GOVERNANCE DEL RISCHIO

Questo esercizio richiede il download delle seguenti risorse:

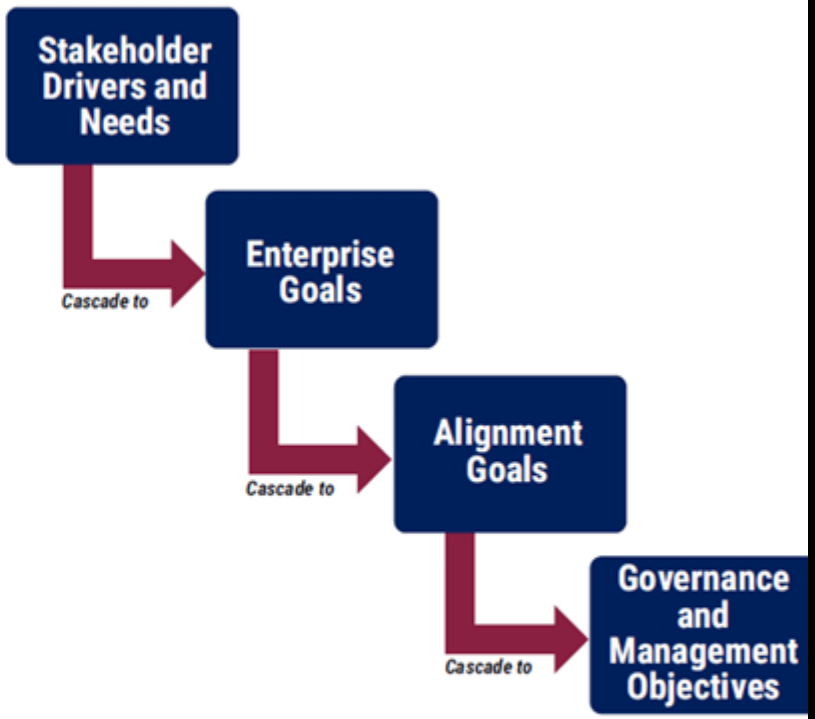
- **A*:** COBIT 2019 Framework: Introduction & Methodology | Digital | English
  https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ko9cEAC
- **B*:** COBIT 2019 Framework: Governance & Management Objectives | Digital | English
  https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ko9ZEAS
- COBIT 2019 Toolkit
  https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/cobit-2019-toolkit.zip
  - **C:** COBIT-2019_RACI-by-role_April 2020_v2.xlsx
  - **D**: COBIT 2019_Governance-Management-Objectives-Practices-Activities_Nov2018.xlsx

* è richiesta solo la registrazione al portale ISACA.

La gestione del rischio è integrata anche nella governance, perciò dobbiamo essere capaci di cogliere i rischi che si possono celara dietro agli obiettivi. Ad esempio, può capitare di dover correggere un obiettivo perchè il rischio collegato è molto elevato oppure individuare dei fattori di rischio nella traduzione degli obiettivi dal livello strategico fino al livello operativo.

L'Alta Direzione ha stabilito di aver bisogno che i dati sensibili degli utenti siano protetti, in conformità alle normative per migliorare anche la fiducia del cliente verso l'organizzazione (l'esigenza non si riferisce alla business continuity, non è richiesto Design Factors e Focus Area).

- collega a questo bisogno, un **Enterprise Goal** tra quelli in «A-Figure 4.17»
- collega all'EG scelto, un **Alignment Goal** tra quelli in «A-Figure 4.18», può essere di aiuto la «B-Figure A.1»
- collega all'AG scelto, un **Governance and Management Objectives**, tra quelli in «B-Chapter 4», può essere di aiuto la «B-Figure A.2»
- scegli una pratica che possa concorrere a soddisfare l'esigenza dell'Alta Direzione tra le pratiche presenti all'interno dell'elemento scelto precedentemente. B/D
  - Quali sono i ruoli e le responsabilità per questa pratica? B/C
  - Quali sono gli input/output per questa pratica? B
  - In quale documento aziendale dovrebbe essere descritta la policy o la procedura? B
  - Quali servizi/infrastrutture/applicazioni sono coinvolti? B



COLLEGA A QUESTO BISOGNO, UN ENTERPRISE GOAL TRA QUELLI IN «**A**-FIGURE 4.17» OTTIMIZZAZIONE DEI COSTI DEI PROCESSI AZIENDALI: RAPPORTO TRA COSTI E LIVELLI DI SERVIZIO RAGGIUNTI, SODDISFAZIONE DEI CONSIGLI DI AMMINISTRAZIONE E DELLA DIRIGENZA ESECUTIVA RISPETTO AI COSTI DI ELABORAZIONE AZIENDALE.

Figure 4.17—Goals Cascade: Enterprise Goals and Metrics *(cont.)*

Reference	BSC Dimension	Enterprise Goal	Example Metrics
EG08	Internal	Optimization of internal business process functionality	• Satisfaction levels of board and executive management with business process capabilities • Satisfaction levels of customers with service delivery capabilities • Satisfaction levels of suppliers with supply chain capabilities
EG09	Internal	Optimization of business process costs	• Ratio of cost vs. achieved service levels • Satisfaction levels of board and executive management with business processing costs
EG10	Internal	Staff skills, motivation and productivity	• Staff productivity compared to benchmarks • Level of stakeholder satisfaction with staff expertise and skills • Percent of staff whose skills are insufficient relative to competencies required for their roles • Percent of satisfied staff
EG11	Internal	Compliance with internal policies	• Number of incidents related to noncompliance with policy • Percent of stakeholders who understand policies • Percent of policies supported by effective standards and working practices
EG12	Growth	Managed digital transformation programs	• Number of programs on time and within budget • Percent of stakeholders satisfied with program delivery • Percent of business transformation programs stopped • Percent of business transformation programs with regular reported status updates
EG13	Growth	Product and business	• Level of awareness and understanding of business

COLLEGA ALL'EG SCELTO, UN ALIGNMENT GOAL TRA QUELLI IN «A-FIGURE 4.18», PUÒ ESSERE DI AIUTO LA «B-FIGURE A.1» IN QUESTO CASO **EG09** CON AG04 AG09 CONSEGNARE PROGRAMMI ENTRO I TEMPI PREVISTI, NEL RISPETTO DEL BUDGET E SODDISFACENDO I REQUISITI E GLI STANDARD DI QUALITÀ

Purpose	
Foster a partnership between IT and enterprise stakeholders to enable the effective and efficient use of I&T-related resources and provide transparency and accountability of the cost and business value of solutions and services. Enable the enterprise to make informed decisions regarding the use of I&T solutions and services.	
The management objective supports the achievement of a set of primary enterprise and alignment goals:	
Enterprise Goals	**Alignment Goals**
• EG01 Portfolio of competitive products and services • EG04 Quality of financial information • EG07 Quality of management information • EG08 Optimization of internal business process functionality • EG09 Optimization of business process costs • EG12 Managed digital transformation programs	• AG04 Quality of technology-related financial information • AG09 Delivering programs on time, on budget and meeting requirements and quality standards
Example Metrics for Enterprise Goals	**Example Metrics for Alignment Goals**

COLLEGA ALL'AG SCELTO, UN GOVERNANCE AND MANAGEMENT OBJECTIVES, TRA QUELLI IN «B-CHAPTER 4», PUÒ ESSERE DI AIUTO LA «B-FIGURE A.2»

- Grado di evidenza dei principi di governance dell'I&T concordati nei processi e nelle pratiche (percentuale di processi e pratiche riconducibili ai principi) Questo punto si riferisce alla misurazione di quanto i principi concordati di governance dell'I&T siano presenti nei processi e nelle pratiche aziendali. Si cerca di valutare quanto i principi siano effettivamente implementati e seguiti nelle operazioni quotidiane.
- b. Frequenza della segnalazione della governance dell'I&T al comitato esecutivo e al consiglio di amministrazione Qui si chiede con quale frequenza vengono presentati rapporti sulla governance dell'I&T all'esecutivo e al consiglio di amministrazione. Ciò assicura che i leader aziendali siano costantemente informati sullo stato e sulle decisioni relative alla gestione dell'informazione e della tecnologia.c. Numero di ruoli, responsabilità e autorità per la governance dell'I&T che sono definiti, assegnati e accettati dalla gestione aziendale e dell'I&T
- Questo punto riguarda la definizione e l'assegnazione dei ruoli, delle responsabilità e delle autorità relativi alla governance dell'I&T. Si tratta di garantire che le persone coinvolte siano chiaramente a conoscenza dei propri ruoli e responsabilità nella gestione dell'informazione e della tecnologia e che tali ruoli siano accettati e compresi sia dalla gestione aziendale che da quella dell'I&T.

National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.1 Preparation (Tasks 2, 3, 4, 5)
Governance Practice	**Example Metrics**
EDM01.02 Direct the governance system. Inform leaders on I&T governance principles and obtain their support, buy-in and commitment. Guide the structures, processes and practices for the governance of I&T in line with the agreed governance principles, decision-making models and authority levels. Define the information required for informed decision making.	a. Degree to which agreed-on I&T governance principles are evident in processes and practices (percentage of processes and practices traceable to principles) b. Frequency of I&T governance reporting to executive committee and board c. Number of roles, responsibilities and authorities for I&T governance that are defined, assigned and accepted by appropriate business and I&T management

Activities	Capability Level
1. Communicate governance of I&T principles and agree with executive management on the way to establish informed and committed leadership.	2
2. Establish or delegate the establishment of governance structures, processes and practices in line with agreed-on design principles.	
3. Establish an I&T governance board (or equivalent) at the board level. This board should ensure that governance of information and technology, as part of enterprise governance, is adequately addressed; advise on strategic direction; and determine prioritization of I&T-enabled investment programs in line with the enterprise's business strategy and priorities	

DIREZIONE TRA LE PRATICHE PRESENTI ALL'INTERNO DELL'ELEMENTO SCELTO PRECEDENTEMENTE. B/D "INDIRIZZARE IL PERSONALE AFFINCHÉ SEGUA LE LINEE GUIDA RILEVANTI PER IL COMPORTAMENTO ETICO E PROFESSIONALE E GARANTIRE CHE LE CONSEGUENZE DELLA NON CONFORMITÀ SIANO CONOSCIUTE ED APPLICATE."

The activities are sorted in the order in which they appear in *COBIT® 2019 Framework: Governance and Management Objectives*.

Activities: 1202

Area	Domain	Objective ID	Objective	Practice ID	Practice Name	Activity
Governance	Evaluate, Direct and Monitor	EDM01	Ensured Governance Framework Setting and Maintenance	EDM01.02	Direct the governance system.	5. Ensure that communication and reporting mechanisms provide those responsible for oversight and decision making with appropriate information.
Governance	Evaluate, Direct and Monitor	EDM01	Ensured Governance Framework Setting and Maintenance	EDM01.02	Direct the governance system.	6. Direct that staff follow relevant guidelines for ethical and professional behavior and ensure that consequences of noncompliance are known and enforced.
Governance	Evaluate, Direct and Monitor	EDM01	Ensured Governance Framework Setting and Maintenance	EDM01.02	Direct the governance system.	7. Direct the establishment of a reward system to promote desirable cultural change.
Governance	Evaluate, Direct and Monitor	EDM01	Ensured Governance Framework	EDM01.03	Monitor the governance system.	1. Assess the effectiveness and performance of those stakeholders given delegated responsibility and authority for governance of enterprise I&T.

53, Revision 5 (Draft), August 2017	

B. Component: Organizational Structures					
Key Governance Practice	Board	Executive Committee	Chief Executive Officer	Chief Information Officer	I&T Governance Board
EDM01.01 Evaluate the governance system.	A	R	R	R	R
EDM01.02 Direct the governance system.	A	R			R
EDM01.03 Monitor the governance system.	A	R	R	R	R
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**				

C. Component: Information Flows and Items (see also Section 3.6)				
Governance Practice	Inputs		Outputs	
EDM01.01 Evaluate the governance system.	From	Description	Description	To
	MEA03.02	Communications of changed compliance requirements	Enterprise governance guiding principles	All EDM; APO01.01; APO01.03 APO01.04
	Outside COBIT	• Constitution/bylaws/ statutes of organization • Governance/decision-making model • Laws/regulations • Business environment trends	Decision-making model	All EDM; APO01.01; APO01.04
			Authority levels	All EDM; APO01.05

E. Component: Principles, Policies and Procedures			
Relevant Policy	Policy Description	Related Guidance	Detailed Reference
Delegation of authority policy	Specifies the authority that the board strictly retains for itself. Enumerates general principles of delegation of authority and schedule of delegation (including clear boundaries). Defines organizational structures to which the board delegates authority.	(1) ISO/IEC 38500:2015(E); (2) ISO/IEC 38502:2017(E); (3) King IV Report on Corporate Governance for South Africa, 2016	(1) 5.2 Principle 1: Responsibility; (2) 5.3 Delegation; (3) Part 5.3: Governing structures and delegation Principle—8 and 10
Governance policy	Provides guiding principles of governance (e.g., I&T governance is critical to enterprise success; I&T and the business align strategically; business requirements and benefits determine priorities; enforcement must be equitable, timely and consistent; industry best practices, frameworks and standards must be assessed and implemented as appropriate). Includes governance imperatives, such as building trust and partnerships, to be successful. Emphasizes that I&T governance reflects a process of continual improvement and must be tailored, maintained and updated to ensure relevance.	National Institute of Standards and Technology Special Publication 800- 53, Revision 5 (Draft), August 2017	3.14 Planning (PL-1)