EPICODE

S3 - L2

Governance del rischio

13 maggio 2024

Team

- Davide di Turo
- Manuel Di Gangi
- Marco Fasani

INDICE

Traccia

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

1. Enterprise Goals

EG02 - Managed business risk

- Percentuale di obiettivi e servizi aziendali critici coperti dalla valutazione del rischio
- Rapporto tra incidenti significativi che non sono stati identificati nelle valutazioni del rischio rispetto al totale degli incidenti
- Frequenza adeguata di aggiornamento del profilo di rischio

EG03 - Compliance with external laws and regulations

- Costo della non conformità normativa, inclusi risarcimenti e multe
- Numero di problemi di non conformità normativa che hanno causato commenti pubblici o pubblicità negativa
- Numero di problemi di non conformità rilevati dalle autorità di regolamentazione o di vigilanza
- Numero di problemi di non conformità normativa relativi ad accordi contrattuali con partner commerciali

EG02	Financial	Managed business risk	• 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	• 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

2. Alignment Goals

		EG01 Portfolio of competitive products and services	EG02 Managed business risk	EG03 Compliance with external laws and regulations
AG01	I&T compliance and support for business compliance with external laws and regulations		S	P
AG02	Managed I&T-related risk		P	
AG03	Realized benefits from I&T-enabled investments and services portfolio	S		
AG04	Quality of technology-related financial information			
AG05	Delivery of I&T services in line with business requirements	P		
AG06	Agility to turn business requirements into operational solutions	P		
AG07	Security of information, processing infrastructure and applications, and privacy		P	
AG08	Enabling and supporting business processes by integrating applications and technology	P		
AG09	Delivering programs on time, on budget and meeting requirements and quality standards	P		
AG10	Quality of I&T management information			
AG11	I&T compliance with internal policies		S	P
AG12	Competent and motivated staff with mutual understanding of technology and business			
AG13	Knowledge, expertise and initiatives for business innovation	P		S

EG02 - Managed business risk

Primary:

- AG02 - Managed I&T-related risk
- AG07 - Security of information, processing infrastructure and applications, and privacy

Secondary:

- AG01 - I&T compliance and support for business compliance with external laws and regulations
- AG11 - I&T compliance with internal policies

EG03 - Compliance with external laws and regulations

- AG01 - I&T compliance and support for business compliance with external laws and regulations
- AG11 - I&T compliance with internal policies

Secondary:

- AG13 - Knowledge, expertise and initiatives for business innovation

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	• 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	• 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
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

Figure 4.18—Goals Cascade: Alignment Goals and Metrics *(cont.)*			
Reference	**IT BSC Dimension**	**Alignment Goal**	**Metrics**
AG11	Internal	I&T compliance with internal policies	• 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	• 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	• 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

3. Governance and Management Objectives

AG01 - I&T compliance and support for business compliance with external laws and regulations

EDM01

Descrizione	
Mettere in atto e mantenere i componenti di governance con chiarezza di autorità e responsabilità per raggiungere la missione, gli obiettivi e gli obiettivi dell'azienda.	
Scopo	
Fornire un approccio coerente, integrato e allineato con l'approccio di governance aziendale. Le decisioni relative all'I&T vengono prese in linea con le strategie e gli obiettivi dell'azienda e viene realizzato il valore desiderato. A tal fine, garantire che i processi relativi all'I&T siano supervisionati in modo efficace e trasparente; il rispetto dei requisiti legali, contrattuali e regolamentari; e i requisiti di governance per i membri del consiglio di amministrazione sono soddisfatti.	
L'obiettivo di governance supporta il raggiungimento di una serie di obiettivi aziendali e di allineamento primari:	
Enterprise Goals	**Alignment Goals**
EG03 - Rispetto delle leggi e dei regolamenti esterni	AG01 - Conformità I&T e supporto per la conformità aziendale con leggi e regolamenti esterni
Governance Practice	
EDM01.02 Dirigere il sistema di governance	
Attività	
1. Comunicare la governance dei principi I&T e concordare con il management esecutivo il modo per stabilire una leadership informata e impegnata.	
2. Stabilire o delegare la creazione di strutture, processi e pratiche di governance in linea con i principi di progettazione concordati.	

3. Istituire un comitato di governance I&T (o equivalente) a livello di consiglio. Questo consiglio dovrebbe garantire che la governance dell'informazione e della tecnologia, come parte della governance aziendale, sia adeguatamente affrontata; consigliare la direzione strategica; e determinare la priorità dei programmi di investimento abilitati all'I&T in linea con la strategia e le priorità aziendali dell'impresa.
4. Assegnare responsabilità, autorità e responsabilità per le decisioni I&T in linea con i principi di progettazione della governance, i modelli decisionali e la delega concordati.
5. Garantire che i meccanismi di comunicazione e reporting forniscono informazioni adeguate ai responsabili della supervisione e del processo decisionale.
6. Dire che il personale segua le linee guida pertinenti per il comportamento etico e professionale e garantire che le conseguenze della non conformità siano note e applicate.
7. Dirigere la creazione di un sistema di ricompensa per promuovere il cambiamento culturale auspicabile.

Guida correlata (standard, quadri normativi, requisiti di conformità)	**Riferimento dettagliato**
CMMI Cyber Maturity 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)

APO01

Descrizione	
Progettare il sistema di gestione per l'I&T aziendale in base agli obiettivi aziendali e ad altri fattori di progettazione. Sulla base di questo progetto, implementare tutti i componenti necessari del sistema di gestione.	
Scopo	
Implementare un approccio di gestione coerente per soddisfare i requisiti di governance aziendale, coprendo le componenti di governance come i processi di gestione; strutture organizzative; ruoli e responsabilità; attività affidabili e ripetibili	
L'obiettivo di governance supporta il raggiungimento di una serie di obiettivi aziendali e di allineamento primari:	
Enterprise Goals	**Alignment Goals**
EG03 - Rispetto delle leggi e dei regolamenti esterni	AG11 - I&T compliance with internal policies
Management Practice	
APO01.01 Design the management system for enterprise I&T.e	
Attività	
1. Comprendere la visione, la direzione e la strategia dell'impresa, nonché il contesto e le sfide attuali dell'impresa	
2. Considerare l'ambiente interno dell'azienda, compresa la cultura e la filosofia di gestione, la tolleranza al rischio, la politica di sicurezza e privacy, i valori etici, il codice di condotta, la responsabilità e i requisiti per l'integrità della gestione.	
3. Applicare la cascata degli obiettivi COBIT e i fattori di progettazione alla strategia e al contesto aziendale per decidere le priorità per il sistema di gestione e, quindi, per l'attuazione delle priorità degli obiettivi di gestione.	

4. Convalidare le priorità selezionate per l'attuazione degli obiettivi di gestione con buone pratiche o requisiti specifici del settore (ad esempio, regolamenti specifici del settore) e con strutture di governance appropriate.

Guida correlata (standard, quadri normativi, requisiti di conformità)	**Riferimento dettagliato**
COSO Enterprise Risk Management, June 2017	7. Strategy and Objective-Setting—Principle 9
ISO/IEC 27001:2013/Cor.2:2015(E)	International standard for establishing, implementing and maintaining a management system (all chapters)
ITIL V3, 2011	Service Strategy, 2.3 Governance and management systems

Implementare un approccio gestionale coerente per soddisfare i requisiti di governance aziendale, coprendo le componenti di governance come i processi di gestione; strutture organizzative; ruoli e responsabilità; attività affidabili e ripetibili; elementi informativi; politiche e procedure; capacità e competenze; cultura e comportamento; servizi, infrastrutture e applicazioni.

Numero e Nome Processo	**Descrizione**	**Azioni Chiave**
APO01.01 - Progettare il sistema di gestione per l'I&T aziendale	Progettare un sistema di gestione adattato alle esigenze dell'azienda. Le esigenze gestionali dell'azienda sono definite attraverso l'uso della cascata degli obiettivi e mediante l'applicazione dei fattori di progettazione. Assicurarsi che i componenti di governance siano integrati e allineati alla filosofia di governance e gestione dell'azienda e allo stile operativo.	- Definire un sistema di gestione su misura per l'azienda. - Integrare e allineare i componenti di governance con la filosofia di governance e gestione dell'azienda.

APO01.02 - Comunicare obiettivi di gestione, direzione e decisioni prese	Comunicare la consapevolezza e promuovere la comprensione degli obiettivi di allineamento e I&T agli stakeholder dell'azienda. Comunicare a intervalli regolari importanti decisioni relative all'I&T e il loro impatto sull'organizzazione.	- Comunicare agli stakeholder gli obiettivi di allineamento e I&T. - Comunicare regolarmente le decisioni importanti relative all'I&T e il loro impatto.
APO01.03 - Implementare processi di gestione (per supportare il raggiungimento degli obiettivi di governance e gestione)	Definire i livelli di capacità dei processi target e le priorità di implementazione in base al design del sistema di gestione.	Definire i livelli di capacità dei processi target. - Prioritzare l'implementazione in base al design del sistema di gestione
APO01.04 - Definire ed implementare le strutture organizzative	Mettere in atto le strutture organizzative interne ed estese necessarie (ad esempio, comitati) secondo il design del sistema di gestione, consentendo una presa di decisione efficace ed efficiente. Assicurarsi che le conoscenze tecnologiche e informative necessarie siano incluse nella composizione delle strutture di gestione.	Mettere in atto le strutture organizzative necessarie. - Assicurarsi che le conoscenze tecnologiche e informative siano incluse nella composizione delle strutture di gestione.
APO01.05 - Stabilire ruoli e responsabilità	Definire e comunicare ruoli e responsabilità per l'I&T aziendale, inclusi livelli di autorità, responsabilità e responsabilità.	Definire e comunicare i ruoli e le responsabilità per l'I&T aziendale.
APO01.06 - Ottimizzare il posizionamento della funzione IT	Posizionare le capacità IT nella struttura organizzativa complessiva per riflettere l'importanza strategica e la dipendenza operativa dell'IT all'interno dell'azienda. La linea gerarchica del CIO e la rappresentazione dell'IT all'interno della direzione aziendale dovrebbero essere commisurate all'importanza dell'I&T all'interno dell'azienda	Posizionare le capacità IT nella struttura organizzativa. - Assicurarsi che la linea gerarchica del CIO e la rappresentazione dell'IT nella direzione aziendale riflettano l'importanza dell'I&T.

APO01.07 - Definire la proprietà delle informazioni (dati) e dei sistemi	Definire e mantenere responsabilità per la proprietà delle informazioni (dati) e dei sistemi informativi. Assicurarsi che i proprietari classifichino le informazioni e i sistemi e li proteggano in linea con la loro classificazione.	Definire e mantenere responsabilità per la proprietà delle informazioni (dati) e dei sistemi. - Assicurarsi che i proprietari classifichino e proteggano le informazioni e i sistemi in linea con la loro classificazione
APO01.08 - Definire competenze e abilità target	Definire le competenze e le abilità necessarie per raggiungere gli obiettivi di gestione rilevanti.	Definire le competenze e le abilità necessarie.
APO01.09 - Definire e comunicare politiche e procedure	Mettere in atto procedure per mantenere la conformità e la misurazione delle prestazioni delle politiche e degli altri componenti del framework di controllo. Applicare le conseguenze della non conformità o delle prestazioni inadeguate. Monitorare le tendenze e le prestazioni e tenerle in considerazione nel futuro design e miglioramento del framework di controllo.	Mettere in atto procedure per mantenere la conformità e la misurazione delle prestazioni delle politiche e degli altri componenti del framework di controllo. - Applicare le conseguenze della non conformità o delle prestazioni inadeguate.
APO01.10 - Definire ed implementare infrastrutture, servizi e applicazioni per supportare il sistema di governance e gestione	Definire ed implementare infrastrutture, servizi e applicazioni per supportare il sistema di governance e gestione (ad esempio, repository architetturali, sistema di gestione dei rischi, strumenti di gestione dei progetti, strumenti di monitoraggio dei costi e strumenti di monitoraggio degli incidenti).	Definire ed implementare infrastrutture, servizi e applicazioni per supportare il sistema di governance e gestione.
APO01.11 - Gestire il miglioramento continuo del sistema di gestione I&T	Migliorare continuamente i processi e gli altri componenti del sistema di gestione per garantire che possano raggiungere gli obiettivi di governance e gestione. Considerare l'orientamento all'implementazione	Migliorare continuamente i processi e gli altri componenti del sistema di gestione. - Considerare l'orientamento all'implementazione COBIT, gli standard emergenti, i requisiti di

	COBIT, gli standard emergenti, i requisiti di conformità, le opportunità di automazione e il feedback degli stakeholder.	conformità, le opportunità di automazione e il feedback degli stakeholder

4. Pratica per soddisfare l'esigenza dell'Alta Direzione

1. Quali sono i ruoli e le responsabilità per questa pratica?

Figura	Ruolo	Responsabilità
Executive Committee	Accountable	APO01.01 APO01.02 APO01.03 APO01.04 APO01.05 APO01.06 APO01.07 APO01.08 APO01.09 APO01.10 APO01.11
Chief Risk Officer	Responsible	APO01.02 APO01.03
Chief Technology Officer	Responsible	APO01.01 APO01.02 APO01.03 APO01.04 APO01.05 APO01.06 APO01.07 APO01.08 APO01.09 APO01.10

		APO01.11
Chief Digital Officer	Responsible	APO01.01 APO01.02 APO01.03 APO01.04 APO01.05 APO01.06 APO01.07 APO01.08 APO01.09 APO01.10 APO01.11
I&T Governance Board	Responsible	APO01.01 APO01.02 APO01.03 APO01.04 APO01.05 APO01.06 APO01.07 APO01.08 APO01.09 APO01.10 APO01.11
Architecture Board	Responsible	APO01.09
Enterprise Risk Committee	Responsible	APO01.06 APO01.07 APO01.09
Chief Information Security Officer	Responsible	APO01.02 APO01.03
Business Process Owners	Responsible	APO01.07 APO01.09 APO01.11
Data Management Function	Responsible	APO01.07 APO01.09

		APO01.10 APO01.11
Head Human Resources	Responsible	APO01.04 APO01.09
Relationship Manager	Responsible	APO01.02
Head Architect	Responsible	APO01.07 APO01.08 APO01.09 APO01.10 APO01.11
Head Development	Responsible	APO01.08 APO01.09 APO01.10 APO01.11
Head IT operations & Head administration	Responsible	APO01.08 APO01.09 APO01.10 APO01.11
Service Manager & Information Security Manager & Business Continuity Manager	Responsible	APO01.09 APO01.10 APO01.11
Privacy Officer	Responsible	APO01.09 APO01.10 APO01.11

2. Quali sono gli input/output per questa pratica?

PRATICA	INPUT	OUTPUT
APO01.01	APO02.05, APO12.01, APO12.02, EDM01.01	All APO; All BAI; All DSS; All MEA
APO01.02	APO12.06, DSS04.01, DSS05.01, DSS05.02, DSS05.03, EDM01.02, EDM04.02	All APO; All BAI; All DSS; All MEA
APO01.03	APO02.04, EDM01.01	All APO; All BAI; All DSS; All MEA
APO01.04	APO03.02, EDM01.01	APO03.02
APO01.05	APO07.03, APO11.01, APO13.01, DSS06.03, EDM01.01, EDM04.02	APO07.01; DSS05.04
APO01.06	Outside COBIT	APO03.02
APO01.07	-	APO03.02; APO14.01; BAI02.01; DSS05.02; DSS06.01
APO01.08	-	APO07.03
APO01.09	DSS01.04, MEA03.02	MEA01.05
APO01.10	APO09.01, Outside COBIT	APO02.02; APO02.03
APO01.11	APO01.03, EDM01.03, MEA03.02	All APO; All BAI; All DSS; All MEA - MEA01.02 - MEA01.03

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

Politiche: Dichiarazioni di intenti e linee guida generali che stabiliscono l'approccio dell'organizzazione alla gestione dei processi APO01, inclusi gli obiettivi strategici, le responsabilità e le aspettative.

Procedure: Dettagliate istruzioni passo-passo su come eseguire specifiche attività o processi all'interno del processo APO01. Ciò potrebbe includere procedure per la definizione di obiettivi e strategie IT, la pianificazione e l'allocazione delle risorse, la definizione dei ruoli e delle responsabilità, ecc.

Responsabilità e Autorizzazioni: Chiarezza sui ruoli e le responsabilità delle persone coinvolte nell'attuazione del processo APO01, nonché sulle autorizzazioni necessarie per eseguire determinate azioni all'interno del processo.

Aggiornamenti e Revisioni: Indicazioni su come le politiche e le procedure relative al processo APO01 vengono aggiornate, revisionate e comunicate all'interno dell'organizzazione.

4. Quali servizi/infrastrutture/applicazioni sono coinvolti?

Executive Committee: Coinvolto nell' orientazione strategica generale dell'organizzazione e potrebbe essere interessato a tutti gli aspetti dell IT che supportano gli obiettivi aziendali.

Chief Risk Officer: Coinvolto nella gestione dei rischi aziendali, compresi i rischi legati alla tecnologia dell'informazione e alla sicurezza informatica.

Chief Technology Officer: Coinvolto nello sviluppo e nell'implementazione delle strategie tecnologiche aziendali, potrebbe essere interessato a una vasta gamma di servizi e infrastrutture IT.

Chief Digital Officer: Coinvolto nello sviluppo e nell'implementazione di iniziative digitali e potrebbe essere interessato a servizi e applicazioni orientate al digitale.

I&T Governance Board: Coinvolto nella governance dell'IT e potrebbe essere interessato a tutte le aree dell'IT che influenzano le decisioni strategiche dell'organizzazione.

Architecture Board: Coinvolto nella definizione e nell'approvazione dell'architettura IT aziendale, quindi potrebbe essere interessato a infrastrutture, applicazioni e servizi che rientrano nell'ambito di questa architettura.

Enterprise Risk Committee: Coinvolto nella gestione dei rischi aziendali a livello strategico e potrebbe essere interessato a rischi legati alla tecnologia dell'informazione.

Chief Information Security Officer: Coinvolto nella sicurezza delle informazioni e potrebbe essere interessato a tutti i servizi, le infrastrutture e le applicazioni che implicano rischi per la sicurezza.

Business Process Owners: Coinvolto nella gestione dei processi aziendali e potrebbe essere interessato alle applicazioni che supportano tali processi.

Data Management Function: Coinvolto nella gestione dei dati aziendali e potrebbe essere interessato alle infrastrutture e alle applicazioni coinvolte nella gestione, nell' archiviazione e nell'analisi dei dati.

Head Human Resources: Coinvolto nella gestione delle risorse umane e potrebbe essere interessato a sistemi IT che supportano le funzioni HR.

Relationship Manager: Coinvolto nel gestire le relazioni con i fornitori esterni di servizi IT.

Head Architect: Coinvolto nella definizione dell'architettura IT e potrebbe essere interessato a infrastrutture e applicazioni che supportano tale architettura.

Head Development: Coinvolto nello sviluppo di software e potrebbe essere interessato a tutti gli strumenti e le tecnologie utilizzate nello sviluppo.

Head IT Operations & Head Administration: Coinvolto nella gestione delle operazioni IT e delle infrastrutture IT generali.

Service Manager & Information Security Manager Coinvolti nella gestione dei servizi IT e nella sicurezza delle informazioni e nella continuità aziendale,

Business Continuity Manager: Coinvolti nella sicurezza delle informazioni e nella continuità aziendale

Privacy Officer: Coinvolto nella gestione della privacy dei dati e potrebbe essere interessato a servizi e applicazioni che coinvolgono dati personali sensibili.