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

* 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 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

Enterprise Goal

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

Alignment Goal

AG07	Internal	Security of information, processing infrastructure and applications, and privacy	• Number of confidentiality incidents causing financial loss, business disruption or public embarrassment • Number of availability incidents causing financial loss, business disruption or public embarrassment • Number of integrity incidents causing financial loss, business disruption or public embarrassment

Governance and Management Objective

Domain: Evaluate, Direct and Monitor **Governance Objective: EDM03 — Ensured Risk Optimization**	**Focus Area: COBIT Core Model**
Description	
Ensure that the enterprise's risk appetite and tolerance are understood, articulated and communicated, and that risk to enterprise value related to the use of I&T is identified and managed.	
Purpose	
Ensure that I&T-related enterprise risk does not exceed the enterprise's risk appetite and risk tolerance, the impact of I&T risk to enterprise value is identified and managed, and the potential for compliance failures is minimized.	
The governance objective supports the achievement of a set of primary enterprise and alignment goals:	
Enterprise Goals	**Alignment Goals**
• EG02 Managed business risk • EG06 Business service continuity and availability	• AG02 Managed I&T-related risk • AG07 Security of information, processing infrastructure and applications, and privacy
Example Metrics for Enterprise Goals	**Example Metrics for Alignment Goals**
EG02 a. Percent of critical business objectives and services covered by risk assessment b. Ratio of significant incidents that were not identified in risk assessments vs. total incidents c. Frequency of updating risk profile	AG02 a. Frequency of updating risk profile b. Percent of enterprise risk assessments including I&T-related risk c. Number of significant I&T-related incidents that were not identified in a risk assessment
EG06 a. Number of customer service or business process interruptions causing significant incidents b. Business cost of incidents c. Number of business processing hours lost due to unplanned service interruptions d. Percent of complaints as a function of committed service availability targets	AG07 a. Number of confidentiality incidents causing financial loss, business disruption or public embarrassment b. Number of availability incidents causing financial loss, business disruption or public embarrassment c. Number of integrity incidents causing financial loss, business disruption or public embarrassment

Pratica Scelta

A. Component: Process	
Governance Practice	**Example Metrics**
EDM01.01 Evaluate the governance system. Continually identify and engage with the enterprise's stakeholders, document an understanding of the requirements, and evaluate the current and future design of governance of enterprise I&T.	a. Number of guiding principles defined for I&T governance and decision making b. Number of senior executives involved in setting governance direction for I&T

Activities	Capability Level
1. Analyze and identify the internal and external environmental factors (legal, regulatory and contractual obligations) and trends in the business environment that may influence governance design.	2
2. Determine the significance of I&T and its role with respect to the business.	
3. Consider external regulations, laws and contractual obligations and determine how they should be applied within the governance of enterprise I&T.	
4. Determine the implications of the overall enterprise control environment with regard to I&T.	
5. Align the ethical use and processing of information and its impact on society, the natural environment, and internal and external stakeholder interests with the enterprise's direction, goals and objectives.	3
6. Articulate principles that will guide the design of governance and decision making of I&T.	
7. Determine the optimal decision-making model for I&T.	
8. Determine the appropriate levels of authority delegation, including threshold rules, for I&T decisions.	

Ruoli e Responsabilità

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

Input/Output

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

Documenti per Policy e Procedure

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)

Servizi/Applicazioni/Infrastrutture Coinvolte

G. Component: Services, Infrastructure and Applications
• COBIT and related products/tools • Equivalent frameworks and standards