *integrity and consistency* of all data stored in electronic form, such as databases, data warehouses and data archives.

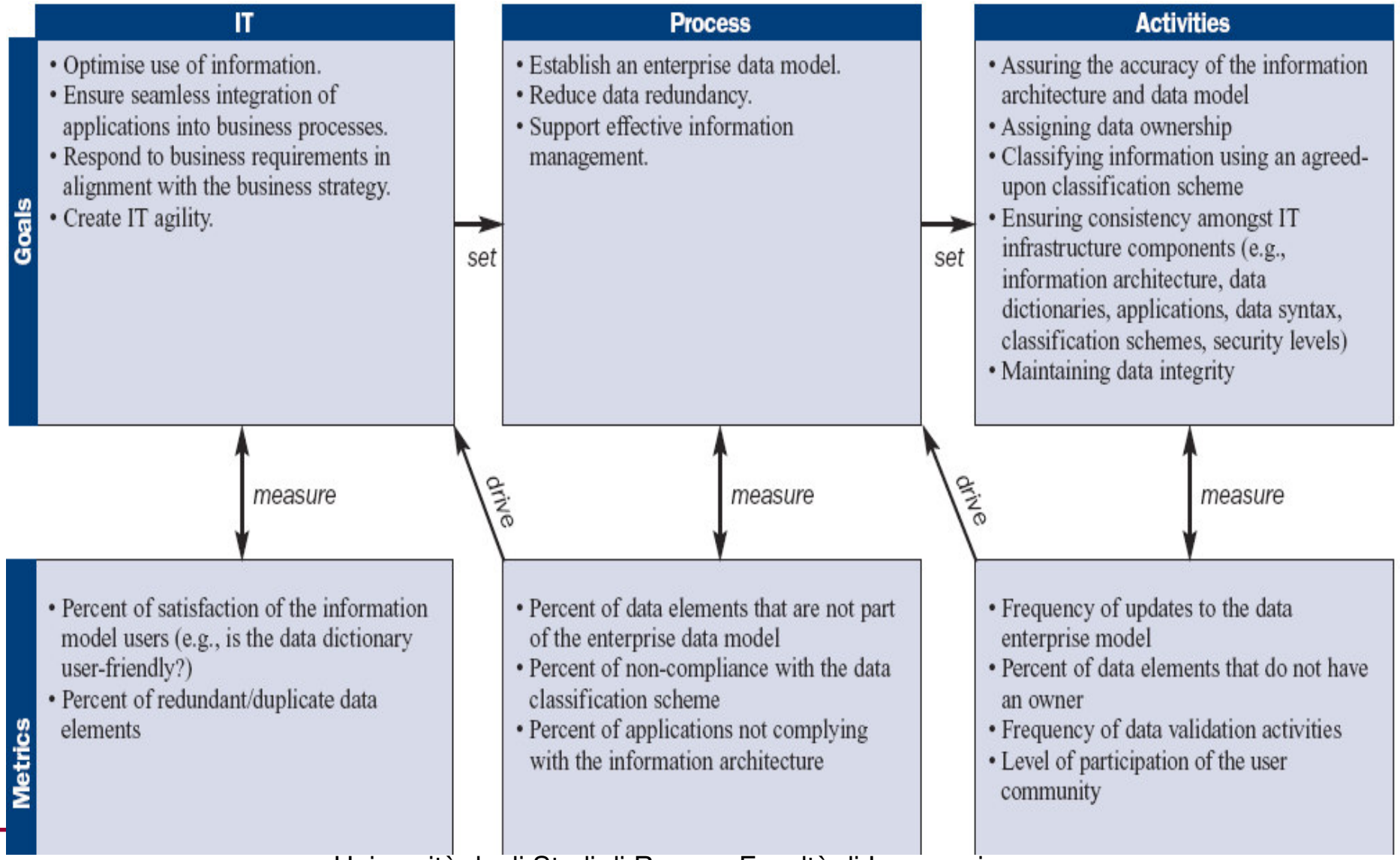
P02- Responsabilità

RACI Chart

Activities \ Functions	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Create and maintain corporate/enterprise information model.		C	I	A	C		R	C	C		C
Create and maintain corporate data dictionary(ies).				I	C		A/R	R			C
Establish and maintain a data classification scheme.	I	C	A	C	C	I	C	C			R
Provide data owners with procedures and tools for classifying information systems.	I	C	A	C	C	I	C	C			R
Utilise the information model, data dictionary and classification scheme to plan optimised business systems.	C	C	I	A	C		R	C			I

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

P02- Obiettivi e Misure



DS11 Manage Data

Control over the IT process of

Manage data

that satisfies the business requirement for IT of

optimising the use of information and ensuring that information is available as required

by focusing on

maintaining the completeness, accuracy, availability and protection of data

is achieved by

- Backing up data and testing restoration
- Managing onsite and offsite storage of data
- Securely disposing of data and equipment

and is measured by

- Percent of user satisfaction with availability of data
- Percent of successful data restorations
- Number of incidents where sensitive data were retrieved after media were disposed

D11 – Control Objectives

DS11.1 Business Requirements for Data Management

Verify that all data expected for processing are received and processed completely, accurately and in a timely manner, and all output is delivered in accordance with business requirements. Support restart and reprocessing needs.

DS11.2 Storage and Retention Arrangements

Define and implement procedures for effective and efficient data storage, retention and archiving to meet business objectives, the organisation's security policy and regulatory requirements

DS11.3 Media Library Management System

Define and implement procedures to maintain an inventory of stored and archived media to ensure their usability and integrity.

DS11.4 Disposal

Define and implement procedures to ensure that business requirements for protection of sensitive data and software are met when data and hardware are disposed or transferred

DS11.5 Backup and Restoration

Define and implement procedures for backup and restoration of systems, applications, data and documentation in line with business requirements and the continuity plan.

DS11.6 Security Requirements for Data Management

Define and implement policies and procedures to identify and apply security requirements applicable to the receipt, processing, storage and output of data to meet business objectives, the organisation's security policy and regulatory requirements.

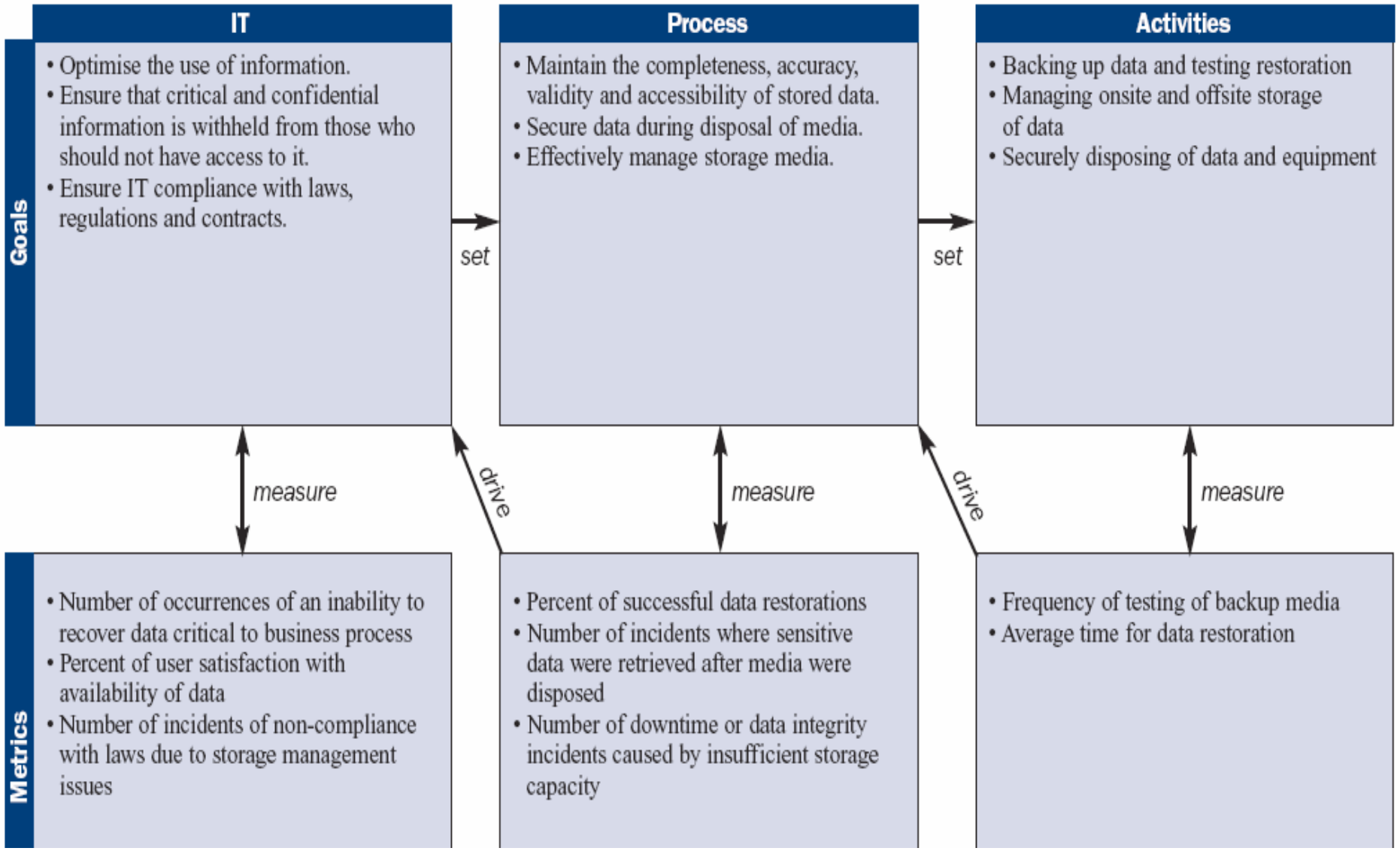
DS11- Responsabilità

RACI Chart

Activities \ Functions	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Translate data storage and retention requirements into procedures.				A	I	C	R				C
Define, maintain and implement procedures to manage the media library.				A		R	C	C	I		C
Define, maintain and implement procedures for secure disposal of media and equipment.				A	C	R			I		C
Back up data according to scheme.				A		R					
Define, maintain and implement procedures for data restoration.				A	C	R	C	C			I

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

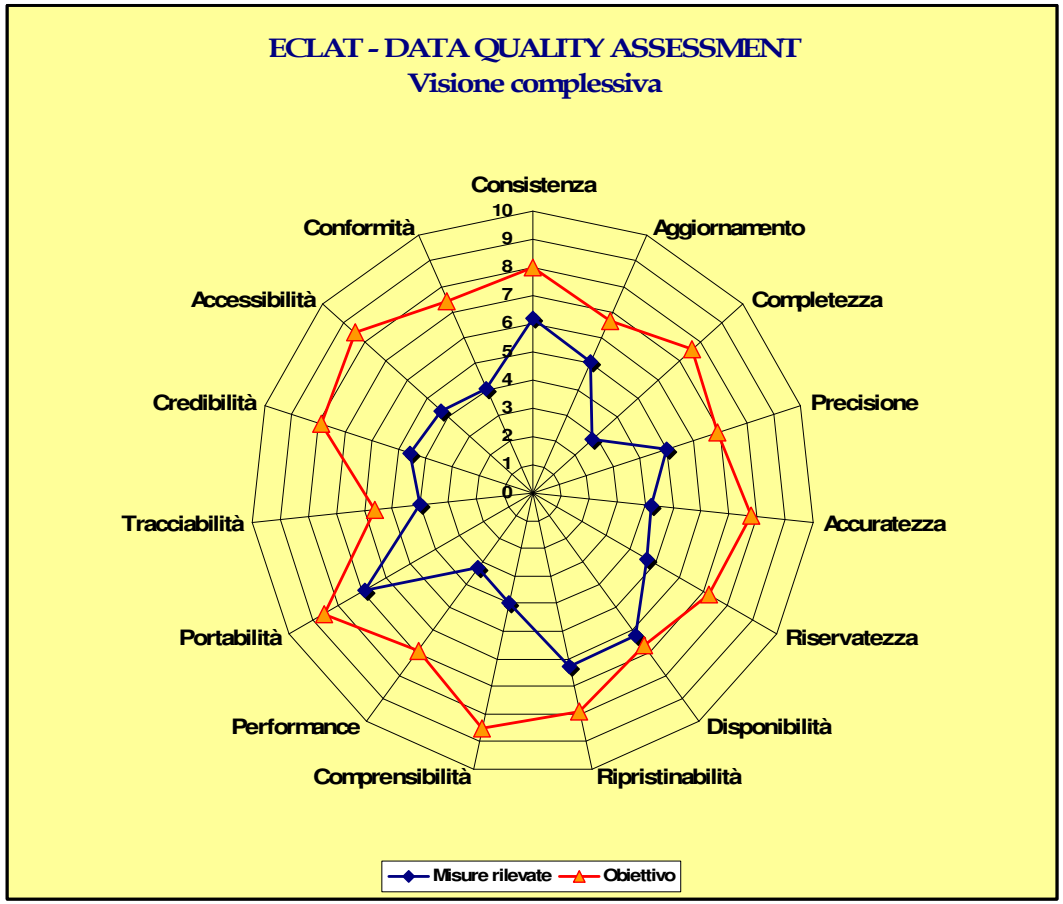
DS11- Obiettivi e Misure



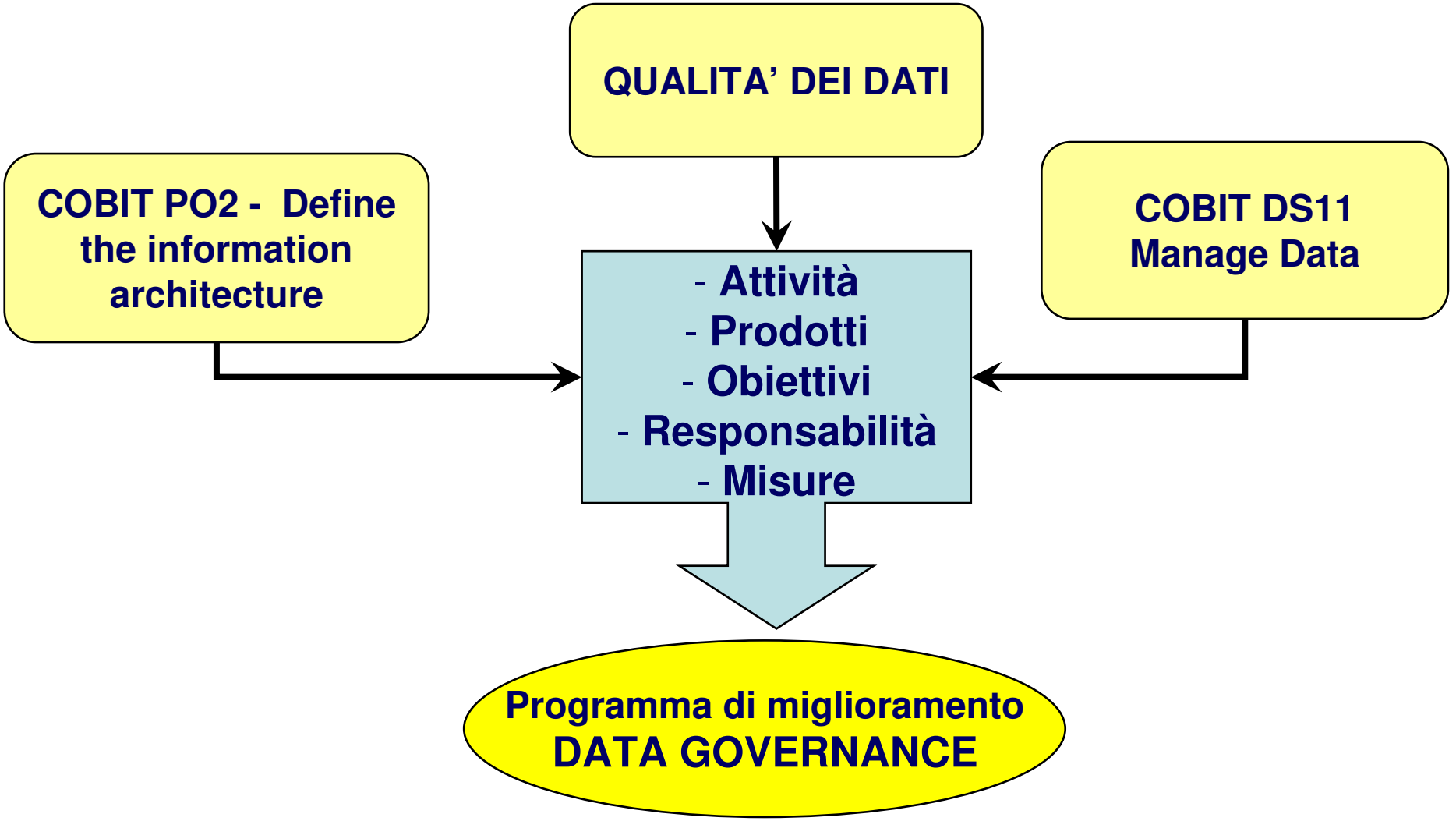
Qualità dei dati - il processo

Qualità dei dati - Misura

	DATA QUALITY	
	Inerente	***Estesa***
Accuratezza	**X**	
Completezza	**X**	
Consistenza	**X**	
Credibilità	**X**	
Aggiornamento	**X**	
Accessibilità	**X**	**X**
Conformità	**X**	**X**
Riservatezza	**X**	**X**
Performance	**X**	**X**
Precisione	**X**	**X**
Tracciabilità	**X**	**X**
Comprensibilità	**X**	**X**
Disponibilità		**X**
Portabilità		**X**
Ripristinabilità		**X**



Sintesi


QUALITA' DEI DATI
COBIT PO2 - Define the information architecture
COBIT DS11 Manage Data
- Attività
- Prodotti
- Obiettivi
- Responsabilità
- Misure
Programma di miglioramento
DATA GOVERNANCE

Link:

www.isaca.org

www.itgi.org

www.isacaroma.it