GOVERNANCE

GETTING STARTED WITH DATA GOVERNANCE USING COBIT® 5

Design and Delivery of Data Governance

COBIT® 5
AN ISACA® FRAMEWORK

ISACA®

CONTENTS

ABSTRACT

Getting Started with Data Governance Using COBIT® 5 extends the application of the COBIT 5 framework to the practice of data governance. The practice of data governance is described and then elements of *COBIT 5: Enabling Information* are explored. Specific examples are provided against each of the COBIT 5 enablers.

Introduction[1]

Data maintenance and management are becoming ever more complicated. Data environments (e.g., the cloud) change rapidly and so do internal enterprise data requirements. COBIT® 5 provides definitions, good practices and modeling to assist practitioners in dealing with the critical role of data within the enterprise. Strong management provides the underpinning of good data governance.

COBIT 5 enablers are germane to the governance of data. This white paper extends the coverage of COBIT 5 enablers to data governance by leveraging guidance found in *COBIT® 5: Enabling Information*.

Note: *COBIT® 5: Enabling Information* provides IT and business stakeholders with:

- A comprehensive information model that is based on the generic COBIT 5 enabler model and that addresses all aspects of data and information
- Guidance for using the COBIT 5 framework, principles and concepts (especially the enablers) to address common data and information governance and management issues
- The reasons why it is critical for data and information to be managed and governed in an appropriate way

Data exists throughout enterprises; almost all stakeholders, processes and business activities rely on data at some level and to some degree. If data cannot be kept accurate, up to date, reliable and secure, risk may increase across business, operational, and compliance domains, to name only a few potential impacts.

This paper explores the design and delivery of governance for data operations and describes the enablers that not only inform data governance and management but also help to address common issues.

Data Governance

Data governance ensures that:

- Stakeholder needs, conditions and options are evaluated to determine balanced, mutually agreed enterprise objectives to be achieved through the acquisition and management of data/information resources.
- Direction is set for data/information management capabilities through prioritization and decision making.
- Performance and compliance of data/information resources are monitored and evaluated relative to mutually agreed-upon (by all stakeholders) direction and objectives.

Data governance reflects the practice of evaluating requirements and bringing direction and control over data and information so that users have access to that data and can trust and rely on it. Data governance also involves monitoring the performance of IT operations, specifically those areas that relate to data and its availability, integrity and confidentiality. The complexity of functions increases as enterprises grow and become more sophisticated in their operations and geographical dispersion, and as information security and other requirements evolve.

1 COBIT 5 content in this white paper is based on information from the following publications: ISACA, *COBIT® 5: A Business Framework for the Governance and Management of Enterprise IT*, USA, 2012 and ISACA, *COBIT® 5: Enabling Information*, USA, 2013.

Data exists in many forms—text, numbers, graphics, sound, video and others in both structured and unstructured format. Information is data made meaningful. After context is defined, data can be reported or interrogated further to provide insight, logical inferences, probabilities or patterns that are inherent in the data, whether it exists inside or outside the enterprise. Within a specified context, data becomes information that drives decision making across governance, management and operational domains. The successful use of data drives the accomplishment of enterprise goals.

Figure 1 shows that data and information fall within in a hierarchy of meaning or significance.

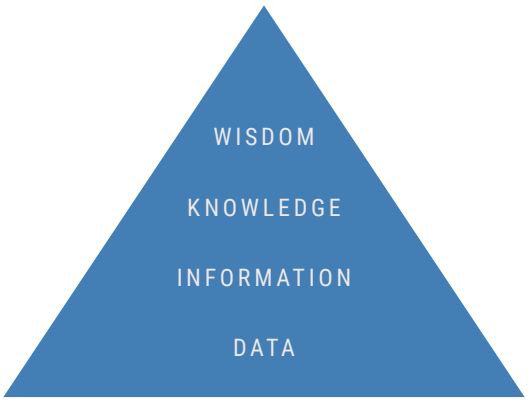

FIGURE 1: Data, Information, Knowledge and Wisdom (DIKW) Hierarchy

Source: Rowley, Jennifer; "The wisdom hierarchy: representations of the DIKW hierarchy," Fig. 6, *Journal of Information Science* 33(2), doi:10.1177/0165551506070706, *http://journals.sagepub.com/doi/abs/10.1177/0165551506070706*

This hierarchy presents the evolution of data through four levels—data, information, knowledge and wisdom. As data is accessed and processed, meaning is applied. For example, sales data can be grouped to compare regional sales. As information is derived from data, it can be used, in turn, to generate organizational knowledge, a set of relevant facts. Knowledge leads to a deeper understanding of an issue and more keen insight. This keener insight is termed wisdom.

Although the DIKW hierarchy is useful to understand the evolution of data, there is a weakness in the model. It locates information and knowledge in a sequence; however, in practice, knowledge is often applied to information in such a way as to create new knowledge or alter existing knowledge. The relationship between information and knowledge is thus dynamic and iterative, not strictly sequential. Nonetheless, the nature of the evolution of data impacts decision making.

Enterprise leaders evaluate the external environment, make decisions about information needs and determine how existing data must be secured and used, thus generating requirements. These requirements are driven by the enterprise stakeholders. Evaluation by enterprise leaders determines the enterprise's strategic objectives and results in the development of specific directives, which are shared with enterprise management. These directives inform management of their responsibilities, prioritize them and provide data governance performance measures, i.e., metrics.

Measurement

Performance measurement is the last key activity of data governance. Performance measurement permits reporting on compliance and supports progress toward the accomplishment of objectives.

Data management comprises the underlying practices that put into action the directives of data governance and provide the concrete results required of the enterprise. Management receives directives and plans how to use enterprise resources to create the required outputs. After plans are established, management builds out the solutions, systems and other structures that are necessary to accomplish the objectives. With solutions built, the business runs in business-as-usual mode to generate the required outputs. Management reports its operational results back up to data governance, and then performance measurement determines target accomplishment and compliance. Management acquires, controls, protects, delivers and enhances the

value of data and information assets, in alignment with the direction that is set by the data and information governance body. The overall data governance structure can be strengthened by aligning it with other internationally accepted standards and frameworks, including those in **figure 2**.

Data Governance in Practice

Implementing a data governance structure requires the identification and deployment of various enablers in the enterprise. As stakeholder requirements are established and understood, specific information quality goals must be defined. **Figure 3** shows the 15 quality goals for information. These goals assist the practitioner in maintaining appropriate depth and breadth of information during the determination of stakeholder requirements.

COBIT 5 uses the goals cascade to establish data governance requirements.[6] As specific data requirements are uncovered, the COBIT 5 Information Model[7] describes the steps (outlined in **figure 4**) to ensure that all relevant practitioners are involved and that they cover the aspects most applicable to their role.

Figure 4 can be used to determine the levels of responsibility of the roles and enterprise organizations

Data Management Association International (DAMA) – Data Management Body of Knowledge (DMBOK)[2]	Data management framework and guide for practitioners, including data analysts through technical operations
TOGAF®[3]	Open Group standard and architecture framework with extensive coverage of data architecture
Object Management Group®[4]	Prescriptive standards for data management syntax, i.e., metamodels
ISO 15489-1:2016 Information and Documentation—Records Management[5]	International standard with guidance for setting policies and standards; developing responsible, accountable, consulted or informed (RACI) charts, which describe and assign responsibility levels for process practices; and establishing procedures and guidelines **Note:** *COBIT® 5: Enabling Information*, Appendix A provides comparisons of COBIT 5 to DMBOK and ISO 15489.

FIGURE 2: Other Standards and Frameworks That Align with COBIT 5 Data Governance

2 Data Management Association International (DAMA), *The DAMA Guide to the Data Management Body of Knowledge (DMBOK)*, USA, 2009

3 The Open Group, "Enterprise Architecture," *www.opengroup.org/subjectareas/enterprise*

4 Object Management Group, OMG®, 2017, *www.omg.org/*

5 International Organization for Standardization, "ISO 15489-1:2016 Information and documentation -- Records management -- Part 1: Concepts and principles," *https://www.iso.org/obp/ui/#iso:std:iso:15489:-1:ed-2:v1:en*

6 For more information about the COBIT 5 goals cascade, see ISACA, *COBIT® 5: A Business Framework for the Governance and Management of Enterprise IT*, USA, 2012.

7 For more information about the COBIT 5 Information model, see ISACA, *COBIT® 5: Enabling Information*, "Chapter 3 The COBIT 5 Information Model," USA, 2013.

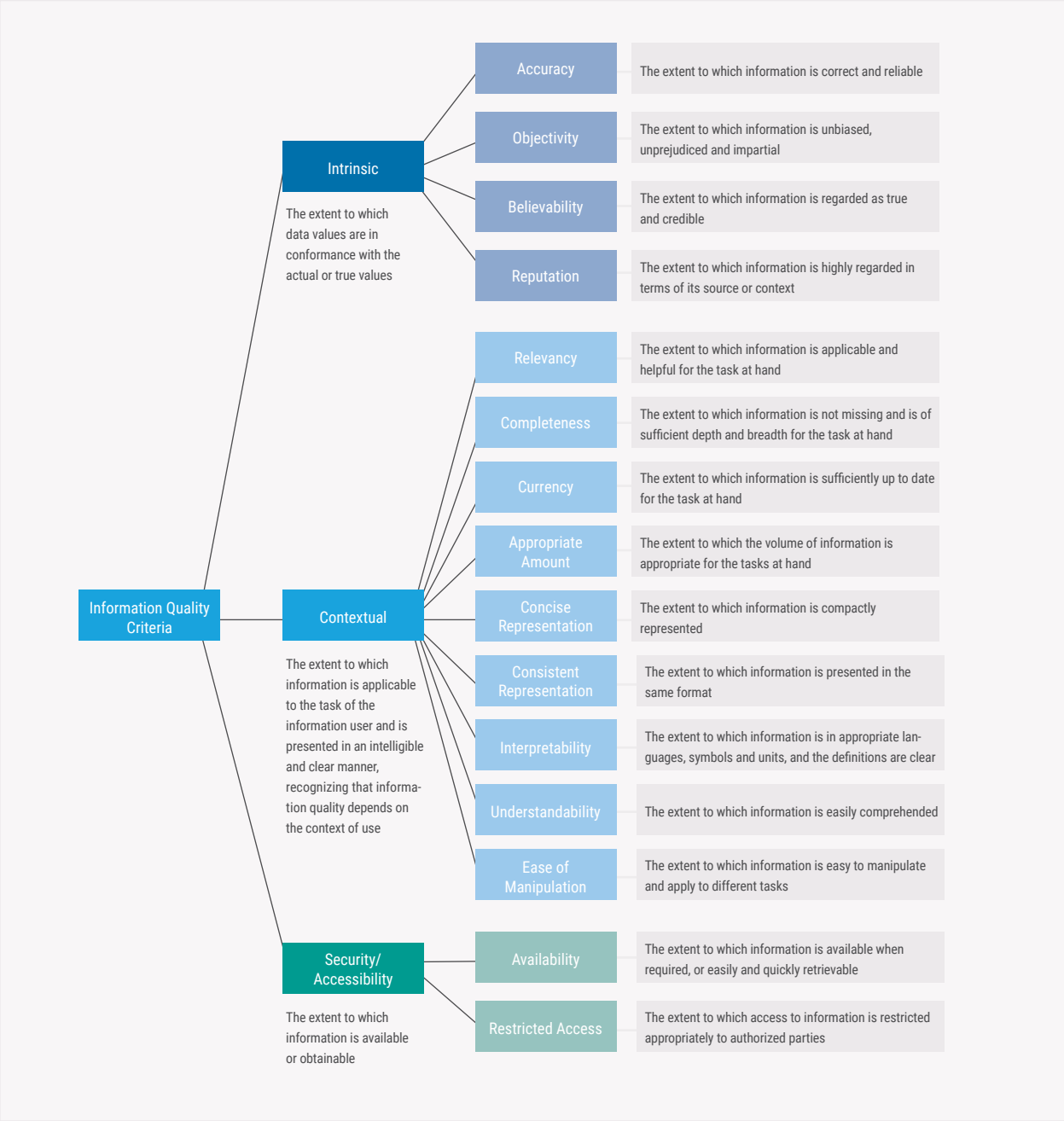

FIGURE 3: Information Goals/Quality Criteria

Source: ISACA, *COBIT® 5: Enabling Information*, USA, 2013, figure 20, page 31

Practical Use of the Information Model for Stakeholders	Board of Directors and Executive Management (CEO, COO, CFO)	CIO and IT Senior Management	Business Process Owners	Enterprise Architects, Data Stewards	IT Architect, IT Solutions Development	IT Operations	IT Security, Continuity and Privacy Professionals	Internal Audit and Compliance, Risk Management
Define and assign accountability and responsibility during different life cycle stages of information, e.g., during planning, design, build, use, monitoring, storage and disposal of sensitive information.	✓	✓	✓					
Define quality criteria for information across a range of different quality goals, e.g., relevancy, completeness and restricted access.	✓	✓	✓	✓				
Define all attributes of information items required for efficient and effective design, development and use of information by business functions.		✓	✓	✓	✓			
Understand which information items (and their criticality) are managed through the applications that are being operated and supported.				✓	✓	✓		✓
Understand which information items are managed through the applications that are being operated and supported and ensure they are managed according to their materiality/criticality.			✓	✓	✓	✓	✓	✓
Relate security and availability requirements to the wider concept of quality criteria for information across a range of 15 quality goals.				✓	✓	✓	✓	✓
Define all attributes of information items required for efficient and effective protection of information.							✓	✓

FIGURE 4: Practical Use of the Information Model

Source: ISACA, *COBIT® 5: Enabling Information*, USA, 2013, figure 14, page 27

for the information goals. For data governance, it can be useful to group stakeholders into one of the following categories, according to how they interact with data and information, and how they process data into relevant information:

- Information creators
- Information custodians
- Information consumers

Practitioners can also identify whether a stakeholder is internal or external to the enterprise. This stakeholder differentiation helps to define the information enabler life cycle and facilitates the most appropriate assignment of practices. After the enterprise identifies and assigns good practices, practitioners can apply relevant metrics to the operation of the information enabler. Metrics permit ongoing monitoring at the management level and support reporting dashboards, data-driven decision making, compliance reporting and monitoring back up to the data governing body. *COBIT® 5: Enabling Information* provides specific examples of the relationship between an information item and information stakeholders during the information item's life cycle, as it flows through an enterprise.[8]

Data constructs should include security-specific considerations. The security elements are confidentiality, integrity and availability (CIA). Each CIA element has quality-criteria concerns:

- Confidentiality relates to restricted access.
- Integrity combines completeness and accuracy.
- Availability relates to timeliness and reliable access.

It is important to plan the life cycle of data along with their placement within the governance structure. As practices operate, the data supporting or underlying them reach the various levels of their natural life cycles. Data is planned, designed, acquired, used, monitored and disposed of (see **figure 5**).

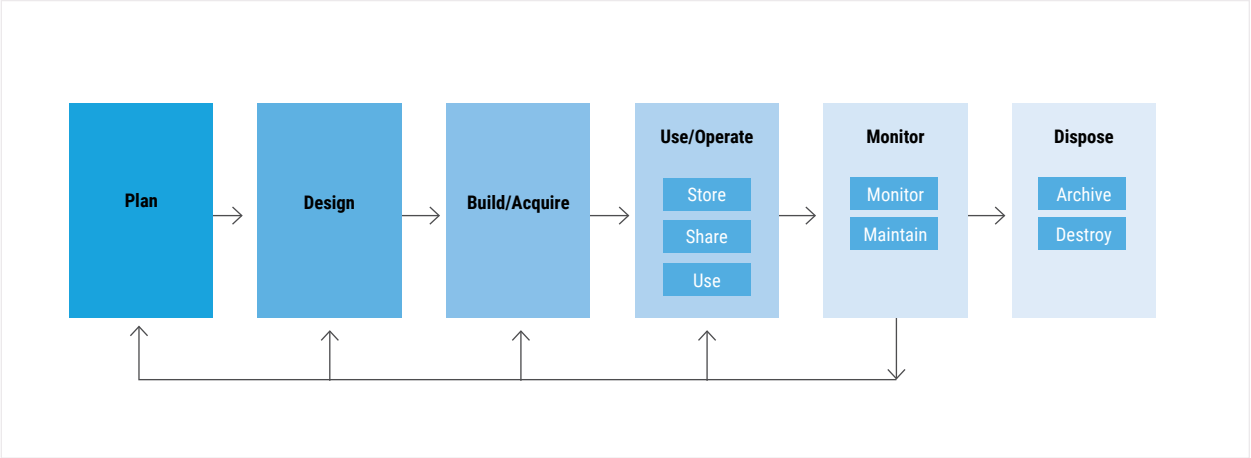

FIGURE 5: Information Life Cycle

Source: ISACA, *COBIT® 5: Enabling Information*, USA, 2013, figure 23, page 33

8 ISACA, *COBIT® 5: Enabling Information*, "3.1.1.1 Stakeholder Information Items and their Relationships to Information Stakeholders," USA, 2013

COBIT® 5: Enabling Information provides several real-world examples of good practices in data governance enablers.[9] **Figure 6** in the appendix to this white paper shows comprehensive detail regarding the application of the following COBIT 5 enablers to a specific information item risk profile:

- Principles, Policies and Frameworks
- Processes
- Organizational Structures
- Culture, Ethics and Behavior
- Information
- Services, Infrastructure and Applications
- People, Skills and Competencies

Note: Chapter 4 in *COBIT® 5: Enabling Information* describes the management aspects of data and information maintenance, which is beyond the scope of this paper, but is valuable for the practitioner to review.[10]

Principles, Policies and Frameworks Enabler

Policies can assist in providing a direct connection between enterprise objectives and underlying data. Policies communicate management's intentions and, thereby, create direction and purpose for data. Policies can also underscore the strategic importance of data or specific data classifications. The practitioner must ensure that data quality and use requirements are covered adequately by all relevant policies.

Processes Enabler

Processes provide the mechanisms by which business activity is undertaken. Processes contain management practices, which include inputs, outputs and activities. Data governance includes the management of data. To apply process assignment and control for data governance, an enterprise might use the COBIT 5 management practice DSS06.03 *Manage roles, responsibilities, access privileges and levels of authority.* The following example shows the application of management practice DSS06.03.

Example:
Management practice DSS06.03 *Manage roles, responsibilities, access privileges and levels of authority* uses the following inputs:

- Assigned responsibilities for resource management (from management practice EDM04.02 *Direct resource management*)
- Quality management system (QMS) roles, responsibilities and decision rights (from management practice APO11.01 *Establish a quality management system [QMS]*)
- Information security management system (ISMS) scope statement (from management practice APO13.01 *Establish and maintain an information security management system [ISMS]*)
- Access logs (from management practice DSS05.05 *Manage physical access to IT assets*)

9 ISACA, *COBIT® 5: Enabling Information*, "3.2 Additional Examples of COBIT 5 Information Model Use," USA, 2013

10 ISACA, *COBIT® 5: Enabling Information*, "Chapter 4 Addressing Information Governance and Management Issues Using COBIT 5," USA, 2013

Example (continued)

Implementing management practice DSS06.03 produces the following outputs:

- Allocated roles and responsibilities (to management practice APO01.02 *Establish roles and responsibilities*)
- Allocated levels of authority (to management practice APO01.02 *Establish roles and responsibilities*)
- Allocated access rights (to management practice APO07.04 *Evaluate employee job performance*)

Management practice DSS06.03 contributes to the overall process of managing business process controls. Its performance is measured when overall process metrics are run. Example metrics used to measure process performance include:

- Number of incidents and audit report findings indicating failure of key controls
- Percent of business process roles with clear separation of duties
- Number of incidents for which transaction history cannot be recovered

Practitioners should establish appropriate metrics for process controls that affect data, its quality and appropriateness of use. Along with metrics, related key performance indicators (KPIs) and key risk indicators (KRIs) should also be developed for each data-related practice.

Organizational Structures Enabler

Per the process DSS06 *Manage Business Process Controls* RACI chart, business executives are accountable for the determination of appropriate data access roles, responsibilities and levels of authority. These executives assign specific responsibilities for these determinations to business process owners and information security managers.

Culture, Ethics and Behavior Enabler

The assignment of appropriate roles and responsibilities for data management contribute to and underscore the need for a risk-aware culture within the enterprise.

Information Enabler

Information is the COBIT 5 process reference model governance enabler that is the subject of, and described in, this white paper.

Services, Infrastructure and Applications Enabler

Data reside in and are processed by numerous applications within the enterprise architecture. The internal control environment must provide appropriate and adequate controls over access to programs and data.

People, Skills and Competencies Enabler

Dependency on data is extremely high in most enterprises. The skills of all personnel who interact with data must be defined, where appropriate, and validated through internal audit tests of controls.

Conclusion

Tying resources directly to enterprise objectives through an enabler model creates efficiency in resource use and provides greater assurance that value can be most effectively and efficiently created and delivered to stakeholders. Using a structured methodology permits practitioners to demonstrate the scope and strength of their data governance to stakeholders. COBIT 5 provides the mechanisms, through its enablers, to design a data governance solution. The COBIT 5 product family provides several resources that practitioners can use for this purpose:

- *COBIT® 5* (the framework)
- *COBIT® 5 Implementation*
- *COBIT® 5: Enabling Processes*
- *COBIT® 5: Enabling Information*

APPENDIX

A risk profile is a description of the overall (identified) risk to which the enterprise is exposed.
A risk profile consists of:

- Risk register
  - Risk scenarios
  - Risk analysis
- Risk action plan
- Loss events (historical and current)
- Risk factors
- Independent assessment findings

LIFE CYCLE AND STAKEHOLDERS	LIFE CYCLE STAGE	INTERNAL STAKEHOLDER	EXTERNAL STAKEHOLDER	DESCRIPTION/STAKE
	Information planning	ERM committee, board	External audit, regulator	• Internal stakeholders: Initiate and drive the implementation and appoint a CRO. Have adequate information on the exposure. • External stakeholders: To have comfort on the risk management capabilities.
	Information design	Risk function, compliance, CIO, CISO, business process owners, internal audit		• CRO: To obtain information from the other roles in order to provide the overview for the governance bodies. • CIO: To be able to develop an adequate information system. • Other roles: To be able to provide relevant information and to ensure completeness/adequacy.
	Information build/acquire	Risk function, internal audit		• CRO: Provides functional requirements and consults others. • Internal audit: Provides quality assurance services on the implementation.
	Information use/operate: store, share, use	Board, ERM committee, business executive, CIO, risk function, CISO, business process owners, compliance, internal audit	External audit, regulator	• Business process owners, business executives and CIO: To efficiently provide relevant information. • Board and ERM committee: To receive relevant information and to enable decision making. • Internal audit, external audit and regulator: Receive relevant information. • CRO: Oversees the caption, processing and interpretation of information.
	Information monitor	Board, ERM committee, risk function, internal audit	External audit	• CRO: Ongoing monitoring on adequacy, completeness and accuracy of information; semi-annual assessment of performance (MEA01) and controls (MEA02) to maintain the information. • Internal audit: Annual validation of format and level of contents.
	Information dispose	Risk function		• CRO: According to data retention policy, to ensure confidentiality of information and to reduce the amount of information.

FIGURE 6: Information Item Risk Profile

GOALS		QUALITY SUBDIMENSION AND GOALS	DESCRIPTION—The extent to which information is...	RELEVANCE*	GOAL
GOALS	INTRINSIC	**Accuracy**	correct and reliable	High	Source information needs to be accurate (confirm through audit) and needs to be aggregated in the risk management application according to fixed rules.
GOALS	INTRINSIC	**Objectivity**	unbiased, unprejudiced and impartial	High	Information is based on verifiable facts and substantiations, using the common risk view established throughout the enterprise.
GOALS	INTRINSIC	**Believability**	regarded as true and credible	Medium	Reporting is fully trusted.
GOALS	INTRINSIC	**Reputation**	regarded as coming from a true and credible source	Medium	Source information is collected from competent and recognised sources.
GOALS	CONTEXTUAL AND REPRESENTATION	**Relevancy**	applicable and helpful for the task at hand	High	The risk profile is structured as defined and the recipient confirms the relevancy of information provided.
GOALS	CONTEXTUAL AND REPRESENTATION	**Completeness**	not missing and is of sufficient depth and breadth for the task at hand	High	The risk profile covers the full enterprise scope and the full risk register. However, not all information might be available and assumptions need to be made and substantiated.
GOALS	CONTEXTUAL AND REPRESENTATION	**Currency**	sufficiently up to date for the task at hand	Low	The need for currency of the risk profile is driven by the frequency and impact of alterations and depending on the component.
GOALS	CONTEXTUAL AND REPRESENTATION	**Amount of information**	is appropriate in volume for the task at hand	High	The volume of information is appropriate to the recipient's needs and shall be defined during the design.
GOALS	CONTEXTUAL AND REPRESENTATION	**Concise representation**	compactly represented	Medium	The risk profile is concisely represented; this is obtained by aggregating data for the entire enterprise and by retaining only individual cases from a predefined threshold onwards.

FIGURE 6: Information Item Risk Profile (continued)

*The relevance column entries are enterprise contextual. This is an illustration, but the actual importance depends on each enterprise's specific context.

GOALS	QUALITY SUBDIMENSION AND GOALS		DESCRIPTION—The extent to which information is...	RELEVANCE*	GOAL
	CONTEXTUAL AND REPRESENTATION	**Consistent representation**	presented in the same format	Low	The risk profile is always presented according to an agreed-on template. However, single scenarios might be analyzed differently when agreed on.
		Interpretability	in appropriate languages, symbols and units, and the definitions are clear	High	To ease decision making, the information 'sweet spot' can be identified and focused on.
		Understandability	easily comprehended	High	In order to make informed decisions, the risk profile should be understood by many stakeholders.
		Manipulation	easy to manipulate and apply to different tasks	Low	Scenarios can be modified and simulated.
	SECURITY	**Availability**	available when required, or easily and quickly retrievable	Medium	The risk profile is at all times available to its stakeholders; a temporary unavailability is acceptable in case of an incident.
		Restricted access	restricted appropriately to authorized parties	High	Access to the risk profile is determined by the risk function, and is restricted as follows: • Write access: Risk function (based on input from contributors) • Read access: All other stakeholders

FIGURE 6: Information Item Risk Profile (continued)

*The relevance column entries are enterprise contextual. This is an illustration, but the actual importance depends on each enterprise's specific context.

GOOD PRACTICE	ATTRIBUTE	DESCRIPTION	VALUE
	Physical	Information carrier/ media	The information carrier for the risk profile can be an electronic or printed document or an information system (e.g., dashboard).
	Empiric	Information access channel	The risk profile is accessible through the ERM portal or printed at specific locations.
	Syntactic	Code/language	The risk profile contains the following subparts: • Risk register (results of risk analysis), which consists of a list of risk scenarios and their associated estimates for impact and frequency (risk map); both current and the previous risk map will be included. • Risk action plan, including action item, status, responsible, deadline, etc. • Loss data related to events occurring over the last reporting period(s). • Risk factors, including both contextual risk factors and capability-related risk factors (vulnerabilities). Result of independent assessments (e.g., audit findings, self-assessments).
	Semantic	Information type	Structured document based on a template and/or an online dashboard with drill-down functionality.
		Information currency	The risk profile contains historical, current and forward looking data.
		Information level	The risk profile aggregates data over the entire enterprise, representing only major risk over a defined threshold and with significant changes to previous periods.

FIGURE 6: Information Item Risk Profile (continued)

GOOD PRACTICE	ATTRIBUTE	DESCRIPTION	VALUE
	Pragmatic	Retention period	The risk profile is to be retained for as long as the data/information over which it reports risk needs to be retained. Updates to the risk register should be logged and retained as defined in legal requirements, e.g., the information is used as evidence or is needed to obtain independent assurance.
		Information Status	The current instance is operational, older ones are historical data.
		Novelty	The risk profile combines several other sources of data that make up a new instance, hence it is novel data. It is updated regularly (e.g., on a monthly basis).
		Contingency	The risk profile relies on the following information being available and understood by the user: • Risk appetite of the enterprise • Risk factors that apply to the enterprise • Risk taxonomy in use in the enterprise
	Social	Context	The risk profile is primarily meaningful and to be used in a context of ERM, but could also be used in other circumstances (e.g., during a merger).

FIGURE 6: Information Item Risk Profile (continued)

LINK TO OTHER ENABLERS	
Processes	The risk profile is an output from the management practices: • APO12.03 Maintain a risk profile. • APO12.04 Articulate risk. The risk register is an input for the governance and management practices: • EDM03.02 Direct risk management. • EDM05.02 Direct stakeholder communication and reporting. • APO02.02 Assess the current environment, capabilities and performance. • MEA02.08 Execute assurance initiatives. It is used in the following government management practices: • EDM03.03 Monitor risk management • APO12.06 Respond to risk It is mentioned in the goal of the process APO12 *Manage Risk*: • A current and complete risk profile exists. And measured by the following metrics: • Percent of key business processes included in the risk profile • Completeness of attributes and values in the risk profile
Organizational Structures	Under the accountability of the CRO, the following roles are responsible for providing/producing the information: • Business process owners • CIO (and IT staff members) • CISO
Infrastructure, Applications and Services	The risk profile is produced by a risk management application or manually maintained by the CRO.
People, Skills and Competencies	The generation of the risk profile requires an understanding of risk management principles and skills. The provision of information requires subject-related expertise and the presentation of information should not require risk management skills but enable governance bodies to steer risk management and to take decisions.
Culture, Ethics and Behavior	The availability of the risk profile supports the transparency of risk as well as trends and a risk-aware culture.
Principles, Policies and Frameworks	Related principles: • Connect to enterprise objectives • Align with ERM • Balance cost/benefit IT risk • Consistent approach

FIGURE 6: Information Item Risk Profile (continued)

Source: ISACA, *COBIT® 5: Enabling Information*, USA, 2013, figure 35, pages 41-44

Acknowledgments

ISACA would like to recognize:

Lead Developer

Peter C. Tessin
CISA, CRISC, CISM, CGEIT, Sr. Manager, BT Risk and Compliance, Discover Financial Services, USA

Expert Reviewers

Sushil Chatterji
CGEIT, COBIT Certified Assessor, Edutech Enterprises, Singapore

Jimmy Heschl
CISA, CISM, CGEIT, Red Bull, Austria

Mark Thomas
CRISC, CGEIT, Escoute, USA

ISACA Board of Directors

Theresa Grafenstine
CISA, CRISC, CGEIT, CGAP, CGMA, CIA, CISSP, CPA, Deloitte-Arlington, VA, USA, Chair

Robert Clyde
CISM, Clyde Consulting LLC, USA, Vice-Chair

Brennan Baybeck
CISA, CRISC, CISM, CISSP, Oracle Corporation, USA, Director

Zubin Chagpar
CISA, CISM, PMP, Amazon Web Services, UK, Director

Peter Christiaans
CISA, CRISC, CISM, PMP, Deloitte Consulting LLP, USA, Director

Hironori Goto
CISA, CRISC, CISM, CGEIT, ABCP, Five-I, LLC, Japan, Director

Mike Hughes
CISA, CRISC, CGEIT, Haines Watts, UK, Director

Leonard Ong
CISA, CRISC, CISM, CGEIT, CPP, CFE, PMP, CIPM, CIPT, CISSP ISSMP-ISSAP, CSSLP, CITBCM, GCIA, GCIH, GSNA, GCFA, Merck & Co., Inc., Singapore, Director

R.V. Raghu
CISA, CRISC, Versatilist Consulting India Pvt. Ltd., India, Director

Jo Stewart-Rattray
CISA, CRISC, CISM, CGEIT, FACS CP, BRM Holdich, Australia, Director

Ted Wolff
CISA, Vanguard, Inc., USA, Director

Tichaona Zororo
CISA, CRISC, CISM, CGEIT, COBIT 5 Certified Assessor, CIA, CRMA, EGIT | Enterprise Governance of IT (Pty) Ltd, South Africa, Director

Christos K. Dimitriadis, Ph.D.
CISA, CRISC, CISM, Intralot, S.A., Greece, Past Chair

Robert E Stroud
CRISC, CGEIT, Forrester Research, Inc., USA, Past Chair

Tony Hayes
CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Past Chair

Matt Loeb
CGEIT, FASAE, CAE, ISACA, USA, Director

About ISACA

Nearing its 50th year, ISACA® (isaca.org) is a global association helping individuals and enterprises achieve the positive potential of technology. Technology powers today's world and ISACA equips professionals with the knowledge, credentials, education and community to advance their careers and transform their organizations. ISACA leverages the expertise of its half-million engaged professionals in information and cyber security, governance, assurance, risk and innovation, as well as its enterprise performance subsidiary, CMMI® Institute, to help advance innovation through technology. ISACA has a presence in more than 188 countries, including more than 215 chapters and offices in both the United States and China.

DISCLAIMER

ISACA has designed and created *Getting Started with Data Governance Using COBIT® 5: Design and Delivery of Data Governance* (the "Work") primarily as an educational resource for professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

RESERVATION OF RIGHTS

ISACA®

3701 Algonquin Road, Suite 1010
Rolling Meadows, Il 60008 USA

Phone: +1.847.660.5505

Fax: +1.847.253.1755

Support: support.isaca.org

Web: www.isaca.org

Provide Feedback:
www.isaca.org/Data-Governance-COBIT-5

Participate in the ISACA Knowledge Center:
www.isaca.org/knowledge-center

Twitter:
www.twitter.com/ISACANews

LinkedIn:
www.linkd.in/ISACAOfficial

Facebook:
www.facebook.com/ISACAHQ

Instagram:
www.instagram.com/isacanews/