



PRATICA S3-L2

GOVERNANCE DEL RISCHIO

FIORILLO ALEX

BONATO LISA

MINOTTI MARIA FLAVIA

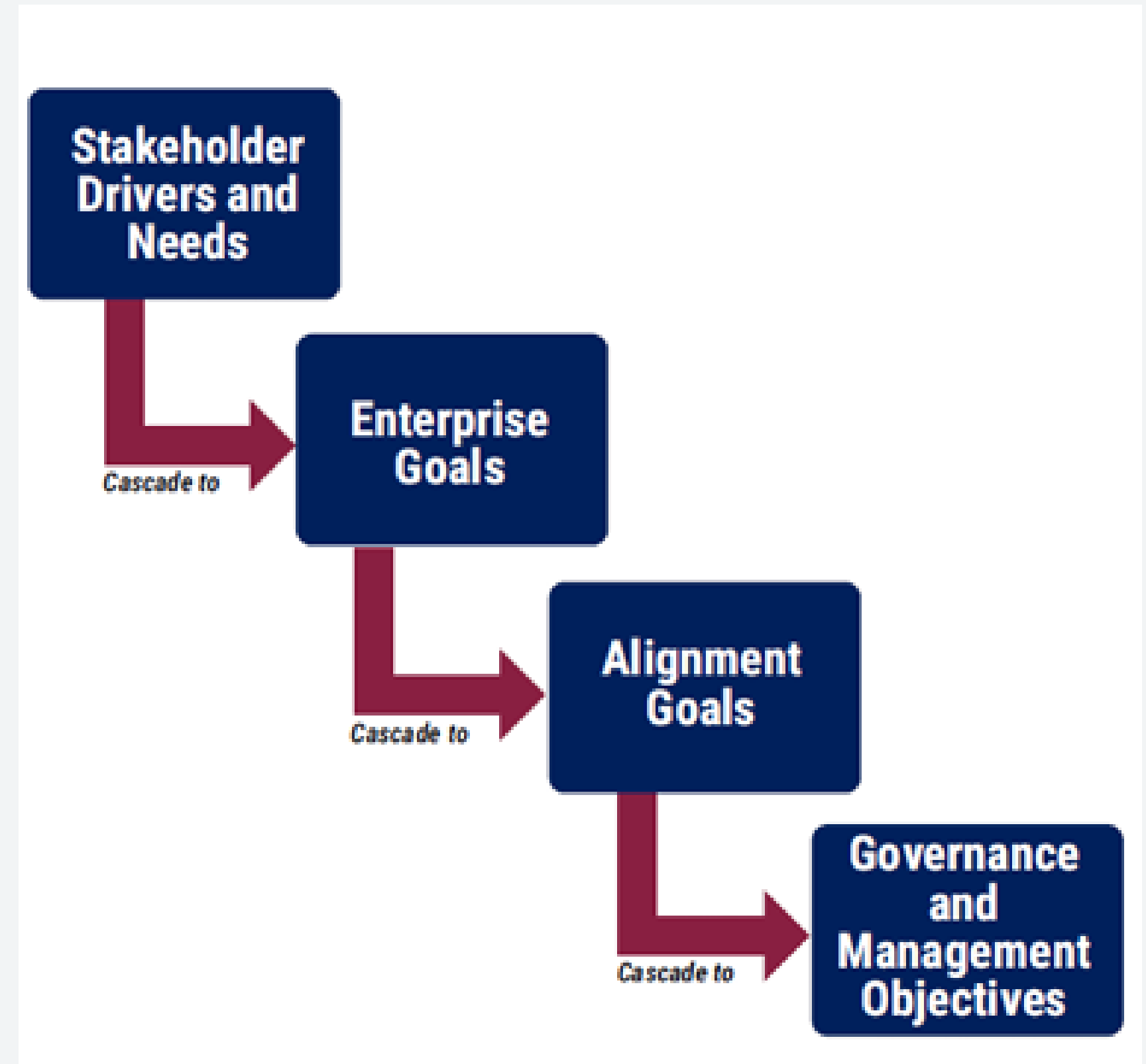
Questo esercizio richiede il download delle seguenti risorse:

- **A:** COBIT 2019 Framework: Introduction & Methodology | Digital | English
- **B:** COBIT 2019 Framework: Governance & Management Objectives | Digital | English
- COBIT 2019 Toolkit
- **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 a quello 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**



Stakeholder Drivers and Needs: bisogno di tutelare i dati sensibili degli utenti in conformità alle normative per migliorare anche la fiducia dei clienti verso l’organizzazione.

Enterprise Goals (EG03): conformità con regolamenti e leggi esterne.

- Costo della non conformità normativa, inclusi accordi transattivi e multe
- Numero di questioni di non conformità normativa che causano commenti pubblici o pubblicità negative
- Numero di questioni di non conformità rilevate da regolatori o autorità di vigilanza
- Numero di questioni di non conformità normativa relative a accordi contrattuali con partner commerciali

Figure 4.17—Goals Cascade: Enterprise Goals and Metrics			
Reference	BSC Dimension	Enterprise Goal	Example Metrics
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

Alignment Goals (AG01): Conformità finanziaria e supporto IT per la conformità aziendale alle leggi e ai regolamenti esterni.

- Costo della non conformità IT, inclusi accordi transattivi e multe, e l'impatto sulla perdita di reputazione
- Numero di questioni di non conformità legate all'IT segnalate al consiglio o che causano commenti pubblici o imbarazzo
- Numero di questioni di non conformità relative agli accordi contrattuali con i fornitori di servizi IT

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

Nella tabella seguente vediamo che uno degli alignment principali (**P**) rispetto all'enterprise goal selezionato è proprio **AG01**.

[illegible]

Governance and Management Objectives (EDM01): Garantito le impostazioni e il mantenimento del governance framework.

Descrizione: Analizzare e articolare i requisiti per la governance dell'I&T aziendale. Creare e mantenere i componenti della governance con chiarezza di autorità e responsabilità per raggiungere la missione, gli obiettivi e le finalità dell'impresa.

Scopo:

Fornire un approccio coerente, integrato e allineato con l'approccio di governance aziendale. Le decisioni relative all'IT devono essere prese in linea con le strategie e gli obiettivi dell'azienda e il valore desiderato deve essere realizzato. A tal fine, assicurarsi che i processi relativi all'IT siano supervisionati in modo efficace e trasparente; confermare la conformità ai requisiti legali, contrattuali e regolamentari; e soddisfare i requisiti di governance per i membri del consiglio.

Figure 5.1—COBIT Core Model: Governance and Management Objectives and Purpose		
Reference	Name	Purpose
EDM01	Ensured governance framework setting and maintenance	Provide a consistent approach, integrated and aligned with the enterprise governance approach. I&T-related decisions must be made in line with the enterprise's strategies and objectives and desired value is realized. To that end, ensure that I&T-related processes are overseen effectively and transparently; compliance with legal, contractual and regulatory requirements is confirmed; and the governance requirements for board members are met.

Nella tabella seguente vediamo che, per l’alignment goal precedentemente scelto, uno dei principali obiettivi di governance e management è **EDM01**.

Figure—A.2 Mapping Governance and Management Objectives to Alignment Goals														
		AG01	AG02	AG03	AG04	AG05	AG06	AG07	AG08	AG09	AG10	AG11	AG12	AG13
		I&T compliance and support for business compliance with external laws and regulations	Managed I&T-related risk	Realized benefits from I&T-enabled investments and services portfolio	Quality of technology-related financial information	Delivery of I&T services in line with business requirements	Agility to turn business requirements into operational solutions	Security of information, processing infrastructure and applications, and privacy	Enabling and supporting business processes by integrating applications and technology	Delivering programs on time, on budget and meeting requirements and quality standards	Quality of I&T management information	I&T compliance with internal policies	Competent and motivated staff with mutual understanding of technology and business	Knowledge, expertise and initiatives for business innovation
EDM01	Ensured governance framework setting and maintenance	P	S	P					S			S		

Pratica scelta (EDM01.01): Valutare il sistema di governance.

Descrizione: Identificare e coinvolgere continuamente gli stakeholder dell'azienda, documentare la comprensione dei requisiti e valutare il design attuale e futuro della governance dell'IT aziendale.

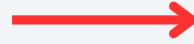
A. Component: Process	
Governance Practice	Example Metrics
EDM01.01 Evaluate the governance system. Continually identify and engage with the enterprise's stakeholders, document an understanding of the requirements, and evaluate the current and future design of governance of enterprise I&T.	a. Number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

Rispetto alla nostra pratica scelta (**EDM01**) si rintracciano tre pratiche:

- EDM01.01 - Valutare il sistema di governance
- EDM01.02 - Dirigere il sistema di governance
- EDM01.03 - Monitorare il sistema di governance

Abbiamo scelto di analizzare la prima pratica per dare risposta alle domande successive.

Quali sono i ruoli e le responsabilità per questa pratica? B/C

B. Component: Organizational Structures					
Key Governance Practice					
 EDM01.01 Evaluate the governance system.	Board	Executive Committee	Chief Executive Officer	Chief Information Officer	I&T Governance Board
	A	R	R	R	R
	A	R			R
	A	R	R	R	R

- **Board** - Accountable
- **Executive Committee** - Responsible
- **Chief Executive Officer** - Responsible
- **Chief Information Officer** - Responsible
- **I&T Governance Board** - Responsible

R (Responsible): la persona o il team che ha la responsabilità primaria per l'esecuzione dell'attività o per il raggiungimento della decisione.

A (Accountable): la persona che ha la responsabilità ultima del completamento dell'attività o del successo della decisione. E' l'owner dell'attività o della decisione e deve approvarla prima che possa essere completata.

Quali sono gli input/output per questa pratica? B

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

Gli **input** sono:

- MEA03.02 - Comunicazioni di cambiamenti di requisiti di compliance
- Esterno al COBIT - Costituzione/leggi/statuti di organizzazione, governance/modello decisionale, leggi/regolamenti, tendenze ambientali del business

Gli **output** invece:

- Principi guida della governance aziendale
- Modello decisionale
- Livelli di autorità

In quale documento aziendale dovrebbe essere descritta la policy o la procedura? B

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)

Quali servizi/infrastrutture/applicazioni sono coinvolti? B

G. Component: Services, Infrastructure and Applications

- COBIT and related products/tools
- Equivalent frameworks and standards

Sono coinvolti:

- COBIT e relativi prodotti/strumenti
- Standard/framework equivalenti