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

Direct the governance system.

Ruoli e Responsabilità

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.	
4. Allocate responsibility, authority and accountability for I&T decisions in line with agreed-on governance design principles, decision-making models and delegation.	3
5. Ensure that communication and reporting mechanisms provide those responsible for oversight and decision making with appropriate information.	
6. Direct that staff follow relevant guidelines for ethical and professional behavior and ensure that consequences of noncompliance are known and enforced.	
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) 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

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.