Digital information governance: selection, organization, long term preservation

- module 2 -

Pierluigi Feliciati

University of Macerata (Italy)

Summer School “Digital Tools for Humanists”

Pisa, June 11th 2019

Laboratorio di Cultura Digitale

ASSOCIAZIONE per l'INFORMATICA UMANISTICA e la CULTURA DIGITALE

UNIVERSITÀ DI PISA

Content in modules

1. Why *Information Governance*?
2. Organizational issues: analysis and actions
3. IG program + Retention/Selection/Appraisal -» Preservation

IG key outputs

A successful IG program should enable organizations to:

1. Use common terms across the enterprise. This means that departments must agree on how they are going to classify document types, which requires a cross-functional effort. With common enterprise terms, searches for information are more productive and complete.
2. Map information creation and usage. This effort can be buttressed with the use of technology tools such as data loss prevention, which can be used to discover the flow of information within and outside of the enterprise. You must first determine who is accessing which information when and where it is going. Then you can monitor and analyze these information flows.

IG key outputs

A successful IG program should enable organizations to:

3. Obtain “information confidence” — that is, the assurance that information has integrity, validity, accuracy, and quality; this means being able to p rove that the information is reliable and that its access, use, and storage meet compliance and legal demands.
4. Harvest and leverage information. Using techniques and tools like data mining and business intelligence, new insights may be gained that provide an enterprise with a sustainable competitive advantage over the long term, since managers will have more and better information as a basis for business decisions.

1. Self-evaluation and assessement

- The ARMA Generally Accepted Recordkeeping Principle (2009/2017) and the Information Governance Maturity Model (2013) can be used as a best-practice framework to evaluate the organizational IRM context and develop a Records Management Strategic Plan and an Information Governance Strategy.
- Moreover, these principles and associated metrics provide an IG framework that can support continuous improvement.

Assessment Report and road map

- As an accepted industry guidance maturity model, the GARP provide a convenient and complete framework for assessing the current state of an organization's recordkeeping and developing a roadmap to identify improvements that will bring the organization into compliance.
- An assessment/analysis of the current RM practices, procedures, and capabilities together with future state practices provides two ways of looking at the future requirements of a complete RM.

The 8 GARP

- Principle of **Accountability**
- Principle of **Transparency**
- Principle of **Integrity**
- Principle of **Protection**
- Principle of **Compliance**
- Principle of **Availability**
- Principle of **Retention**
- Principle of **Disposition**

Figure 12.1. Generally Accepted Recordkeeping Principles.

Source: Adapted from ARMA International, "Generally Accepted Recordkeeping Principles," accessed February 14, 2013, http://www.arma.org/garp/. Courtesy of ARMA International.

The GARP Mnemonic A TIP CARD

GARP - Accountability

(RT responsibility)

- A senior executive (or a person of comparable authority) shall oversee the information governance program and delegate responsibility for information management to appropriate individuals.
- The regulatory and legal framework for RM must be clearly identified and understood. The senior executive must have a sound knowledge of the organization's information and technological architecture and actively participate in strategic decisions for IT systems acquisition and implementation.
- An audit process must be developed to cover all aspects of RM within the organization, including confirming that sufficient levels of accountability have been assigned and accountability deficiencies are identified and remedied.

GARP - Transparency

(RT documentation)

- An organization's business processes and activities, including its information governance program, shall be documented in an open and verifiable manner, and that documentation shall be available to all personnel and appropriate, interested parties.
- To be effective, policies must be formalized and integrated into business processes. Employees must have ready access to RM policies and procedures.
- In addition to policies and procedures, guidelines and operational instructions, diagrams and flowcharts, system documentation, and user manuals must include clear guidance on how records are to be created, retained, stored, and dispositioned.

GARP - Integrity

(RT authenticity and reliability)

- An information governance program shall be constructed so the information assets generated by or managed for the organization have a reasonable guarantee of authenticity and reliability.
- Records integrity, reliability, and trustworthiness are confirmed by ensuring that a record was created by a competent authority according to established processes.
- A formalized process must be in place for acquiring or developing new systems, including requirements for capturing the metadata required for lifecycle management of records in the systems.

GARP - Protection

(RT security)

- An information governance program shall be constructed to ensure an appropriate level of protection to information assets that are private, confidential, privileged, secret, classified, essential to business continuity, or that otherwise require protection.
- The protection of records has to ensure they are unaltered through loss, tampering, or corruption. This includes technological change or the failure of digital storage media and protecting records against damage or deterioration.
- This principle applies equally to physical and electronic records, each of which has unique requirements and challenges.

GARP - Compliance

(RT adherence to policies)

- An information governance program shall be constructed to comply with applicable laws, other binding authorities, and the organization's policies.
- Monitoring for compliance involves reviewing and inspecting the various facets of records management, including ensuring records are being properly created and captured, implementation of user permissions and security procedures, workflow processes through sampling to ensure adherence to policies and procedures, ensuring records are being retained following disposal authorization, and documentation of records destroyed or transferred to determine whether destruction/transfer was authorized in accordance with disposal instructions.

GARP - Availability

(RT access, retrieval)

- An organization shall maintain its information assets in a manner that ensures their timely, efficient, and accurate retrieval.
- Organizations should evaluate how effectively and efficiently records and information are stored and retrieved using present equipment, networks, and software.
- The evaluation should identify current and future requirements and recommend new systems as appropriate. Certain factors should be considered before upgrading or implementing new systems like cost, and effectiveness of new configurations.

GARP - Retention

(RT appraisal, preservation)

- An organization shall maintain its information assets for an appropriate time, taking into account its legal, regulatory, fiscal, operational, and historical requirements.
- Organizations must identify the scope of their recordkeeping requirements for documenting business activities based on regulated activities and jurisdictions that impose control over records.
- Records appraisal is the process of assessing the value and risk of records to determine their retention and disposition requirements. The retention periods for different records should be based on legislative or regulatory as well as on administrative and operational requirements.

GARP - Disposition

(RT archiving, destruction)

- An organization shall provide secure and appropriate disposition for information assets no longer required to be maintained, in compliance with applicable laws and the organization's policies.
- When the retention requirements have been met and the records no longer serve a useful business purpose, records may be destroyed. Records requiring long-term or permanent retention should be transferred to an archive for preservation.
- Destruction of records must be carried out under controlled, confidential conditions and approved methods of destruction must be specified for each media type to ensure that information cannot be reconstructed.

The Information Governance Maturity Model

- The Generally Accepted Recordkeeping Principles maturity model can be leveraged to develop a current state assessment of an organization's recordkeeping practices and resources, identify gaps and assess risks, and develop priorities for desired improvements.
- The model associates characteristics that are typical in five levels of recordkeeping capabilities ranging from 1 (substandard) to 5 (transformational).
- The levels are both descriptive and color coded for ease of understanding. The eight principles and the levels (metrics) are applied to the current state of an organization's recordkeeping capabilities and can be cross-referenced to the policies and procedures.

The Information Governance Maturity Levels

Level 1 Substandard	Characterized by an environment where recordkeeping concerns are either not addressed at all or are addressed in an ad hoc manner.
Level 2 In Development	Characterized by an environment where there is a developing recognition that recordkeeping has an impact on the organization, and the organization may benefit from a more defined information governance program.
Level 3 Essential	Characterized by an environment where defined policies and procedures exist that address the minimum or essential legal and regulatory requirements, but more specific actions need to be taken to improve recordkeeping.
Level 4 Proactive	Characterized by an environment where information governance issues and considerations are integrated into business decisions on a routine basis, and the organization consistently meets its legal and regulatory obligations.
Level 5 Transformational	Characterized by an environment that has integrated information governance into its corporate infrastructure and business processes to such an extent that compliance with program requirements is routine.

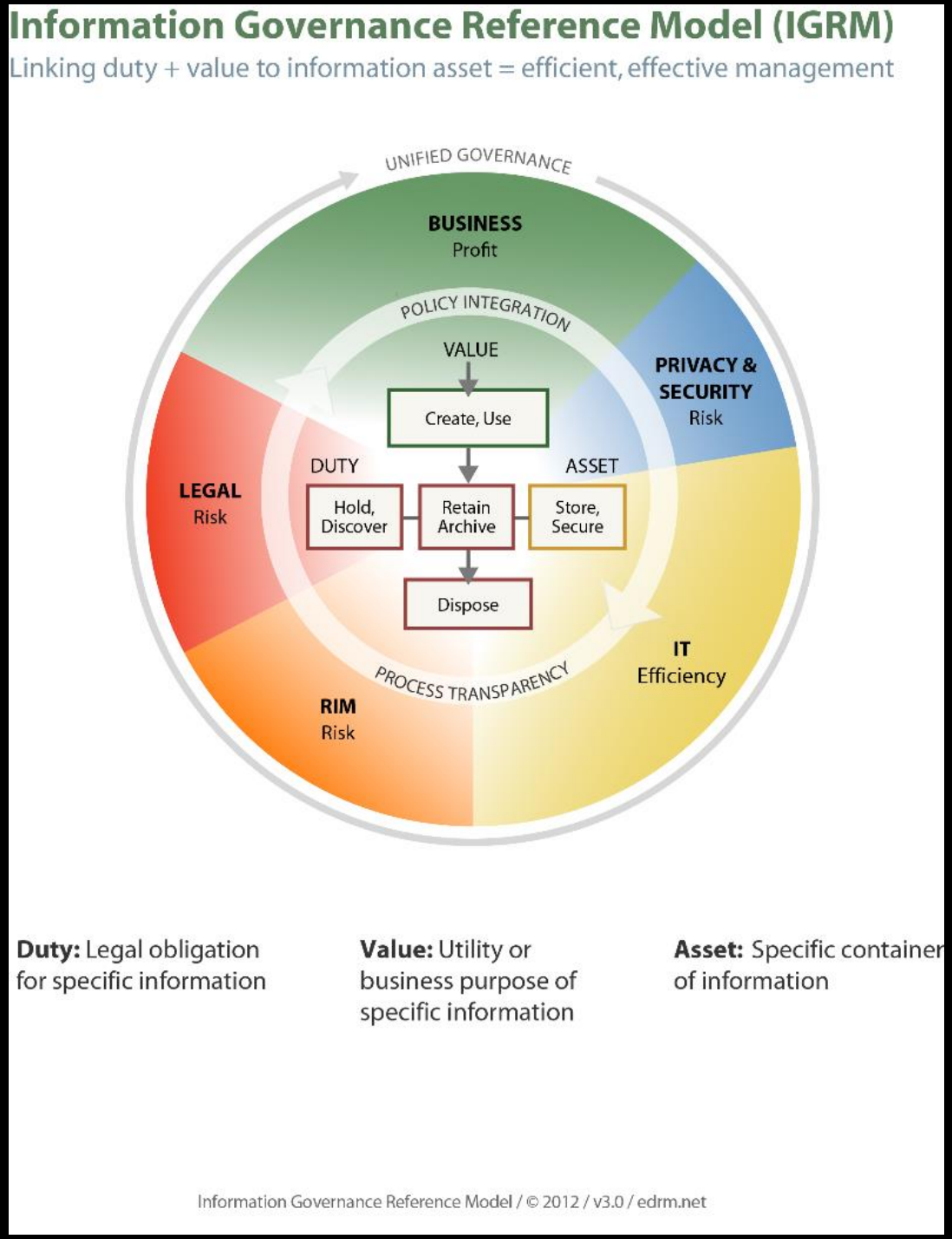
The improvement areas for the GARP

- RM and information governance are business disciplines that must be tightly integrated with operational policies, procedures, and infrastructure.
- The Principles can be mapped to four improvement areas

Improvement Area	Accountability	Transparency	Integrity	Protection	Compliance	Availability	Retention	Disposition
Roles and responsibilities	◊				◊		◊	
Policies and procedures	◊	◊	◊	◊	◊	◊	◊	◊
Communication and training	◊	◊		◊	◊		◊	
Systems and automation	◊			◊	◊	◊	◊	◊

IRG Reference Model for policy development

- To develop an **information governance** (IG) policy, you must inform the policy with internal and external frameworks, models, best practices, and standards—those that apply to your organization and the scope of its planned IG program.
- Using the RK principles and maturity model, organizations can assess where they are in terms of IG, identify gaps, and take steps to improve. Remember? A TIP CARD and the 5 levels of maturity…
- The EDRM (Electronic Discovery Reference Model) project, with the support of GCOC and ARMA released in 2012 the version 3.0 of its IGRM (Information Governance Reference Model) adding Information Privacy and Security as key functions, not covered before



IGRM model

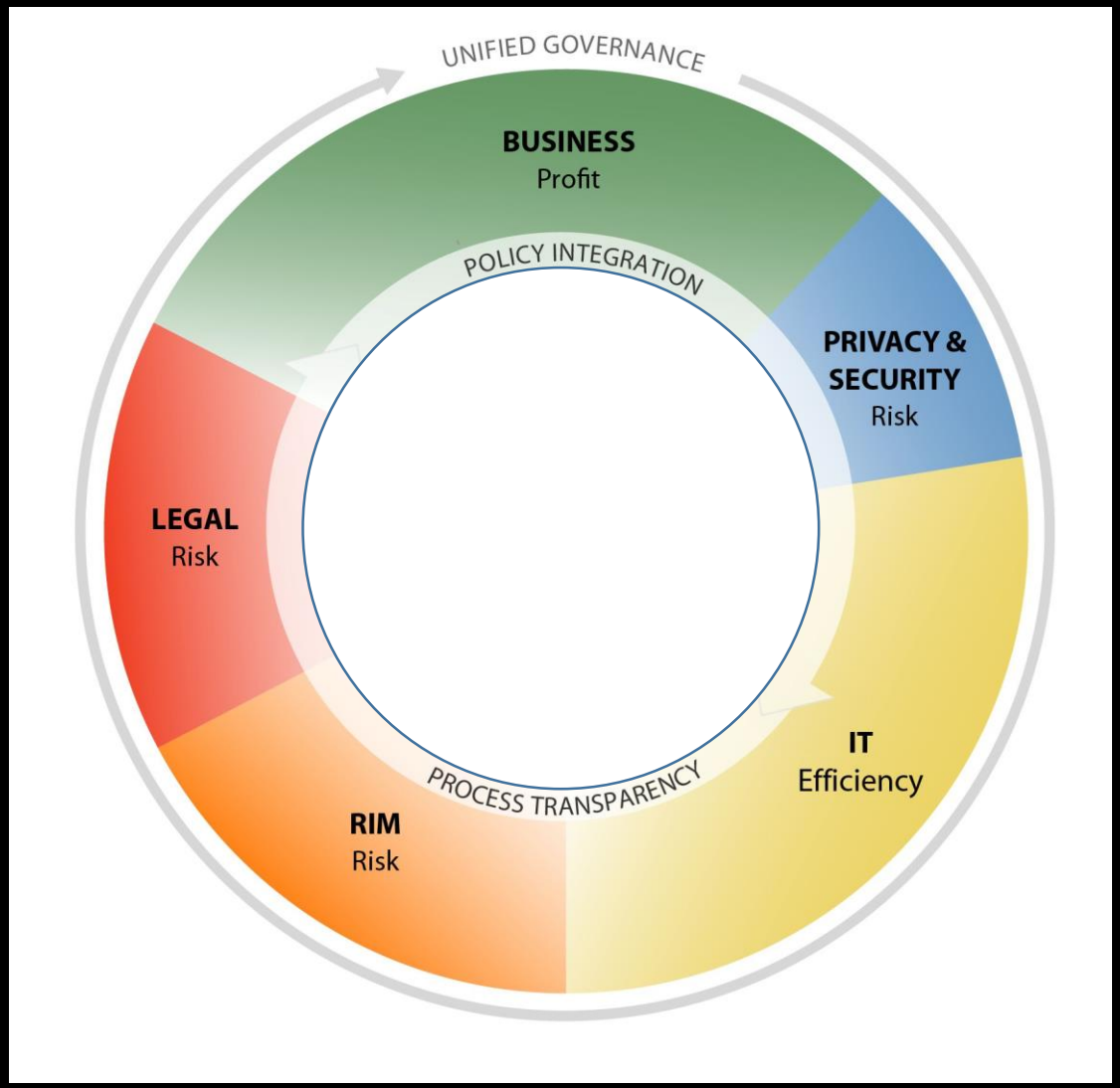
It is aimed at fostering IG adoption by facilitating communication and collaboration between disparate (and often overlapping)

IG functions:

- information technology (IT),
- legal,
- RIM,
- risk management
- business unit stakeholders

The growing CGOC community (2,000+ members and rising) has widely adopted the IGRM and developed a process maturity model that accompanies and leverages IGRM v3.0, complementing GARP.

IGRM model

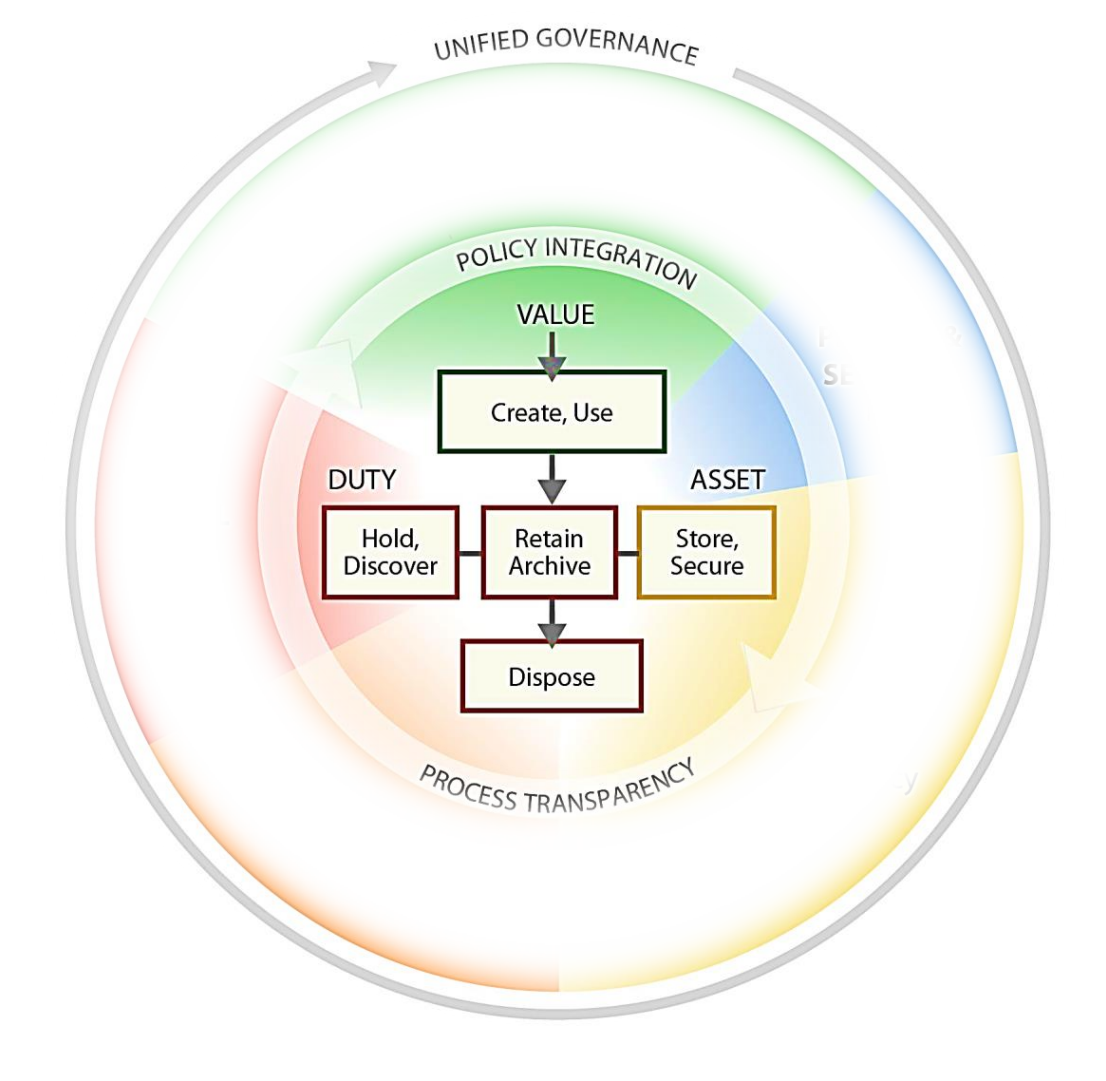


Outer Ring

Starting from the outside of the diagram, successful information management is about conceiving a complex set of interoperable processes and implementing the procedures and structural elements to put them into practice. They are stakeholders, not principles. It requires:

- An understanding of the business imperatives
- Knowledge of the appropriate tools and infrastructure for managing information (Privacy, Security, IT efficiency)
- An efficient RIM strategy, set of policies and plans
- Sensitivity to the legal and regulatory obligations with which the enterprise must comply.

IGRM model

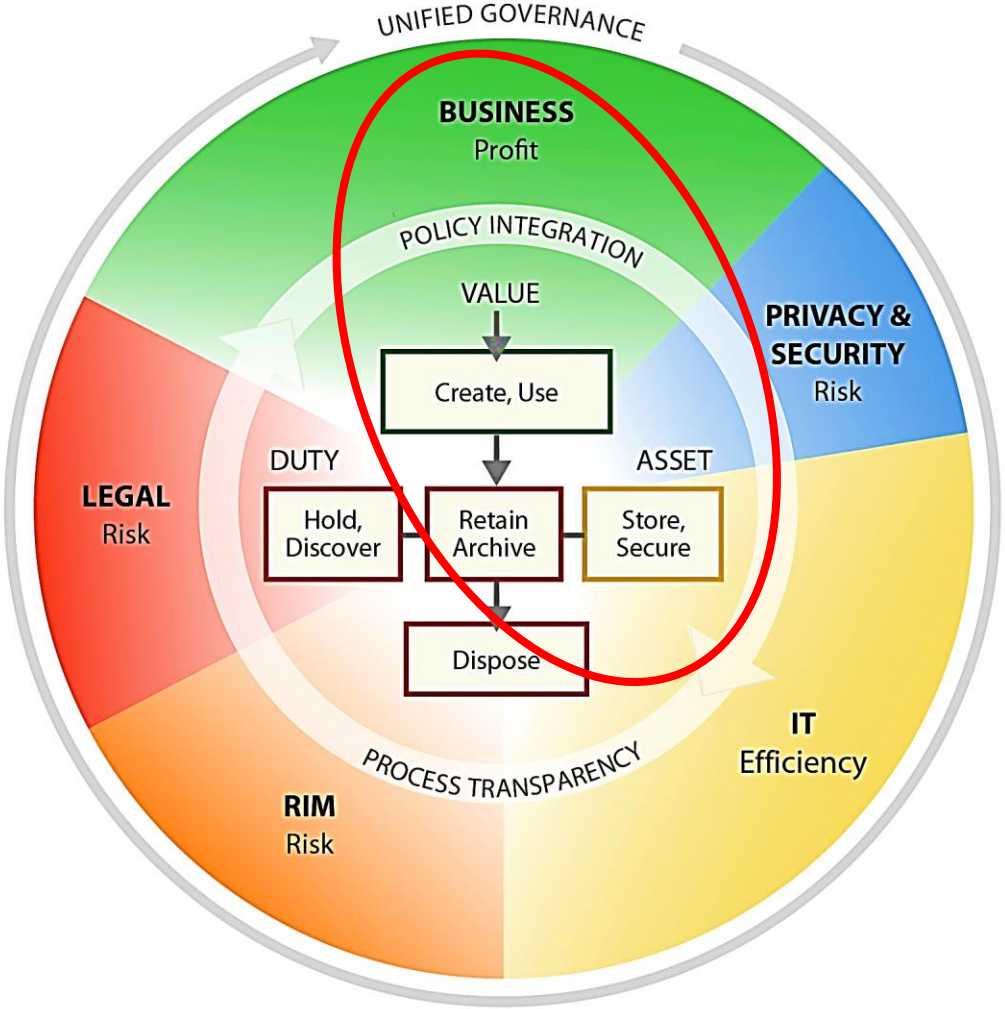


Center circle

In the center of the diagram is a work-flow of **information life-cycle**, to illustrate that *information management is important at all stages of the information life cycle—from its creation through its ultimate disposition.*

The relationship among duty, value, and the information asset demonstrates cooperation among stakeholder groups to achieve the desired level of maturity of effective information governance.

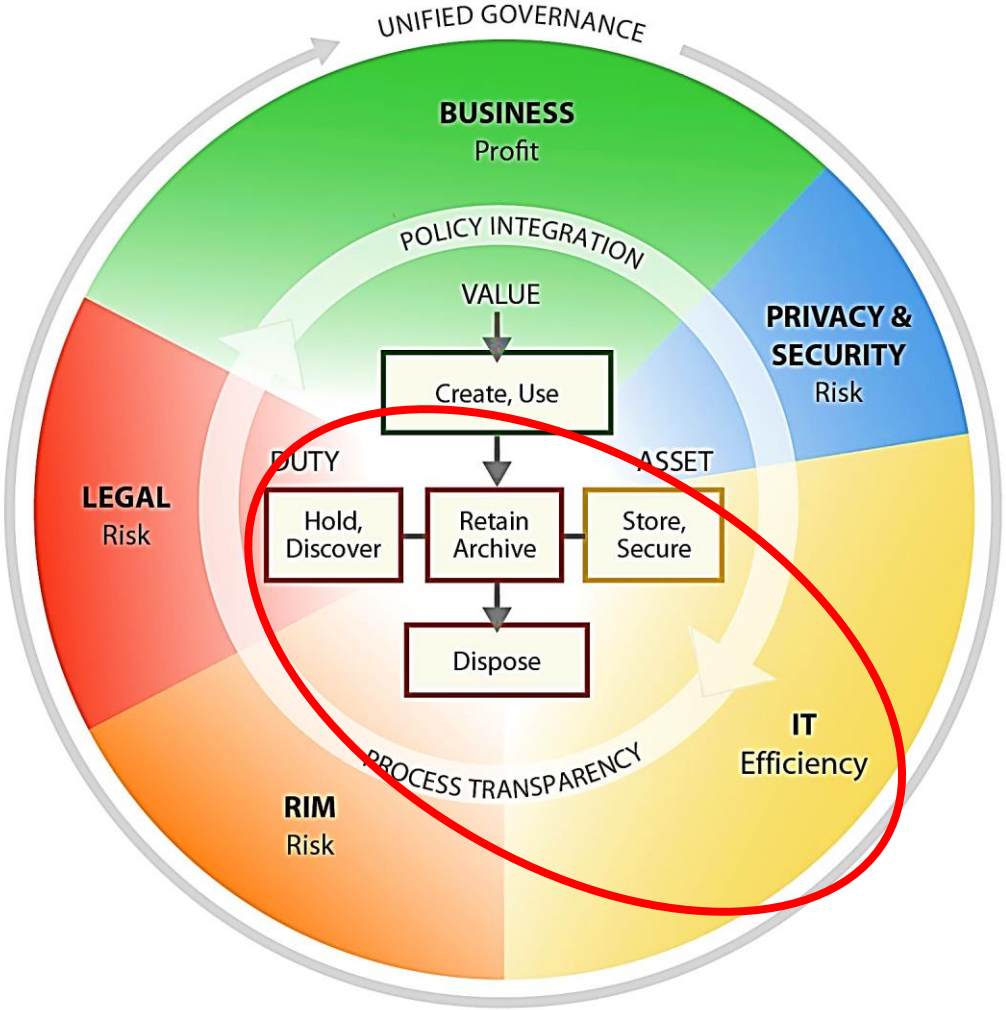
IGRM model



Starting at the top and moving clockwise, the business is responsible for generating revenue, reducing costs and satisfying customers (value). Information is created and used to satisfy those concerns.

Then, organizations have a duty to ensure information is properly handled and personal or confidential information is appropriately protected.

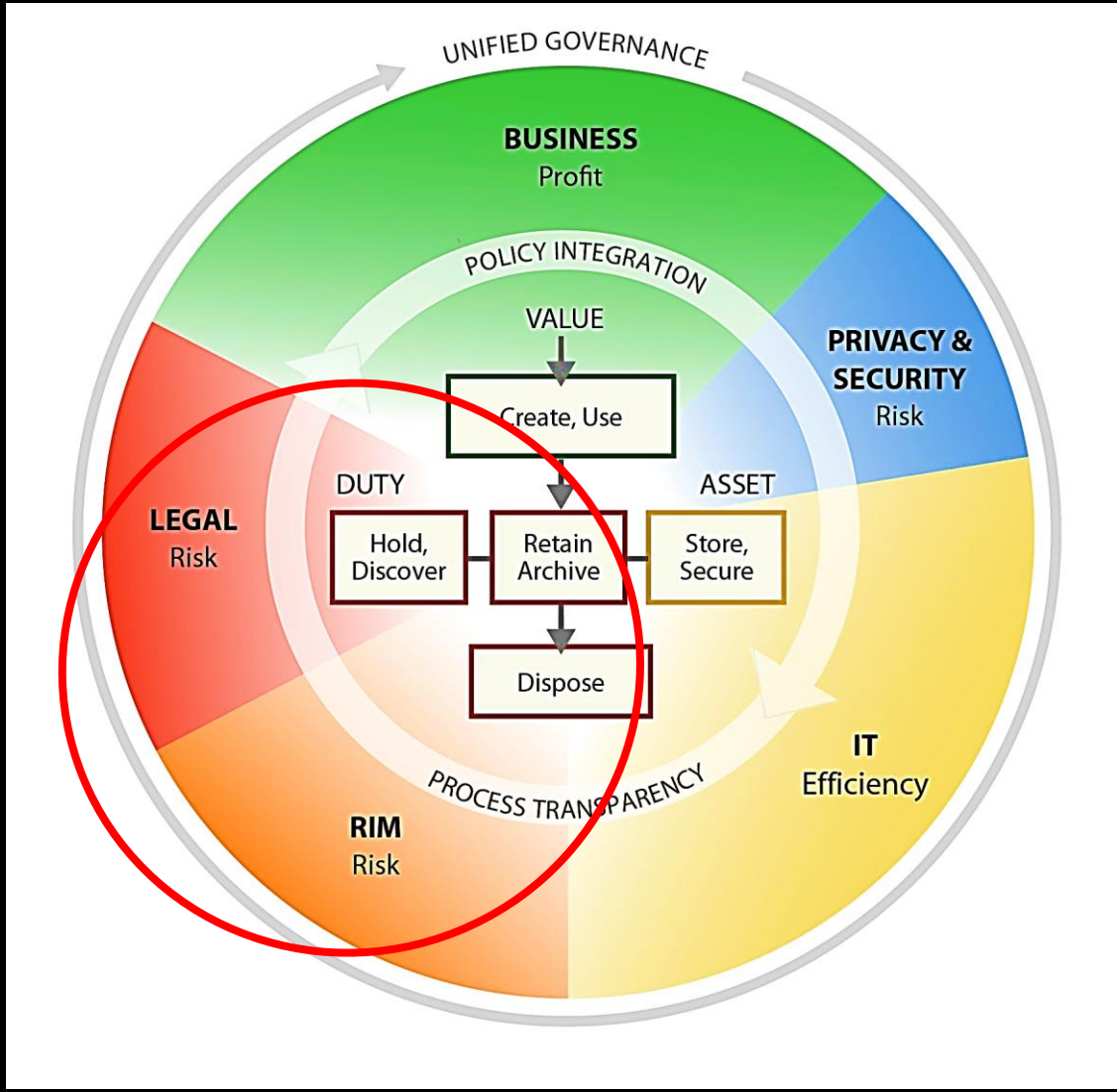
IGRM model



Classifying information for easy retrieval results in faster access while Business is using the information, and classification makes it easier to access data needed for discovery and/or investigation.

As information exists, IT is chartered with *storing* and *securing* information and executing on the requirements established by Legal, RIM, and the Privacy & Security stakeholders for compliance.

IGRM model



As organizations are governed by the laws and regulations in their domains, RIM brings forth the obligations for information and recordkeeping, including what, how, for how long, where, and in what format information is *retained* and *archived*.

Once data is created, it is potentially subject to legal hold and discovery as part of investigations, litigation, or other adversarial proceedings. Organizations need access to information to prove their own claims as well as to defend against claims made against them by customers, employees, competitors, law enforcement/regulators or other adversaries.

The importance of best practices

- Smallwood lists and comments 25 best practices, to be considered in policy formulation.
- Best practices in IG are obviously evolving and expanding, and those that apply to our organizational scenarios may vary. This process of testing, proving, and sharing best practices will continue for some time as the practices are expanded, revised, and refined.
- A best practices review should be conducted, customized for each particular organization, better engaging a third-party consultant, who can more easily contact, study, and interview your competitors in regard to their practices.

Benefits and risks of Standards

There are two types of standards: *de jure* and *de facto*.

- De jure ("the law") standards are those published by recognized standards-setting bodies, such as: the International Organization for Standardization (ISO), American National Standards Institute (ANSI), National Institute of Standards and Technology (NIST—this is how most people refer to it, as they do not know what the acronym stands for), British Standards Institute (BSI), Standards Council of Canada, and Standards Australia.
- De facto ("the fact") standards are not formal standards but are regarded by many as if they were. They may arise though popular use (e.g., Windows business desktop in the last decade) or may be published by other bodies, such as the U.S. National Archives and Records Administration (NARA), ARMA, etc.

Benefits and risks of Standards

Some risks with standards may be:

- Possible decreased flexibility in development or implementation.
- “Standards confusion” from competing and overlapping standards.
- Real-world shortcomings due to theoretical basis.
- Changing and updating requires cost and maintenance.

Benefits and risks of Standards

Some benefits of developing, promoting and apply standards are:

- Quality assurance support.
- Interoperability support.
- Implementation frameworks and certification checklists.
- Cost reduction.
- International consensus.

A (incomplete) list of *de jure* standards for RIG

- ISO 31000 is a broad risk management standard that applies to all types of businesses.
- ISO/IEC 27001 and ISO/IEC 27002 are ISMS standards that provide guidance in the development of security controls.
- ISO 15489 is the international RIM standard.
- DoD 5015.2 is the U.S. ERM standard.
- MoReq2010 is the European ERM standard.
- ISO 16175 offers principles and functional requirements for e-records. It does not contain a testing regime for certification. Australia has adopted all three parts of ISO 16175 as its e-records management standard.
- The ISO 30300 series of e-records standards are written for a managerial audience and encourage ERM that is aligned to organizational objectives.
- ISO 16363 (OAIS) represents the gold standard of audit and certification for trustworthy digital repositories.
- ISO 38500 provides high-level principles and guidance for senior executives and directors responsible for IT governance.

Roles and responsabilities

- Engaged and vested executive sponsors are necessary for IG program success.
- The executive sponsor must be: (1) directly tied to the success of the program, (2) fully engaged in and aware of the program, and (3) actively eliminating barriers and resolving issues.
- While the executive sponsor role is high level, the project manager's role and tasks involve more detailed and day-to-day management.
- The IG team must include a cross-functional group of stakeholders from various departments, including legal, records management, IT, and risk management.
- The IG strategic plan must be aligned and synchronized with the organization's overall strategic plans, goals, and business objectives.

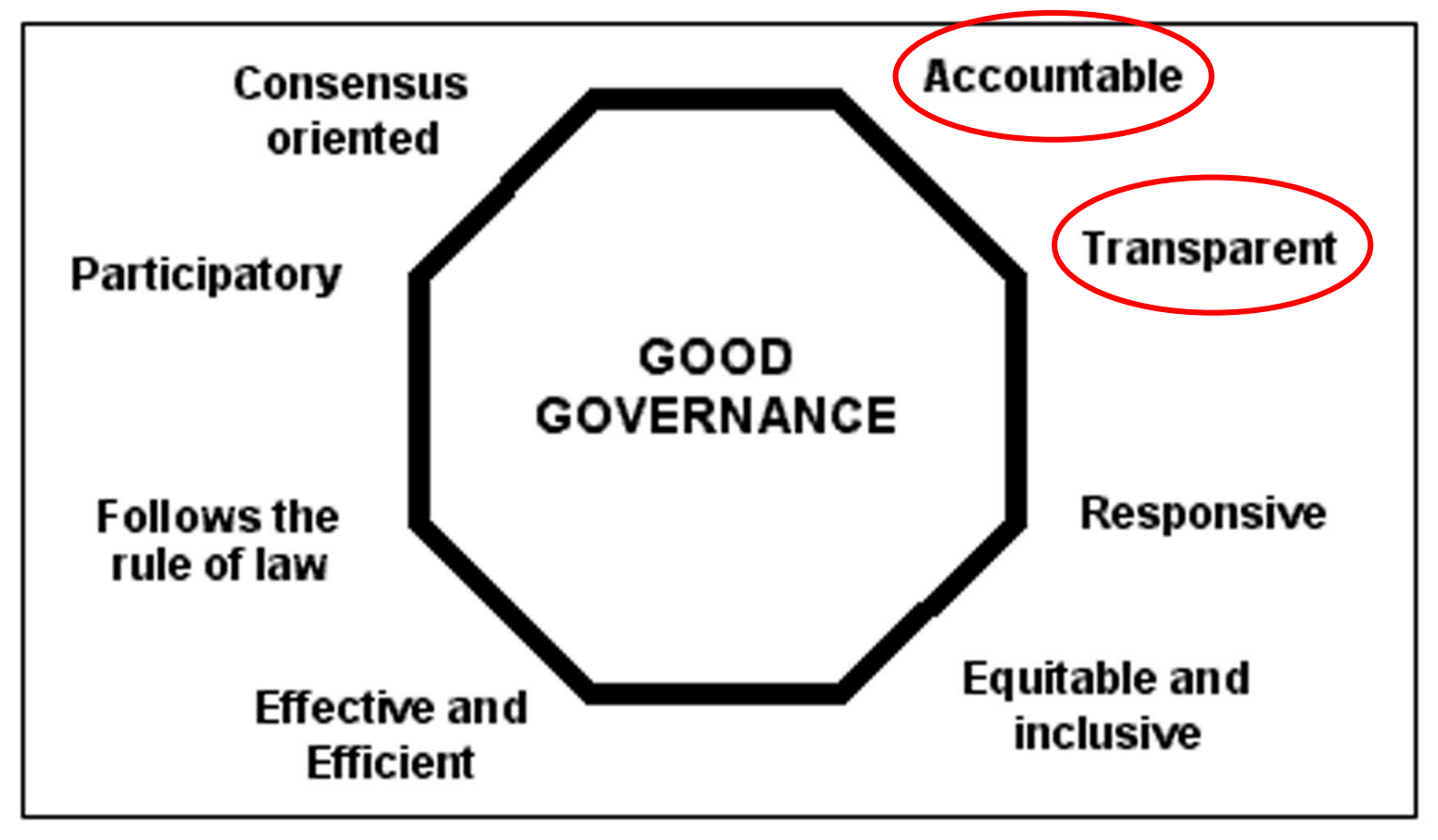
Accountability as a key goal

- The obligation to answer for actions for which one is responsible
- The obligation of an individual or organization to account for its activities, accept responsibility for them, and to disclose the results in a transparent manner.
- A senior executive (or person of comparable authority) shall oversee the information governance program and delegate responsibility for records and information management to appropriate individuals. The organization adopts policies and procedures to guide personnel and ensure that the program can be audited. (See GARP)

Accountability and democracy

- Accountability is partly a matter of institutional design: formal checks and balances can and should be built into any constitutional architecture.
- This is true is true also *within* governments: horizontal accountability depends upon the ability of one part of government to find out—and, where necessary, to stop or correct— what other sectors are doing.
- Those demanding accountability must be confident that they can do so safely, that officials will respond honestly, and that social needs and demands are taken seriously.

Accountability, transparency and governance



The primary tenets of good governance

Accountability and the value of appraisal

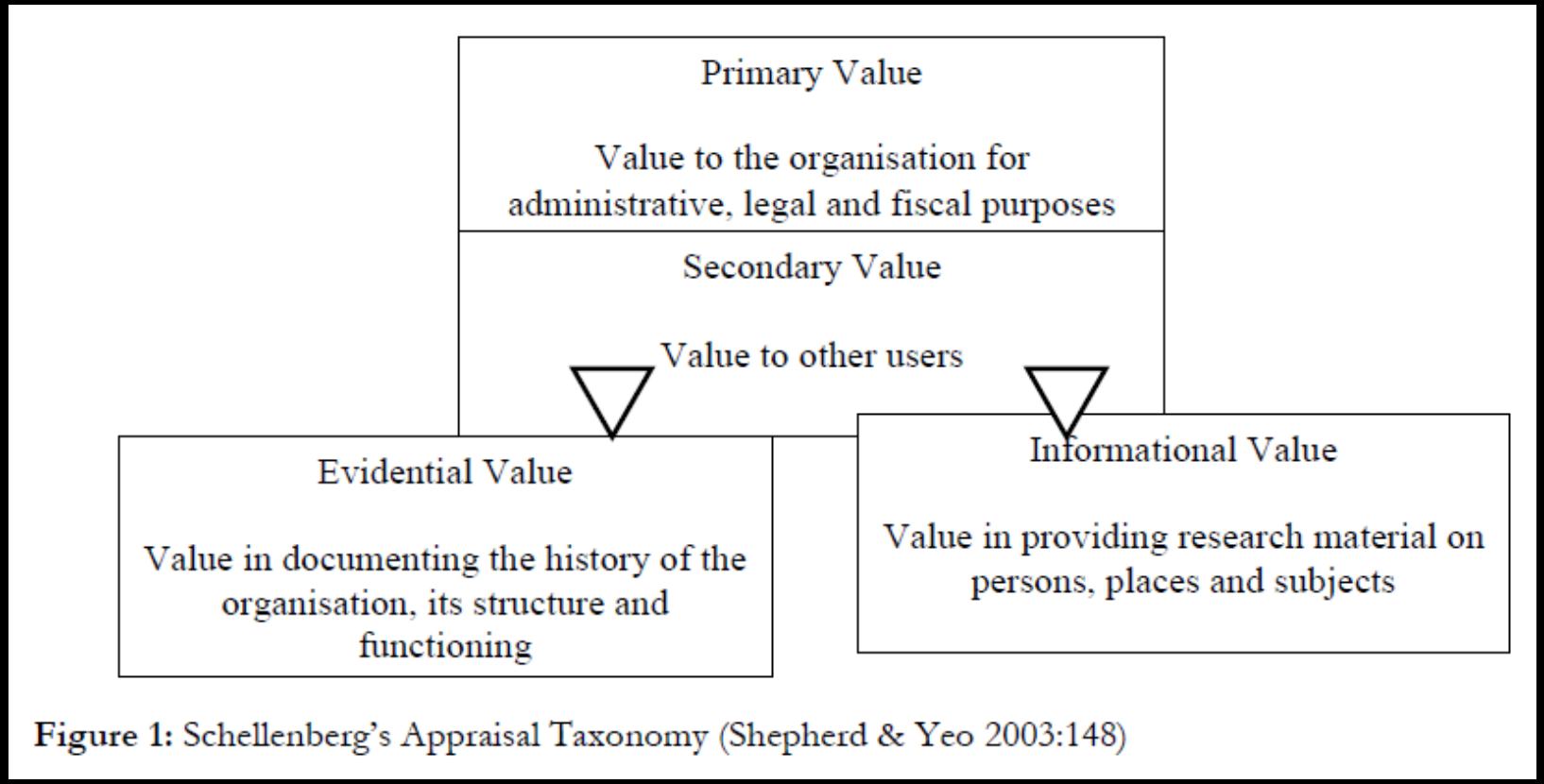


Figure 1: Schellenberg's Appraisal Taxonomy (Shepherd & Yeo 2003:148)

The value of good RM and archives: internal and external

Accountability and RIG: conclusions

Even if the RIG approach tends to be mostly internal, it ads some principles to the «civic» value of accountability:

- The cruciality of good RM and transparency to connect responsibility, actions and records.
- the centrality of a good organization, i.e. an effective and clear (transparent) delegation system *(delegate responsibility for records and information management to appropriate individuals)*;
- The cruciality to have governing position/responsibility for Records and Information Manager in any organization;
- The estabilishment of an accountability assessment process to ensure that organization's goals are routinely reviewed and revised.

Transparency

- An organization’s business processes and activities, including its information governance program, shall be documented in an open and verifiable manner, and the documentation shall be available to all personnel and appropriate interested parties. (GARP)
- In a free society, transparency is government's obligation to share information with citizens.

Transparency, as used in science, engineering, business, and in other social contexts, operates in such a way that it is easy for others to see what actions are performed. Transparency implies openness, communication, and accountability.

The meaning of **transparent** is totally different in a computer science context, coming closer to **invisible or undetectable**

Transparency and good governance

- Transparency requires significant resources, so it may slow down administrative procedures.
- It also has necessary limits: legitimate issues of security and the privacy rights of citizens form two such boundaries.
- But without it, “good governance” has little meaning.
- Accountability requires energy too: people, interest groups, civil society, the courts, the press, and opposition parties must insist that those who govern follow legitimate mandates and explain their actions.