



**PHANTOM
SRL**

PREPARED FOR :
BCC ICCREA

GOVERNANCE DEL RISCHIO

PRESENTED BY:
GIUSEPPE PIGNATELLO
ALESSIO D'OTTAVIO
LUCA IANNONE

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

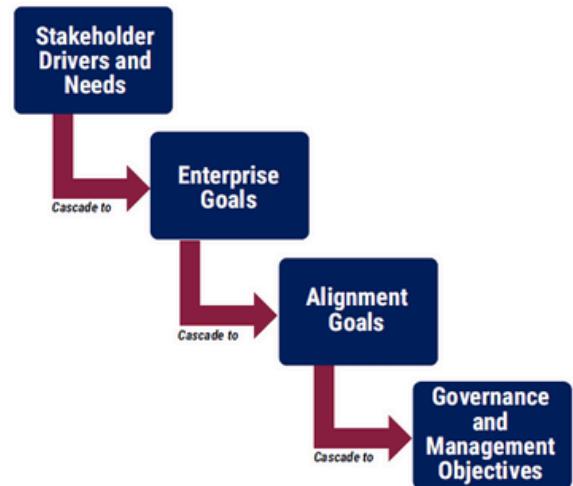
* è richiesta solo la registrazione al portale ISACA.

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 perché il rischio collegato è molto elevato oppure individuare dei fattori di rischio nella traduzione degli obiettivi dal livello strategico fino al livello operativo.

3

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**



4

FRAMEWORK COBIT

COS'È E COME FUNZIONA

Il framework **COBIT** (Control Objectives for Information and Related Technologies) rappresenta un pilastro essenziale per la governance e il controllo dei sistemi informativi all'interno delle organizzazioni. Fu concepito per guidare le imprese attraverso la complessità dei processi IT, COBIT mira a garantire una gestione efficace delle risorse digitali, allineata agli obiettivi strategici aziendali, nel rispetto delle normative vigenti e con un'attenzione costante alla gestione dei rischi connessi alla tecnologia dell'informazione.

COBIT si distingue per la sua articolazione su quattro principi fondamentali: allineamento tra IT e obiettivi aziendali, trasparenza delle responsabilità, gestione dei rischi e monitoraggio delle prestazioni.

Questi principi si traducono in una serie di domini di processo, obiettivi di controllo e linee guida pratiche che fungono da bussola per le organizzazioni nell'ottimizzare l'utilizzo delle risorse IT, migliorare la trasparenza e l'accountability, e garantire la conformità normativa.

Figure 5—COBIT Components of a Governance System



TABELLA A-4.17:

Reference	BSC Dimension	Enterprise Goal	Example Metrics
EG01	Financial	Portfolio of competitive products and services	<ul style="list-style-type: none"> • Percent of products and services that meet or exceed targets in revenues and/or market share • Percent of products and services that meet or exceed customer satisfaction targets • Percent of products and services that provide competitive advantage • Time-to-market for new products and services
EG02	Financial	Managed business risk	<ul style="list-style-type: none"> • Percent of critical business objectives and services covered by risk assessment • Ratio of significant incidents that were not identified in risk assessments vs. total incidents • Appropriate frequency of update of risk profile
EG03	Financial	Compliance with external laws and regulations	<ul style="list-style-type: none"> • Cost of regulatory noncompliance, including settlements and fines • Number of regulatory noncompliance issues causing public comment or negative publicity • Number of noncompliance matters noted by regulators or supervisory authorities • Number of regulatory noncompliance issues relating to contractual agreements with business partners
EG04	Financial	Quality of financial information	<ul style="list-style-type: none"> • Satisfaction survey of key stakeholders regarding the transparency, understanding and accuracy of enterprise financial information • Cost of regulatory noncompliance with finance-related regulations
EG05	Customer	Customer-oriented service culture	<ul style="list-style-type: none"> • Number of customer service disruptions • Percent of business stakeholders satisfied that customer service delivery meets agreed levels • Number of customer complaints • Trend of customer satisfaction survey results
EG06	Customer	Business service continuity and availability	<ul style="list-style-type: none"> • Number of customer service or business process interruptions causing significant incidents • Business cost of incidents • Number of business processing hours lost due to unplanned service interruptions • Percent of complaints as a function of committed service-availability targets
EG07	Customer	Quality of management information	<ul style="list-style-type: none"> • Degree of board and executive management satisfaction with decision-making information • Number of incidents caused by incorrect business decisions based on inaccurate information • Time to provide supporting information to enable effective business decisions • Timeliness of management information
EG08	Internal	Optimization of internal business process functionality	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 innovation	<ul style="list-style-type: none"> • Level of awareness and understanding of business innovation opportunities • Stakeholder satisfaction with levels of product and innovation expertise and ideas • Number of approved product and service initiatives resulting from innovative ideas

Per soddisfare l'esigenza dell'azienda, abbiamo pensato di implementare l'Enterprise Goal con referenza **EG05**. Questo obiettivo si concentra sull'instaurare una cultura orientata al cliente all'interno dell'organizzazione, con l'obiettivo di fornire servizi di alta qualità che soddisfino le esigenze e le aspettative dei clienti. Una mentalità orientata verso il cliente impone anche di proteggere i dati sensibili dei clienti col fine di migliorare la fiducia fra cliente e azienda.

TABELLA A-4.18:

Figure 4.18—Goals Cascade: Alignment Goals and Metrics

Reference	IT BSC Dimension	Alignment Goal	Metrics
AG01	Financial	I&T compliance and support for business compliance with external laws and regulations	<ul style="list-style-type: none"> Cost of IT noncompliance, including settlements and fines, and the impact of reputational loss Number of IT-related noncompliance issues reported to the board or causing public comment or embarrassment Number of noncompliance issues relating to contractual agreements with IT service providers
AG02	Financial	Managed I&T-related risk	<ul style="list-style-type: none"> Appropriate frequency of update of risk profile Percent of enterprise risk assessments including I&T-related risk Number of significant I&T-related incidents that were not identified in a risk assessment
AG03	Financial	Realized benefits from I&T-enabled investments and services portfolio	<ul style="list-style-type: none"> Percent of I&T-enabled investments for which claimed benefits in the business case are met or exceeded Percent of I&T services for which expected benefits (as stated in the service level agreements) are realized
AG04	Financial	Quality of technology-related financial information	<ul style="list-style-type: none"> Satisfaction of key stakeholders regarding the level of transparency, understanding and accuracy of IT financial information Percent of I&T services with defined and approved operational costs and expected benefits
AG05	Customer	Delivery of I&T services in line with business requirements	<ul style="list-style-type: none"> Percent of business stakeholders satisfied that IT service delivery meets agreed service levels Number of business disruptions due to IT service incidents Percent of users satisfied with the quality of IT service delivery
AG06	Customer	Ability to turn business requirements into operational solutions	<ul style="list-style-type: none"> Level of satisfaction of business executives with IT's responsiveness to new requirements Average time-to-market for new I&T-related services and applications Average time to turn strategic I&T objectives into an agreed and approved initiative Number of critical business processes supported by up-to-date infrastructure and applications
AG07	Internal	Security of information, processing infrastructure and applications, and privacy	<ul style="list-style-type: none"> 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
AG08	Internal	Enabling and supporting business processes by integrating applications and technology	<ul style="list-style-type: none"> Time to execute business services or processes Number of I&T-enabled business programs delayed or incurring additional cost due to technology integration issues Number of business process changes that need to be delayed or reworked because of technology integration issues Number of applications or critical infrastructures operating in silos and not integrated
AG09	Internal	Delivery of programs on time, on budget and meeting requirements and quality standards	<ul style="list-style-type: none"> Number of programs/projects on time and within budget Number of programs needing significant rework due to quality defects Percent of stakeholders satisfied with program/project quality
AG10	Internal	Quality of I&T management information	<ul style="list-style-type: none"> Level of user satisfaction with quality and timeliness and availability of I&T-related management information, taking into account available resources Ratio and extent of erroneous business decisions in which erroneous or unavailable I&T-related information was a key factor
AG11	Internal	I&T compliance with internal policies	<ul style="list-style-type: none"> Number of incidents related to noncompliance with IT-related policies Number of exceptions to internal policies Frequency of policy review and update
AG12	Learning and Growth	Competent and motivated staff with mutual understanding of technology and business	<ul style="list-style-type: none"> Percent of I&T-savvy business people (i.e., those having the required knowledge and understanding of I&T to guide, direct, innovate and see opportunities of I&T for their domain of expertise) Percent of business-savvy IT people (i.e., those having the required knowledge and understanding of relevant business domains to guide, direct, innovate and see opportunities of I&T for the business domain) Number or percentage of business people with technology management experience
AG13	Learning and Growth	Knowledge, expertise and initiatives for business innovation	<ul style="list-style-type: none"> Level of business executive awareness and understanding of I&T innovation possibilities Number of approved initiatives resulting from innovative I&T ideas Number of innovation champions recognized/awarded

L'obiettivo consultivo che abbiamo scelto, in linea con l'esigenza del cliente è l'**advisory goal 07 (AG07)** "Security of information, processing infrastructure and applications, and privacy" nel framework COBIT si concentra sull'**assicurare la sicurezza delle informazioni**, delle infrastrutture di elaborazione e delle applicazioni, nonché sulla protezione della **privacy dei dati**. Questo obiettivo mira a garantire che le risorse informatiche e i dati aziendali siano protetti da minacce interne ed esterne attraverso l'implementazione di controlli di sicurezza appropriati. Inoltre, AG07 si preoccupa di garantire la **conformità alle normative sulla privacy** e alla legislazione relativa alla protezione dei dati, assicurando che le informazioni sensibili siano gestite in modo sicuro e rispettoso della privacy degli individui.

TABELLA B-CAP.4

Figure 5.1 – COBIT Core Model: Governance and Management Objectives and Purpose (cont.)

Reference	Name	Purpose
AP005	Managed portfolio	Optimize the performance of the overall portfolio of programs in response to individual program, product and service performance and changing enterprise priorities and demand.
AP006	Managed budget and costs	Foster a partnership between IT and enterprise stakeholders to enable the effective and efficient use of IT-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 IT solutions and services.
AP007	Managed human resources	Optimize human-resources capabilities to meet enterprise objectives.
AP008	Managed relationships	Enable the right knowledge, skills and behaviors to create improved outcomes, increased confidence, mutual trust and effective use of resources that stimulate a productive relationship with business stakeholders.
AP009	Managed service agreements	Ensure that IT products, services and service levels meet current and future enterprise needs.
AP010	Managed vendors	Optimize available IT capabilities to support the IT strategy and road map, minimize the risk associated with nonperforming or noncompliant vendors, and ensure competitive pricing.
AP011	Managed quality	Ensure consistent delivery of technology solutions and services to meet the quality requirements of the enterprise and satisfy stakeholder needs.
AP012	Managed risk	Integrate the management of IT-related enterprise risk with overall enterprise risk management (ERM) and balance the costs and benefits of managing IT-related enterprise risk.
AP013	Managed security	Keep the impact and occurrence of information security incidents within the enterprise's risk appetite levels.
AP014	Managed data	Ensure effective utilization of the critical data assets to achieve enterprise goals and objectives.
BAI01	Managed programs	Realize desired business value and reduce the risk of unexpected delays, costs and value erosion. To do so, improve communications to and involvement of business and end users, ensure the value and quality of program deliverables and follow-up of projects within the programs, and maximize program contribution to the investment portfolio.
BAI02	Managed requirements definition	Create optimal solutions that meet enterprise needs while minimizing risk.
BAI03	Managed solutions identification and build	Ensure agile and scalable delivery of digital products and services. Establish timely and cost-effective solutions (technology, business processes and workflows) capable of supporting enterprise strategic and operational objectives.
BAI04	Managed availability and capacity	Maintain service availability, efficient management of resources and optimization of system performance through prediction of future performance and capacity requirements.
BAI05	Managed organizational change	Prepare and commit stakeholders for business change and reduce the risk of failure.
BAI06	Managed IT changes	Enable fast and reliable delivery of change to the business. Mitigate the risk of negatively impacting the stability or integrity of the changed environment.
BAI07	Managed IT change acceptance and transitioning	Implement solutions safely and in line with the agreed expectations and outcomes.

Nella tabella B-CAP.4, abbiamo selezionato 3 punti che fanno al caso dell'azienda in questione per risolvere e migliorare la loro situazione.

- 1. APO12 - Manage Risk:** Questo obiettivo di processo si concentra sulla gestione dei rischi correlati all'IT. Include l'identificazione, l'analisi, la valutazione e la gestione dei rischi per assicurare che l'IT supporti e protegga gli obiettivi aziendali.
- 2. APO13 - Manage Security:** APO13 riguarda la gestione della sicurezza dell'IT. Questo processo si occupa di proteggere le risorse IT da minacce interne ed esterne attraverso l'implementazione di controlli di sicurezza adeguati e il mantenimento di livelli appropriati di sicurezza delle informazioni.
- 3. APO14 - Manage Data:** APO14 è incentrato sulla garanzia della privacy e dei dati nell'ambiente IT. Questo processo si occupa di garantire che le informazioni personali e sensibili siano gestite in conformità con le normative sulla privacy e che siano implementati adeguati controlli per proteggere la privacy dei dati.

Questi obiettivi di processo sono fondamentali per garantire che l'IT supporti gli obiettivi aziendali, proteggendo le risorse e rispettando le normative e le politiche relative alla gestione del rischio, della sicurezza e della privacy.

Ruoli e responsabilità per le pratiche scelte (APO12 - Manage Risk, APO13 - Manage Security, APO14 - Manage Data):

Responsabile della gestione del rischio: Mario Rossi, Chief Information Security Officer (CISO), è responsabile di coordinare e supervisionare l'intero processo di gestione del rischio, inclusa l'identificazione dei rischi, l'analisi, la valutazione e la gestione delle risposte ai rischi.

Responsabile della sicurezza dell'IT: Laura Bianchi, Responsabile della Sicurezza IT, è incaricata dell'implementazione e del mantenimento dei controlli di sicurezza dell'IT per proteggere le risorse e i dati aziendali da minacce interne ed esterne.

Responsabile della privacy dei dati: Alessandro Verdi, Data Protection Officer (DPO), è responsabile di garantire che le informazioni personali e sensibili siano gestite in conformità con le normative sulla privacy e di implementare i controlli necessari per proteggere la privacy dei dati.

Input/Output per le pratiche scelte (APO12 - Manage Risk, APO13 - Manage Security, APO14 - Manage Data):

Input: Gli input includono l'analisi dei rischi condotta dal team di sicurezza dell'IT, le valutazioni della sicurezza dell'IT, le politiche aziendali sulla privacy e sui dati, i requisiti normativi e legali applicabili, nonché i risultati di revisioni interne ed esterne condotte dal team di conformità.

Output: Gli output di queste pratiche possono includere piani di gestione del rischio approvati, procedure operative standard per la sicurezza dell'IT, politiche sulla privacy dei dati aggiornate, rapporti di conformità normativa, risultati di test di vulnerabilità e analisi delle minacce.

Documenti aziendali per descrivere la policy o la procedura:

Le policy e le procedure relative alla gestione del rischio, alla sicurezza dell'IT e alla privacy dei dati dovrebbero essere documentate nei seguenti documenti:

Politica di sicurezza dell'IT: Questa politica, sviluppata dal team di sicurezza dell'IT con il supporto del CISO, definisce le regole e le linee guida per proteggere le risorse IT dall'accesso non autorizzato, dalle minacce e dagli attacchi.

Politica sulla gestione del rischio: Questo documento, sviluppato dal team di gestione del rischio sotto la supervisione del CISO, stabilisce i principi e le procedure per identificare, valutare e gestire i rischi associati all'IT e alle operazioni aziendali.

Politica sulla privacy dei dati: Questa politica, sviluppata dal DPO in collaborazione con il team legale e il team IT, specifica come l'azienda raccoglie, utilizza, conserva e protegge le informazioni personali dei clienti e degli utenti, garantendo la conformità alle normative sulla privacy.

Servizi coinvolti:

Uno dei servizi critici coinvolti è il nostro sistema di archiviazione cloud, utilizzato per conservare dati aziendali sensibili come informazioni finanziarie e personali dei clienti. Inoltre, il servizio di gestione delle identità e degli accessi (**IAM**) è cruciale per garantire che solo persone autorizzate possano accedere ai nostri sistemi e alle nostre risorse digitali.

Non possiamo trascurare il servizio di monitoraggio della rete, fondamentale per rilevare e mitigare le minacce informatiche in tempo reale.

Infrastrutture coinvolti:

La nostra infrastruttura di comunicazione, che include **router**, **switch** e **firewall**, costituisce la base della nostra rete aziendale e deve essere protetta da intrusioni e attacchi.

Il nostro data center aziendale è il cuore pulsante delle nostre operazioni, quindi garantire la sicurezza fisica e logica di questa infrastruttura è una priorità.

Utilizziamo anche l'infrastruttura cloud fornita da provider come **AWS** e **Azure** per sostenere le nostre applicazioni e i nostri servizi digitali.

Applicazioni coinvolti:

Le applicazioni aziendali critiche, come il nostro sistema di contabilità e il **CRM**, sono fondamentali per il funzionamento quotidiano dell'azienda e devono essere protette da accessi non autorizzati e violazioni della sicurezza.

Le applicazioni Web che offriamo ai nostri clienti, come il nostro portale self-service, devono garantire la sicurezza delle transazioni online e la protezione dei dati personali. Inoltre, abbiamo applicazioni di gestione documentale per gestire e archiviare documenti sensibili come contratti e report finanziari.



**PHANTOM
SRL**

PREPARED FOR :
BCC ICCREA

GRAZIE

PRESENTED BY:
GIUSEPPE PIGNATELLO
ALESSIO D'OTTAVIO
LUCA IANNONE