## Governance del rischio

## Traccia

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

La gestione del rischio è integrata anche nella governance, perciò dobbiamo essere capaci di cogliere i rischi che si possono celare 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

<sup>\*</sup> è richiesta solo la registrazione al portale ISACA.

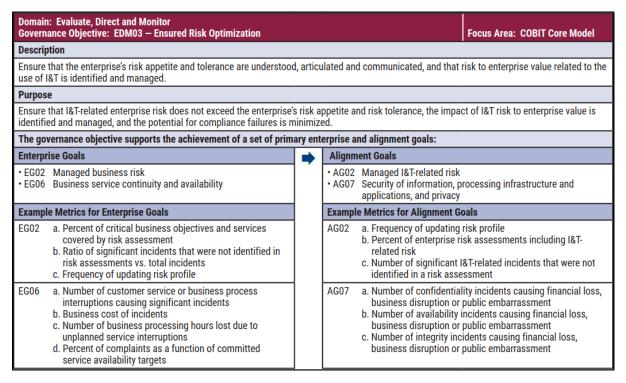
#### **Enterprise Goal**

Reference	BSC Dimension	Enterprise Goal	Example Metrics
EG08	Internal	Optimization of internal business process functionality	<ul> <li>Satisfaction levels of board and executive management with business process capabilities</li> <li>Satisfaction levels of customers with service delivery capabilities</li> <li>Satisfaction levels of suppliers with supply chain capabilities</li> </ul>
		6 H 1 H 21 C 1	

#### **Alignment Goal**

AG07	process	of information of the control of th	ructure a	nd	<ul> <li>Number of confidentiality incidents causing financial loss, business disruption or public embarrassment</li> <li>Number of availability incidents causing financial loss, business disruption or public embarrassment</li> <li>Number of integrity incidents causing financial loss, business disruption or public embarrassment</li> </ul>
4000	 - 11:			-	

#### **Governance and Management Objective**



# **Pratica Scelta**

Direct the governance system.

### Ruoli e Responsabilità

Activities	Capability Level		
Communicate governance of I&T principles and agree with executive management on the way to establish informed and committed leadership.			
<ol><li>Establish or delegate the establishment of governance structures, processes and practices in line with agreed-on design principles.</li></ol>			
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.			
Allocate responsibility, authority and accountability for I&T decisions in line with agreed-on governance design principles, decision-making models and delegation.			
5. Ensure that communication and reporting mechanisms provide those responsible for oversight and decision making with appropriate information.			
<ol><li>Direct that staff follow relevant guidelines for ethical and professional behavior and ensure that consequences of noncompliance are known and enforced.</li></ol>			
7. Direct the establishment of a reward system to promote desirable cultural change.			

# Input/Output

# **Example Metrics**

- a. Degree to which agreed-on I&T governance principles are evident in processes and practices (percentage of processes and practices traceable to principles)
- Frequency of I&T governance reporting to executive committee and board
- Number of roles, responsibilities and authorities for I&T governance that are defined, assigned and accepted by appropriate business and I&T management

### **Documenti per Policy e Procedure**

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	GE.DG Direct Governance System
ISF, The Standard of Good Practice for Information Security 2016	SG1.1 Security Governance Framework
ISO/IEC 38500:2015(E)	5.2 Principle 1: Responsibility (Direct)
ISO/IEC 38502:2017(E)	Governance of IT - Framework and model (all chapters)
King IV Report on Corporate Governance for South Africa, 2016	Part 5.4: Governance functional areas - Principle 12
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.14 Planning (PL-2, PL-10)

### Servizi/Applicazioni/Infrastrutture Coinvolte

Firewall, Sistemi di rilevamento delle intrusioni (IDS), Antivirus, Crittografia dei dati, VPN, Controlli di accesso, Servizi di gestione dell'identità e degli accessi (IAM), Backup e ripristino dei dati, Monitoraggio della sicurezza, Analisi dei rischi e delle vulnerabilità, Patch management, Audit e conformità, Formazione sulla sicurezza informatica, Protezione dei dispositivi endpoint, Protezione dei dati in transito e a riposo.