4.1

Versione Italiana

Framework

Control Objectives

Management Guidelines

Maturity Models

COBIT®
4.1

Traduzione italiana

Capitolo di Milano

Maggio 2007
Versione originale
pubblicata dall'IT Governance Institute™

Marzo 2008
Traduzione italiana a cura di
Associazione Italiana Information Systems Auditors – AIEA
Capitolo di Milano di ISACA

INGLESE

COBIT®: Control Objectives for Information and related Technology 4.1 (COBIT 4.1) is translated into Italian from the English language version of COBIT 4.1 by the Milan Chapter of the Information Systems Audit and Control Association (ISACA) with the permission of the IT Governance Institute. The Milan Chapter assumes sole responsibility for the accuracy and faithfulness of the translation.

ITGI created COBIT 4.1 ("Work") primarily as an educational resource for controls professionals. ITGI makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, the controls professional should apply his or her own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

ITALIANO

Autorizzazione

COBIT®: Control Objectives for Information and related Technology 4.1 (COBIT 4.1) è tradotto in lingua italiana dalla versione inglese di COBIT 4.1 a cura del Capitolo di Milano di Information Systems Audit and Control Association (ISACA) con l'autorizzazione dell'IT Governance Institute. Il Capitolo di Milano si assume la sola responsabilità della accuratezza della traduzione e della aderenza alla versione originale.

Copyright

Disclaimer

ITGI ha prodotto COBIT 4.1 (Prodotto) innanzitutto come una risorsa formativa per gli esperti del controllo. ITGI non assicura alcun risultato dovuto all'utilizzo del Prodotto. Il Prodotto non deve essere considerato come comprensivo di tutte le informazioni, procedure e test relativi ai controlli, o alternativo ad altre informazioni, procedure e test che ragionevolmente possono permettere di ottenere lo stesso risultato. Nel determinare l'applicabilità di ciascuna specifica informazione, procedura o test, l'esperto dei controlli deve valutare sotto la propria responsabilità la particolare circostanza influenzata dallo specifico sistema o dallo specifico ambito tecnologico.

Avvertenze

Pubblicazione edita in Italia con autorizzazione di ITGI. La traduzione italiana è curata da AIEA – Associazione Italiana Information Systems Auditors - ISACA - Capitolo di Milano.
Per usi commerciali si suggerisce di abbinare il testo italiano con quello inglese.

AIEA – Associazione Italiana Information Systems Auditors
20141 Milano— Via Valla, 16
Tel 0039 02 84742.365- Fax 0039 02 84742.366
E-mail: aiea@aiea.it; Sito: www.aiea.it
P.IVA 10899720154 C.F. 97109000154

AIEA – Associazione Italiana Information Systems Auditors (Capitolo di Milano di ISACA) – ringrazia tutte le aziende di appartenza dei componenti il Gruppo di Ricerca per la disponibilità e per il valore del contributo apportato dai rispettivi rappresentanti. A questi ultimi un particolare ringraziamento per l'impegno, la professionalità dimostrate e per aver contribuito al successo dell'iniziativa.

Coordinamento

Orillo Narduzzo, CISA, CISM	Banca Popolare di Vicenza Vicepresidente AIEA

Gruppo di Ricerca

Stefano Niccolini, CISA, CISM	Federazione Lombarda BCC
Leonardo Nobile, CISA	Deloitte
Alberto Piamonte	Ing. Alberto Piamonte
Marco Salvato, CISM	KPMG
Giulio Spreafico, CISA, CISM	Studio Spreafico

AVVISO

Il Gruppo di Ricerca sollecita i lettori a segnalare correzioni e miglioramenti scrivendo alla Segreteria AIEA all'indirizzo: aiea@aiea.it; sottolinea inoltre l'opportunità di utilizzare nella pratica le due versioni, italiana ed inglese, con il testo a fronte.

Al servizio dei professionisti dell'IT Governance

Capitolo di Milano

Pagina intenzionalmente bianca

MONITORAGGIO E VALUTAZIONE

ME1 Monitorare e valutare le prestazioni dell'IT

ME2 Monitare e valutare i controlli interni

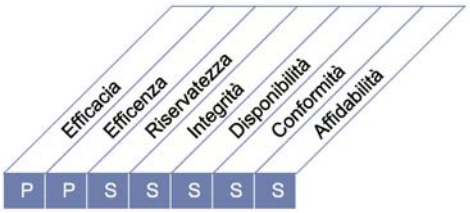
ME3 Assicurare la conformità ai requisiti esterni

ME4 Istituire l'IT Governance

DESCRIZIONE DEL PROCESSO

ME1 Monitorare e valutare le prestazioni dell'IT

Una gestione efficace delle prestazioni IT richiede un processo di monitoraggio. Tale processo comprende la definizione dei più importanti indicatori di prestazione, una informativa sistematica e tempestiva alla Direzione sulle prestazioni rilevate, l'individuazione di interventi solleciti in caso di scostamenti. Il monitoraggio è necessario per assicurarsi che siano adottate le giuste misure e che esse siano in linea con le indicazioni e le politiche aziendali stabilite.



Il controllo del processo IT

Monitorare e valutare le prestazioni dell'IT

che soddisfa i requisiti aziendali per l'IT di

trasparenza e comprensione dei costi IT, dei benefici attesi, della strategia, delle politiche e dei livelli di servizio secondo quanto stabilito dai requisiti di governance aziendale

ponendo l'attenzione su

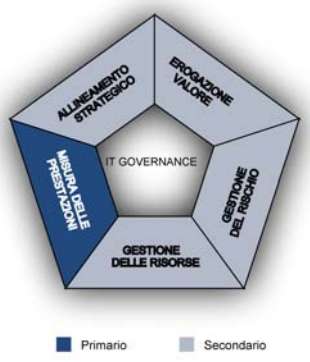
le metriche del processo di monitoraggio e di reporting e la individuazione e l'implementazione di azioni per il miglioramento delle prestazioni

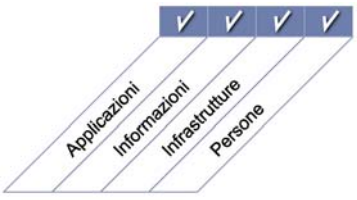
è ottenuto tramite

- il processo di raccolta delle informazioni sulle prestazioni e la loro traduzione in report per la Direzione
- la revisione delle prestazioni rispetto agli obiettivi concordati e l'avvio delle opportune azioni correttive

e viene misurato tramite

- la soddisfazione della Direzione e delle entità/comitati di governo dell'impresa delle informazioni disponibili sulle prestazioni del sistema informativo aziendale
- il numero di azioni di miglioramento indotte dall'attività di monitoraggio
- la percentuale di processi critici monitorati





OBIETTIVI DI CONTROLLO

ME1 Monitorare e valutare le prestazioni dell'IT

ME1.1 Approccio al monitoraggio

Definire un quadro di riferimento e un approccio generale al monitoraggio, che stabilisca l'ambito, la metodologia e il processo da seguire per monitorare il contributo dell'IT ai risultati aziendali, alla erogazione di servizi e soluzioni. Integrare il quadro di riferimento con il sistema aziendale di misurazione delle prestazioni.

ME1.2 Definizione e raccolta di dati per il monitoraggio

Di concerto con le altre funzioni aziendali, definire un insieme bilanciato di obiettivi e farlo approvare dalle funzioni aziendali non-IT e dai principali stakeholder.

Definire dei benchmark con cui confrontare gli obiettivi e identificare i dati disponibili per essere raccolti ed elaborati per misurare il raggiungimento degli obiettivi stessi.

Definire i processi di misurazione in modo da poter raccogliere tempestivamente e accuratamente i dati per riferire sui progressi conseguiti rispetto agli obiettivi.

ME1.3 Metodo di monitoraggio

Identificare e tradurre operativamente un metodo di monitoraggio delle prestazioni (es. cruscotto aziendale o balanced scorecard) per registrare i risultati raggiunti e le misure effettuate, per fornire una sintetica vista complessiva delle prestazioni IT; il metodo deve essere in sintonia con il sistema di monitoraggio aziendale.

ME1.4 Valutazione delle prestazioni

Revisionare periodicamente le prestazioni rispetto agli obiettivi, effettuare un'analisi delle cause di ogni scostamento e avviare azioni correttive per rimuovere le cause stesse. Ogniqualvolta richiesto, effettuare un'analisi delle cause sulla base degli scostamenti.

ME1.5 Reporting ai vertici aziendali e al consiglio di amministrazione

Fornire analisi ai vertici aziendali per consentire loro di effettuare una valutazione del contributo dell'IT al perseguimento degli obiettivi aziendali, in particolare per quanto riguarda le prestazioni dei servizi/prodotti offerti dall'azienda, le iniziative di investimento facilitate dall'IT, i livelli di efficacia delle singole iniziative per l'erogazione del servizio e delle soluzioni.

Inserire nelle analisi il grado di raggiungimento degli obiettivi pianificati, la quota di utilizzo del budget, gli obiettivi di prestazione raggiunti e i rischi mitigati. Anticipare la verifica della Direzione suggerendo le azioni correttive che riducano i principali scostamenti. Fornire il reporting alla Direzione, sollecitare un feedback dalla valutazione dei responsabili.

ME1.6 Azioni correttive

Identificare e avviare azioni correttive basate sul monitoraggio, sulle valutazioni e sui report riguardanti le prestazioni. Questo comprende il follow-up di tutti i monitoraggi, di tutte le valutazioni e di tutte le analisi, attraverso:

- la verifica, la negoziazione e la conferma delle risposte del management
- l'assegnazione delle responsabilità per le azioni correttive
- la tracciatura dei risultati delle azioni per cui il management si è impegnato.

LINEE GUIDA PER LA GESTIONE

ME1 Monitorare e valutare le prestazioni dell'IT

Da	Inputs
PO5	Analisi dei costi e dei benefici
PO10	Valutazione delle prestazioni dei progetti
AI6	Report sullo stato delle richieste di modifica
DS1-13	Analisi delle prestazioni dei processi
DS3	Piano delle performance e delle prestazioni (requsiti)
DS8	Analisi della soddisfazione degli utenti
ME2	Valutazione sull'efficacia dei controlli IT
ME3	Valutazione della conformità ai requisiti di legge e delle norme interne per le attività IT
ME4	Valutazione dello stato della governance del sistema informativo aziendale

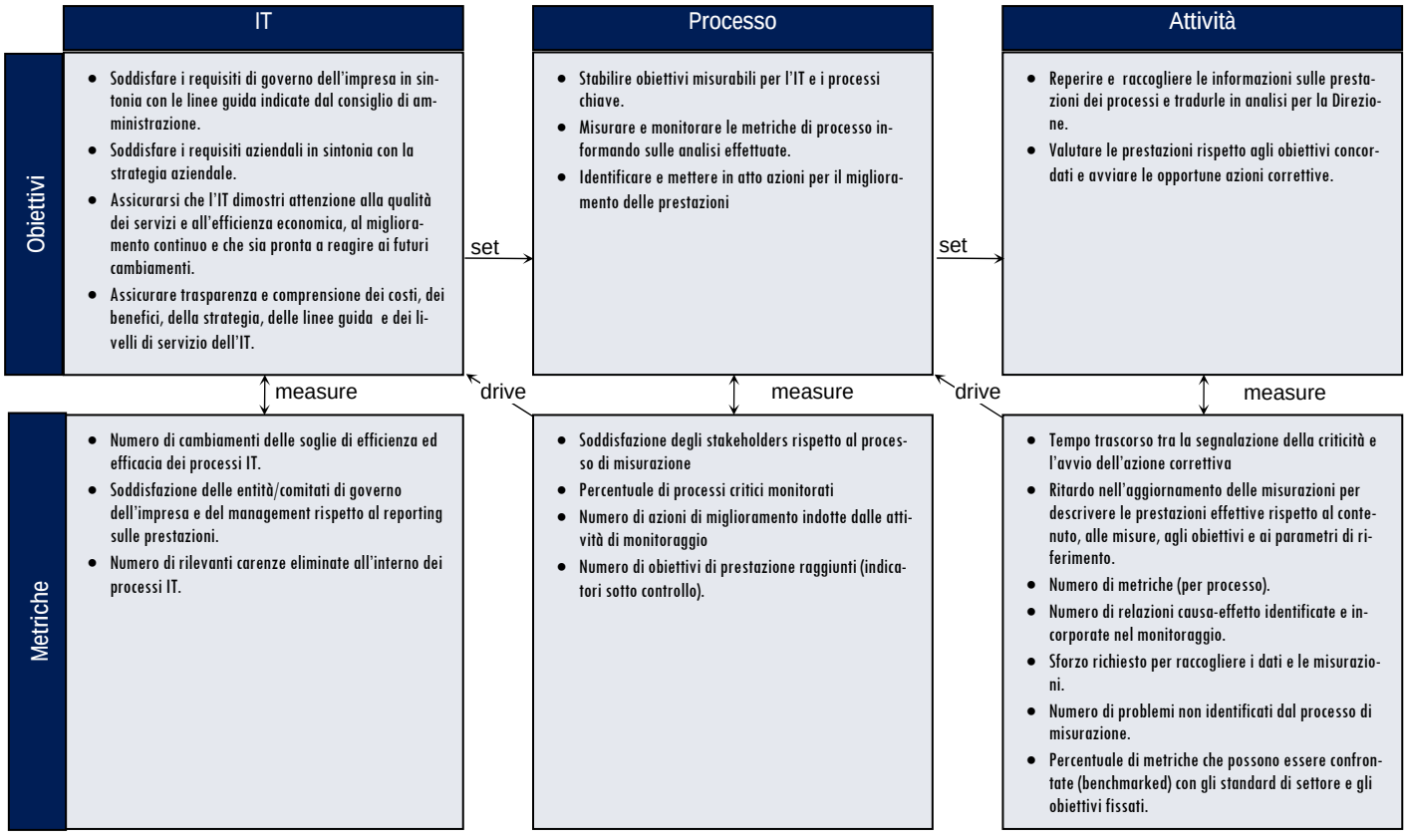
Outputs	a						
Input alla pianificazione IT relativamente alle prestazioni	PO1	PO2	DS1				
Piani delle azioni correttive	PO4	PO8					
Eventi e serie storiche relativi ai rischi	PO9						
Analisi delle prestazioni dei processi	ME2						

RACI Chart

Ruoli

Attività	Consiglio d'amministrazione	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utenza IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architetture IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Conformità, audit, rischio e sicurezza
Definire l'approccio al monitoraggio		A	R	C	R	I	C	I	C	I		C
Identificare e raccogliere dati relativi a obiettivi misurabili che supportano gli obiettivi aziendali		C	C	C	A	R	R		R			
Creare cruscotti aziendali (scorecards)					A		R	C	R	C		
Misurare le prestazioni			I	I	A	R	R	C	R	C		
Analizzare le prestazioni	I	I	I	R	A	R	R	C	R	C		I
Identificare e monitorare le azioni di miglioramento delle prestazioni					A	R	R	C	R	C		C

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

ME1 Monitorare e valutare le prestazioni dell'IT

Il grado di strutturazione del processo *Monitorare e valutare le prestazioni dell'IT* che soddisfa i requisiti aziendali per l'IT di *trasparenza e comprensione dei costi IT, dei benefici attesi, della strategia, delle politiche e dei livelli di servizio secondo quanto stabilito dai requisiti di governance aziendale* è:

0 Non esistente quando

L'organizzazione non dispone di processi di monitoraggio. L'IT non effettua autonomamente il monitoraggio di progetti e processi. Non sono disponibili informazioni utili, tempestive e accurate. Non è riconosciuta la necessità di obiettivi di processo definiti chiaramente.

1 Iniziale / ad hoc quando

La Direzione riconosce la necessità di raccogliere e valutare informazioni sul monitoraggio dei processi. Non sono stati identificati processi standard di raccolta e valutazione. Il monitoraggio è implementato e le metriche sono scelte caso per caso, in funzione delle necessità di specifici progetti e processi IT. Il monitoraggio è di norma attivato in reazione ad un incidente che ha causato una qualche perdita o imbarazzo all'Azienda. L'amministrazione svolge un monitoraggio delle misure economico - finanziare di base per l'IT.

2 Ripetibile ma intuitivo quando

Sono stati identificati gli indicatori di base da monitorare. Esistono metodi e tecniche di raccolta e verifica, ma tali processi non sono stati adottati in tutta l'Azienda. L'analisi e l'interpretazione dei risultati dell'attività di monitoraggio si basano sulla competenza di individui chiave. Vengono identificati ed implementati strumenti limitati per la raccolta di informazioni, ma la raccolta delle informazioni non prevede un approccio strutturato.

3 Definito quando

La Direzione ha comunicato ed istituzionalizzato processi standard di monitoraggio. Sono stati attivati programmi di istruzione e formazione per il monitoraggio. È stata sviluppata una base di dati strutturata di informazioni sulle prestazioni storiche. Le valutazioni si riferiscono ancora a singoli processi o progetti IT e non esiste una visione complessiva e integrata di tutti i processi. Sono stati definiti strumenti per il monitoraggio dei processi IT interni e per la misurazione dei livelli di servizio. Sono state definite metriche per la misurazione del contributo della funzione Sistemi Informativi alle prestazioni dell'Azienda, utilizzando criteri tradizionali di tipo sia economico - finanziario sia operativo. Sono state definite misurazioni delle prestazioni specifiche dell'IT, misurazioni non di tipo economico - finanziario, misurazioni dell'impatto strategico dell'IT, misurazioni della soddisfazione dei clienti e i livelli di servizio. È stato definito un modello per la misurazione delle prestazioni.

4 Gestito e misurabile quando

La Direzione ha definito i limiti di tolleranza entro i quali devono operare i processi. Si sta standardizzando e normalizzando il reporting sui risultati del monitoraggio. Sono state integrate le metriche fra tutti i progetti e processi IT. I sistemi di monitoraggio aziendali per l'informativa della Direzione IT sono formalizzati. In tutta l'Azienda sono stati attivati e integrati strumenti automatizzati per raccogliere e monitorare informazioni operative sul portafoglio delle applicazioni, sui sistemi e sui processi IT. La Direzione è in grado di valutare le prestazioni sulla base di criteri concordati e approvati dagli stakeholder. Le misure della funzione IT sono allineate con gli obiettivi aziendali.

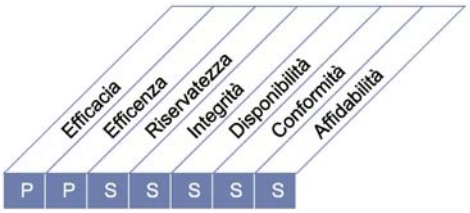
5 Ottimizzato quando

È stato sviluppato un processo di miglioramento continuo della qualità per aggiornare gli standard e le politiche di monitoraggio dell'intera organizzazione al fine di incorporare le migliori pratiche di settore. Tutti i processi di monitoraggio sono ottimizzati e supportano gli obiettivi dell'intera Azienda. Le metriche derivate dal core business sono usate correntemente per misurare le prestazioni e sono integrate in un quadro di riferimento per il monitoraggio strategico quale, ad esempio, l'IT Balanced Scorecard. Il monitoraggio e la continua riprogettazione dei processi sono coerenti con i piani di miglioramento dei processi di business dell'intera Azienda. Il confronto con il mercato e con i concorrenti di riferimento è effettuato con modalità formalizzate e con criteri di comparazione ben compresi.

DESCRIZIONE DEL PROCESSO

ME2 Monitorare e valutare i controlli interni

La realizzazione di un efficace programma di controllo interno per l'IT richiede un processo di monitoraggio ben definito. Tale processo riguarda il monitoraggio e l'informativa sulle eccezioni ai controlli, sui risultati delle autovalutazioni, sulle verifiche di terze parti. Un importante beneficio prodotto dal monitoraggio dei controlli interni è costituito dalla garanzia (assurance) riguardo l'efficienza e l'efficacia delle operazioni e la conformità a leggi e regolamenti.



Il controllo del processo IT

Monitorare e valutare i controlli interni

che soddisfa i requisiti aziendali per l'IT di

tutelare il raggiungimento degli obiettivi IT ed essere conformi alle leggi, ai regolamenti relativi all'IT ed ai contratti in essere

ponendo l'attenzione su

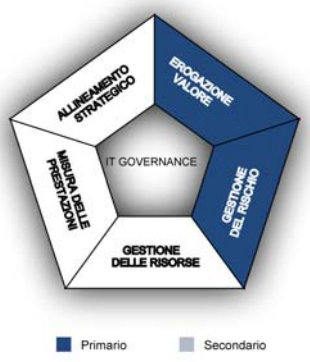
l'attività di verifica dei processi di controllo interno per le attività relative all'IT e sull'individuazione delle azioni di miglioramento

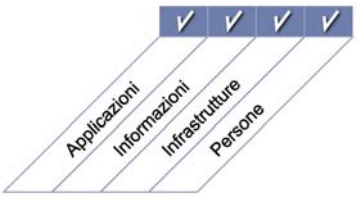
è ottenuto tramite

- la definizione di un sistema di controllo interno inserito nella struttura dei processi IT
- il monitoraggio e le segnalazioni sull'efficacia dei controlli interni IT
- il reporting alla Direzione sulle eccezioni ai controlli per consentire l'avvio delle azioni correttive

e viene misurato tramite

- numero di violazioni significative ai controlli
- numero di iniziative di miglioramento dei controlli
- numero e copertura delle iniziative di autovalutazione dei controlli





OBIETTIVI DI CONTROLLO

ME2 Monitorare e valutare i controlli interni

ME2.1 Valutazione del modello del sistema di controllo interno

Monitorare in modo continuo, effettuare benchmark e migliorare il sistema di controllo interno IT e il modello dei controlli per facilitare il raggiungimento degli obiettivi aziendali.

ME2.2 Controlli di secondo livello

Monitorare e valutare l'efficacia e l'efficienza della verifica, da parte della direzione IT, sui controlli interni.

ME2.3 Eccezioni ai controlli

Registrare le informazioni riguardanti tutte le eccezioni ai controlli e assicurarsi che sia svolta un'analisi delle cause sottostanti. Le eccezioni debbono essere riportate ai livelli organizzativi superiori ove necessario e ove opportuno ai diversi stakeholder. Avviare le necessarie azioni correttive.

ME2.4 Attività di controllo promosse autonomamente (Self – assessment)

Valutare la completezza e l'efficacia dei controlli interni sui processi, sulle procedure e sui contratti dell'IT attraverso un programma continuo di autovalutazione.

ME2.5 Garanzie (Assurance) sui controlli interni

Ottenere, quando necessario, ulteriori garanzie (assurance) sulla completezza e sull'efficacia dei controlli interni attraverso verifiche svolte da terzi.

ME2.6 Controllo interno presso terze parti

Valutare lo stato del sistema di controllo interno di ogni terza parte fornitrice di servizi. Assicurarsi che il fornitore di servizi esterno sia conforme alle leggi e ai regolamenti e alle obbligazioni contrattuali.

ME2.7 Azioni correttive

Identificare, avviare e monitorare azioni correttive basate sulle analisi e valutazioni dei controlli.

LINEE GUIDA PER LA GESTIONE

ME2 Monitorare e valutare i controlli interni

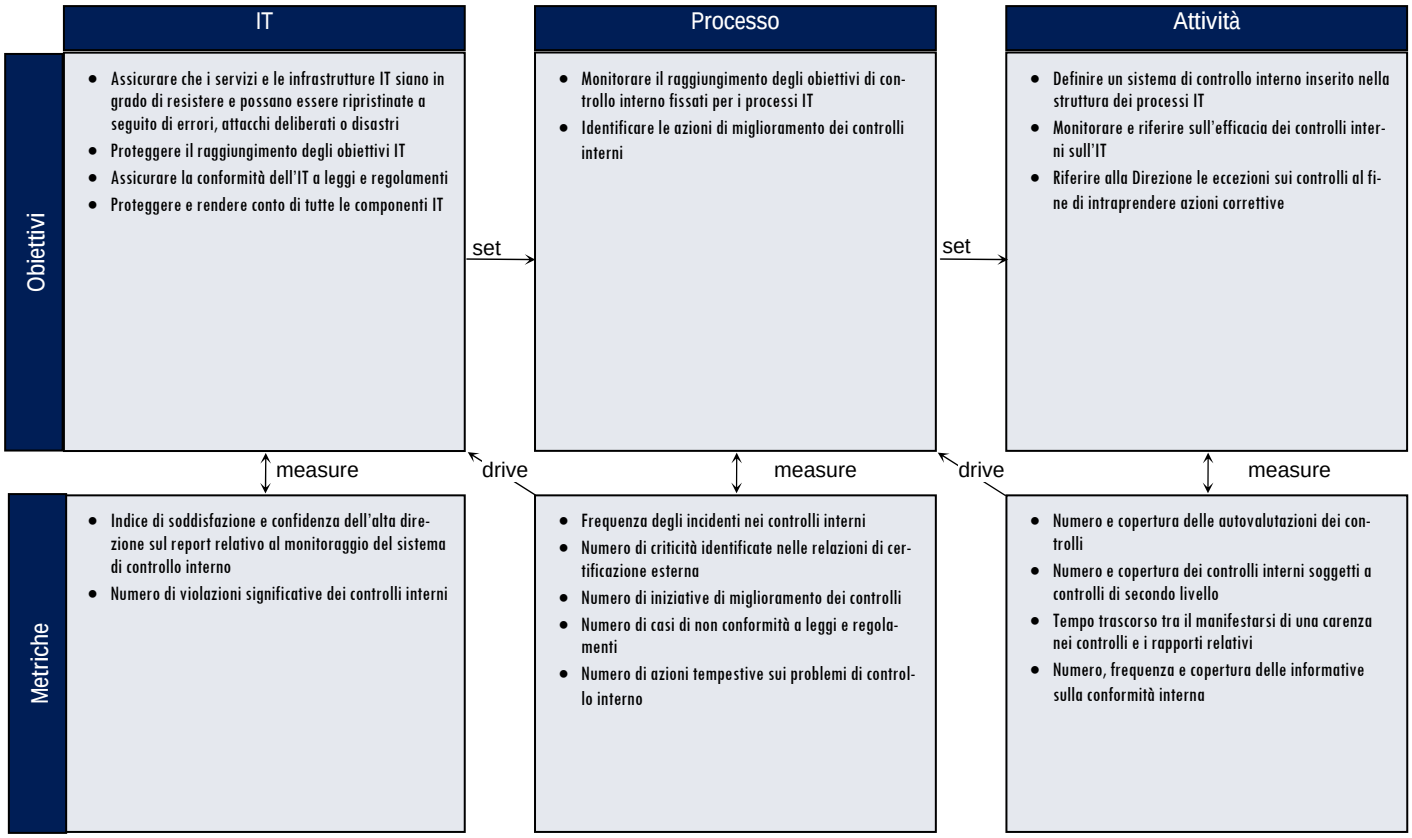
Da	Inputs
ME1	Analisi delle prestazioni dei processi
AI7	Monitoraggio dei controlli interni

Outputs	a						
Informativa sull'efficacia dei controlli IT	PO4	PO6	ME1	ME4			

RACI Chart

Attività	Consiglio d'amministrazione	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architetture IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Conformità, audit, rischio e sicurezza
Monitare e controllare le attività di controllo interno sull'IT					A		R		R	R		R
Monitorare il processo di autovalutazione				I	A		R		R	R		C
Monitorare le prestazioni di verifiche indipendenti, audit e ispezioni				I	A		R		R	R		C
Monitorare il processo per ottenere garanzia sui controlli operati da terze parti		I	I	I	A		R		R	R		C
Monitorare il processo per identificare e valutare le eccezioni ai controlli		I	I	I	A	I	R		R	R		C
Monitorare il processo per identificare e correggere le eccezioni ai controlli		I	I	I	A	I	R		R	R		C
Riferire alle parti interessate (key stakeholders)	I	I	I		A/R							I

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

ME2 Monitorare e valutare i controlli interni

Il grado di strutturazione del processo *Monitorare e valutare i controlli interni* che soddisfa i requisiti aziendali per l'IT di *tutelare il raggiungimento degli obiettivi IT ed essere conformi alle leggi, ai regolamenti relativi all'IT ed ai contratti in essere* è:

0 Non esistente quando

L'Azienda non dispone di procedure per monitorare l'efficacia dei controlli interni. Non vi sono metodi per riportare al management sul controllo interno. C'è una generalizzata mancanza di consapevolezza sugli aspetti di sicurezza delle attività IT e sull'esigenza di garanzia dell'operatività del controllo interno. La Direzione e il personale hanno una generale mancanza di consapevolezza del sistema dei controlli interni

1 Iniziale / ad hoc quando

La Direzione riconosce il bisogno di una garanzia in merito alla corretta gestione e al controllo dell'IT. Sono utilizzate competenze individuali per la valutazione caso per caso dell'adeguatezza del controllo interno. La Direzione IT non ha assegnato formalmente la responsabilità del monitoraggio dell'efficacia dei controlli interni. La valutazione dei controlli interni IT è realizzata come parte degli audit contabili, con metodologie e competenze che non riflettono le necessità della funzione IT.

2 Ripetibile ma intuitivo quando

L'Azienda utilizza relazioni informali sui controlli interni per attivare azioni correttive. La valutazione del sistema di controllo interno è dipendente dalle competenze di individui chiave. L'Azienda ha un'accresciuta consapevolezza sul monitoraggio del controllo interno. La Direzione dei Sistemi Informativi monitora su base regolare l'efficacia di quelli che ritiene siano i controlli interni critici. Metodologie e strumenti per il monitoraggio dei controlli interni iniziano ad essere usati ma non sulla base di un piano. I fattori di rischio specifici per l'ambiente IT sono identificati sulla base delle competenze degli individui.

3 Definito quando

La Direzione sostiene ed ha istituzionalizzato il monitoraggio del controllo interno. Sono state sviluppate politiche e procedure per la preparazione e la valutazione di rapporti sulle attività di monitoraggio dei controlli interni. È stato definito un programma di formazione per il monitoraggio del controllo interno. È stato definito un processo di autovalutazione e di verifiche di certificazione dei controlli interni, con ruoli per i manager aziendali e per i manager dell'IT. Si stanno utilizzando strumenti per la misurazione e per la valutazione dei controlli interni, ma essi non sono necessariamente integrati in tutti i processi. Sono utilizzate politiche per la valutazione dei rischi nell'ambito di un quadro di riferimento sviluppato specificamente per il controllo interno dell'IT. Sono definiti rischi specifici di processo e le relative azioni di mitigazione/riduzione del rischio.

4 Gestito e misurabile quando

La Direzione ha realizzato una struttura per il monitoraggio dei controlli interni IT. L'azienda ha stabilito le soglie di tolleranza per il processo di monitoraggio del controllo interno. Sono stati implementati strumenti per standardizzare le valutazioni e per rilevare automaticamente le eccezioni ai controlli. È stata attivata una funzione formalmente definita per la gestione del controllo interno sull'IT, dotata di personale specializzato e certificato e che utilizza un quadro di riferimento di controllo formalizzato ed approvato dall'Alta Direzione. Personale IT competente partecipa regolarmente alle verifiche sui controlli interni. È stata realizzata una base di conoscenza storica di metriche sul monitoraggio del controllo interno. Sono state avviate attività di riesame fra pari grado per il monitoraggio del controllo interno.

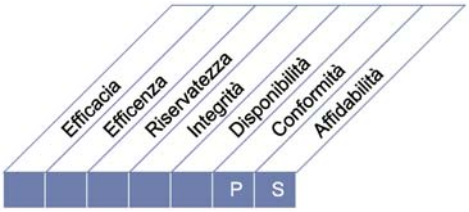
5 Ottimizzato quando

La Direzione ha stabilito un programma di miglioramento continuo per l'intera organizzazione, che prende in considerazione le esperienze maturate e le migliori prassi di settore per il monitoraggio del controllo interno. L'azienda utilizza strumenti integrati e aggiornati che, quando opportuno, permettono un efficace valutazione dei controlli IT critici e una rapida rilevazione degli incidenti nel monitoraggio dei controlli IT. La condivisione delle conoscenze, in particolare per la funzione Sistemi Informativi, è formalmente implementata. È formalizzato lo sviluppo di analisi comparative con gli standard di settore e con le pratiche di riferimento.

DESCRIZIONE DEL PROCESSO

ME3 Assicurare la conformità ai requisiti esterni

Un'efficace supervisione del rispetto dei regolamenti richiede la definizione di un processo di valutazione per assicurare la conformità ai requisiti di legge, di norme e di contratti. Tale processo include l'identificazione dei requisiti di conformità, l'ottimizzazione e valutazione dei risultati, l'assicurazione che i requisiti di conformità sono stati effettivamente soddisfatti, in fine, l'integrazione del reporting relativo alla conformità di competenza dell'IT nell'ambito del reporting di conformità aziendale.



Il controllo del processo IT

Assicurare la conformità a requisiti esterni

che soddisfa i requisiti aziendali per l'IT di

assicurare la conformità a leggi, regolamenti ed a requisiti contrattuali

ponendo l'attenzione su

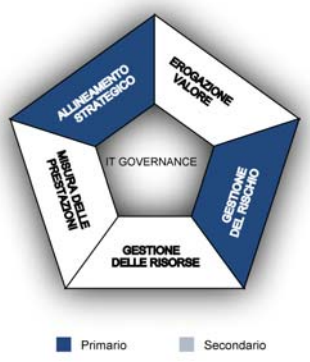
l'identificazione di tutte le leggi, regolamenti e requisiti contrattuali applicabili, sulla definizione del corrispondente livello di conformità richiesto all'IT ed infine sull'ottimizzazione dei processi IT per ridurre il rischio di non conformità

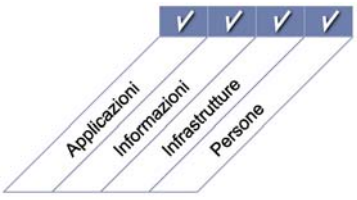
è ottenuto tramite

- l'identificazione dei requisiti legali, normativi e contrattuali relativi all'IT
- la valutazione dell'impatto dei requisiti legali e normativi
- il monitoraggio e il reporting sulla conformità a questi requisiti

e viene misurato tramite

- Costo della non conformità dell'IT, inclusi pagamenti e multe
- Tempo medio trascorso tra l'identificazione di problemi di conformità con norme esterne e la loro risoluzione
- Frequenza delle verifiche di conformità a leggi e regolamenti esterni





OBIETTIVI DI CONTROLLO

ME3 Assicurare la conformità ai requisiti esterni

ME3.1 Identificazione dei requisiti esterni di compliance relativi a leggi, normative e contratti.

Identificare, in modo sistematico, leggi nazionali ed internazionali, normative ed altri requisiti - di natura esogena rispetto all'azienda – che l'azienda deve rispettare, al fine di farli integrare nelle politiche, negli standard, nelle procedure e nelle metodologie specifici dell'IT.

ME3.2 Ottimizzazione della gestione dei requisiti normativi

Rivedere e adeguare le politiche, gli standard, le procedure ed i metodi IT per assicurare che i requisiti di legge, normativi e contrattuali siano efficientemente soddisfatti e conosciuti. .

ME3.3 Valutazione del rispetto dei requisiti esterni

Confermare che le politiche, gli standard, le procedure e i metodi IT rispettano i requisiti normativi e di legge.

ME3.4 Garanzia di conformità

Ottenere e riferire sulla garanzia di conformità con e rispetto di tutte le politiche interne che derivano dall'applicazione di direttive interne o di leggi e normative esterne o di contratti; confermare che i proprietari dei processi interessati abbiano adottato le opportune azioni correttive per superare eventuali lacune di conformità.

ME3.5 Reporting integrato

Integrare, con analoghe informative provenienti da altre funzioni aziendali, il reporting dell'IT riguardante la conformità a requisiti di legge, normativi e contrattuali.

LINEE GUIDA PER LA GESTIONE

ME3 Assicurare la conformità ai requisiti esterni

Da	Inputs
*	Requisiti legali e normativi di conformità
PO6	Politiche IT

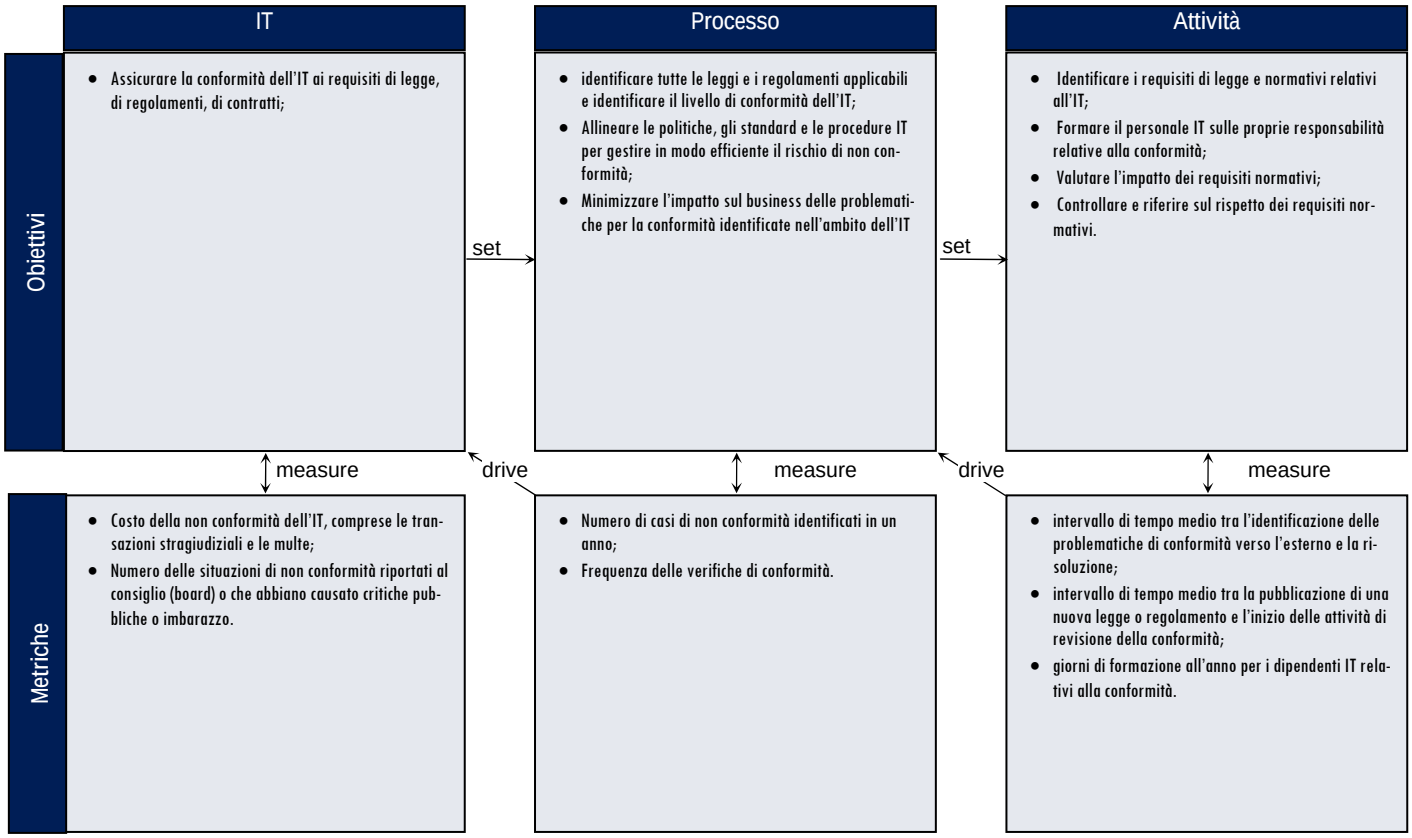
Outputs	a						
Elenco (catalogue) dei requisiti di legge e normativi che si riferiscono alla fornitura di servizi IT	PO4	ME4					
Valutazione della conformità IT ai requisiti legali e normativi delle attività aziendali	ME1						

RACI Chart

Ruoli

Attività	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architetture IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Conformità, audit, rischio e sicurezza	Consiglio d'amministrazione
definire e realizzare un processo per identificare i requisisti di legge, contrattuali, di policy e normativi				A/R	C	I	I	I	C	I	R	
valutare la conformità delle attività IT con le politiche , gli standard e le procedure IT	I	I	I	A/R	I	R	R	R	R	R	R	I
riferire in merito alla garanzia di conformità delle attività IT con le politiche, gli standard e le procedure IT				A/R	C	C	C	C	C	C	R	
definire le azioni (input) per allineare le politiche, le procedure e gli standard IT ai requisiti di conformità				A/R	C	C	C	C	C		R	
integrare il reporting sull'IT sui requisiti normativi con output analoghi delle altre funzioni di business				A/R		I	I	I	R	I	R	

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

ME3 Assicurare la conformità ai requisiti esterni

Il grado di strutturazione del processo *assicurare la conformità ai requisiti esterni* che soddisfa i requisiti aziendali per l'IT di *assicurare la conformità a leggi, regolamenti ed a requisiti contrattuali* è:

0 Non esistente quando

C'è poca consapevolezza dei requisiti esterni che influiscono sull'ambito IT, non c'è un processo riguardante la conformità con normative, con reuisiti di natura legale o contrattuale.

1 Iniziale / ad hoc quando

Si è consapevoli dell'impatto che hanno sull'azienda le norme, i contratti o la legislazione. Vengono adottate procedure informali per garantire la compliance, ma solo a seguito di un'esigenza emersa in un nuovo progetto o come reazione ad una verifica o ad una ispezione.

2 Ripetibile ma intuitivo quando

E' compresa la necessità di rispettare le regole esterne e tale esigenza è comunicata. Ogniqualvolta la compliance diventa un obbligo ricorrente, come nel caso di normative del settore finanziario o della legislazione sulla privacy, sono sviluppate procedure particolari, applicate con cadenza annuale. Tuttavia non esiste un approccio standard. Si fa molto affidamento sull'esperienza e sulla responsabilità dei singoli individui, e di conseguenza sono possibili errori. La formazione sui regolamenti esterni e su quanto concerne il loro rispetto è fatta in modo informale.

3 Definito quando

Politiche, procedure e piani che garantiscono il rispetto di norme, leggi e contratti sono stati sviluppati, documentati e comunicati ma non sempre vengono rispettati ed in alcuni casi possono essere superati o di difficile applicazione. Il controllo è limitato e non tutte le esigenze di adeguamento sono state prese in considerazione. La formazione viene fornita per quanto riguarda i requisiti legali e normativi che interessano l'organizzazione ed i processi di compliance definiti. Per ridurre i rischi relativi alle responsabilità contrattuali sono disponibili fac-simili di contratti e di procedure legali.

4 Gestito e misurabile quando

I problemi e i rischi connessi al rispetto di requisiti legali esterni e l'esigenza di garantirne l'osservanza a tutti i livelli sono fortemente compresi. Un piano di formazione è definito per garantire che tutto il personale conosca le regole da rispettare. Le responsabilità sono chiare e note, in particolare è assegnata la responsabilità di ciascun processo. Il processo di compliance include un'analisi della situazione attuale per identificare le regole da rispettare e via via i cambiamenti da apportare. Esiste un meccanismo per controllare il non rispetto delle regole esterne, per garantire l'applicazione delle procedure interne e per adottare azioni correttive. I problemi di non rispetto delle regole sono analizzati in modo standard per ricercarne le cause, con l'obiettivo di individuare le soluzioni sostenibili. Prassi operative interne standard, vengono utilizzate per esigenze specifiche quali ad esempio le disposizioni permanenti e i contratti di servizio ricorrenti.

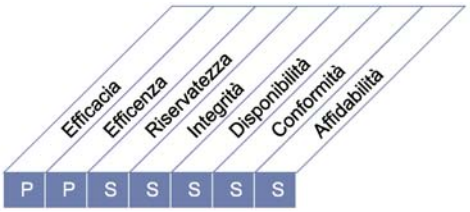
5 Ottimizzato quando

Esiste un processo ben organizzato, efficiente e rispettato di conformità alle regole esterne, basato su una singola funzione centrale che fornisce guida e coordinamento a tutta l'azienda. C'è una conoscenza approfondita delle norme da applicare, delle relative future evoluzioni, delle modifiche prevedibili e dell'esigenza di nuove soluzioni. Per capire ed influenzare la definizione delle normative esterne che possono interessarla, l'azienda partecipa ad iniziative di natura normativa promosse dalle autorità. Sono state sviluppate regole interne per garantire una efficiente conformità con le normative esterne, tali regole hanno ridotto al minimo i casi di non rispetto delle norme. Esiste un sistema centrale di registrazione valido per tutta l'azienda, tale funzione consente alla direzione di documentare i flussi operativi e di misurare e migliorare la qualità e l'efficacia del processo di supervisione della compliance. Viene utilizzato ed affinato, a livello di regola interna, un processo di auto-valutazione relativo ai requisiti normativi esterni. Lo stile e la cultura dei responsabili aziendali riguardo al rispetto delle regole esterne sono sufficientemente forti, il processo è ben definito in modo tale da consentire che l'addestramento sia limitato al nuovo personale o al verificarsi di cambiamenti significativi.

DESCRIZIONE DEL PROCESSO

ME4 Istituire l'IT Governance

Istituire un'efficace struttura per la governance compresa la definizione delle strutture organizzative, dei processi, della leadership, dei ruoli e delle responsabilità, al fine di garantire che gli investimenti dell'impresa in tecnologie informatiche siano allineati ed erogati in accordo con le strategie e con gli obiettivi aziendali.



Il controllo del processo IT

Istituire l'IT Governance

che soddisfa i requisiti aziendali per l'IT di

integrare l'IT governance con gli obiettivi di corporate governante e di conformità con leggi, regolamenti e contratti

ponendo l'attenzione su

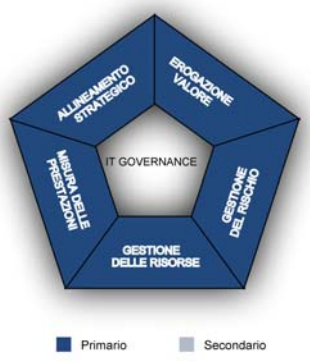
l'attività di redazione di reportistica indirizzata al board in merito a strategie, prestazioni e rischi legati all'IT, e sull'attività di soddisfacimento dei requisiti di governance coerentemente con le indicazioni del board.

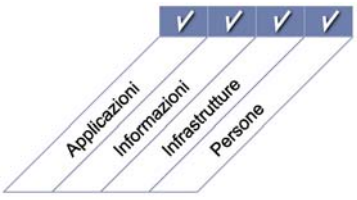
è ottenuto tramite

- l'istituzione di una struttura di IT governance integrata con la corporate governance
- l'ottenimento di una valutazione indipendente sullo stato dell'IT governance

e viene misurato tramite

- frequenza delle comunicazioni indirizzate agli stakeholder in merito alle tematiche IT, anche con riferimento al grado di strutturazione dei processi IT.
- frequenza della reportistica dell'IT al board, anche con riferimento al grado di strutturazione dei processi IT frequenza delle verifiche indipendenti in merito alla conformità dei processi IT





OBIETTIVI DI CONTROLLO

ME4 Istituire l'IT Governance

ME4.1 Istituzione di un quadro di riferimento per l'IT Governance

Definire, realizzare un quadro di riferimento per la governance dell'IT e mantenerlo allineato con il contesto stabilito per la governante ed il controllo dell'intera azienda. Il quadro di riferimento dovrebbe essere basato su un adeguato modello di controllo e dei processi IT e indicare responsabilità non ambigue e procedure che consentano di prevenire errori nell'ambito di attività di controllo e di supervisione. Confermare che il quadro di riferimento per la governance dell'IT è funzionale a garantire la conformità con la legislazione e le normative, l'allineamento alle strategie aziendali ed il perseguimento degli obiettivi aziendali. Definire un sistema di reporting che relazioni sullo stato e sulle problematiche dell'IT Governance.

ME4.2 Allineamento strategico

Facilitare la comprensione da parte del Consiglio di Amministrazione e dell'Alta Direzione delle problematiche strategiche dell'IT, come il ruolo dell'IT, le caratteristiche e le potenzialità delle tecnologie informatiche in azienda. Assicurarsi che il potenziale contributo dell'IT alla strategia aziendale sia compreso sia dall'azienda sia dalla funzione sistemi informativi. Collaborare con il Consiglio di Amministrazione al fine di definire ed implementare organismi di controllo, come il Comitato Strategico per l'IT, con l'obiettivo di fornire un orientamento strategico al management che si deve relazionare con l'IT, in modo da assicurare che strategia ed obiettivi siano diffusi all'interno delle unità operative sia di business sia delle singole funzioni IT, e che tra utenti aziendali e specialisti della funzione sistemi informativi si sviluppi un rapporto di fiducia reciproca. Facilitare l'allineamento dell'IT all'azienda per quanto riguarda strategia e processi operativi, incoraggiando la condivisione di responsabilità fra process owner e l'IT al fine di pervenire a decisioni strategiche e produrre valore a fronte di investimenti in tecnologie informatiche.

ME4.3 Apporto di valore

Gestire i programmi di investimento dove l'IT è fattore abilitante e di altre risorse e servizi IT in modo che possano apportare il maggiore valore possibile nel perseguimento della strategia e degli obiettivi dell'impresa. Assicurarsi che i risultati degli investimenti IT attesi dall'azienda e che tutti gli sforzi necessari per ottenerli vengano compresi, che siano prodotti e approvati dagli stakeholder degli studi di fattibilità significativi e coerenti, che le risorse e gli investimenti siano controllati durante tutto il loro ciclo di vita economico e che ci sia una gestione finalizzata alla realizzazione dei benefici, come il contributo a nuovi servizi, guadagni in efficienza e una maggiore capacità di risposta alla domanda del cliente. Assicurare una gestione puntuale a livello di portafoglio, di programmi e di progetti, incoraggiando l'assunzione di risponsabilità da parte delle strutture e dei processi di business sugli investimenti favoriti dall'IT e che la funzione sistemi informativi garantisca un efficiente ed efficace supporto.

ME4.4 Gestione delle risorse

Supervisionare gli investimenti, l'utilizzo e l'allocazione delle risorse IT attraverso una attività di verifica sistematica delle iniziative e delle operations IT assicurandosi che la funzione sistemi informativi disponga di una quantità sufficiente di risorse competenti e allineate con gli attuali e futuri obiettivi strategici ed esigenze irrinunciabili dell'azienda.

ME4.5 Gestione del rischio

Collaborare con il Consiglio di Amministrazione al fine di definire la propensione al rischio IT dell'impresa; ottenere una ragionevole garanzia che le modalità di gestione del rischio informatico sono appropriate e che il rischio informatico attuale non supera il livello stabilito dal Consiglio. Incorporare le responsabilità di gestione del rischio nell'organizzazione, assicurando che l'azienda e l'IT valutino e comunichino in maniera sistematica i rischi correlati all'IT ed il loro impatto sui processi di business. La posizione assunta dall'azienda nei confronti del rischio IT dovrebbe essere trasparente e nota a tutti gli stakeholder.

ME4.6 Valutazione delle prestazioni

Confermare che gli obiettivi IT sui quali si è raggiunto un accordo sono stati raggiunti o superati, o che i miglioramenti nel perseguimento degli obiettivi IT è coerente con le aspettative. Ove gli obiettivi non siano stati raggiunti o le aspettative siano state insoddisfatte, verificare gli interventi risolutivi adottati dalla Direzione. verso Fornire al Consiglio informazioni dettagliate sugli aspetti più importanti legati al portafoglio delle iniziative che riguardano l'IT, ai programmi e alle prestazioni dei processi IT, attraverso dei report che mettano in condizione la Direzione di verificare i progressi dell'azienda verso gli obiettivi definiti.

ME4.7 Certificazione indipendente

Ottenere una certificazione indipendente (interna o esterna) relativamente alla conformità dell'IT con la legislazione ele normative vigenti; con le politiche, gli standard e le procedure dell'azienda, con le pratiche generalmente accettate, con l'attesa efficienza ed efficacia delle performance IT.

LINEE GUIDA PER LA GESTIONE

ME4 Istituire l'IT Governance

Da	Inputs
PO4	Quadro di riferimento dei processi IT
PO5	Reporting sul rapporto costi/benefici
PO9	Valutazione del rischio e reporting
ME2	Report sull'efficacia dei controlli IT
ME3	Elenco (catalogue) dei requisiti di legge e normativi che si riferiscono alla fornitura di servizi IT

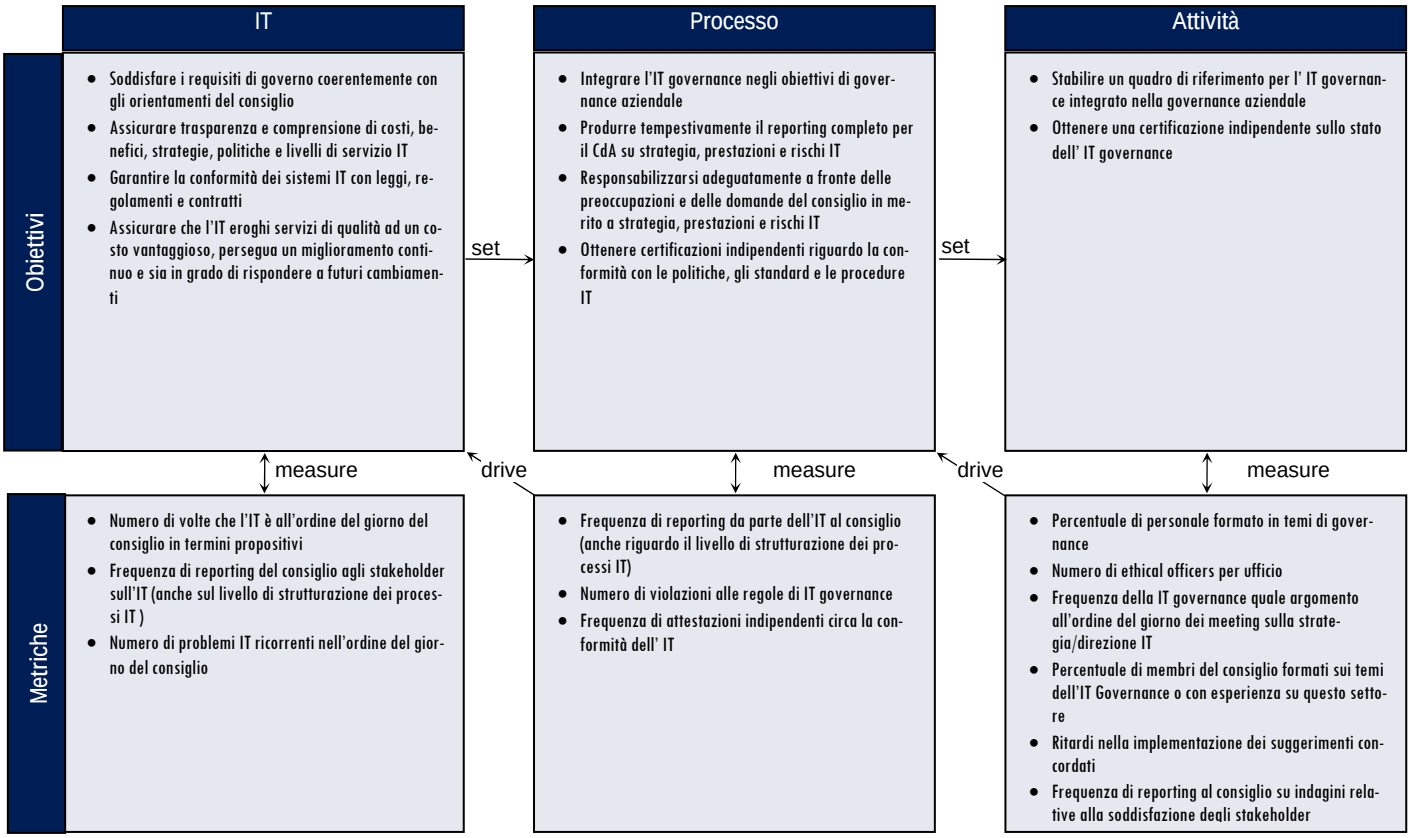
Outputs	a						
Miglioramenti del quadro di riferimento dei processi	PO4						
Valutazione dello stato della governance del sistema informativo aziendale	PO1	ME1					
Benefici attesi dall'azienda relativamente agli investimenti IT	PO5						
Orientamento strategico dell'impresa verso l'IT	PO1						
Propensione ai rischi IT dell'azienda	PO9						

RACI Chart

Ruoli

Attività	Consiglio d'amministrazione	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architetture IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Conformità, audit, rischio e sicurezza
Stabilire la supervisione e la promozione delle attività di IT da parte del Consiglio di Amministrazione e dell'Alta Direzione	A	R	C	C	C							C
Analizzare, approvare, allineare e comunicare le performance, la strategia , la gestione del rischio e delle risorse IT rispetto alla strategia aziendale	A	R	I	I	R							C
Ottenere periodicamente valutazioni indipendenti relativamente alle prestazioni e alla conformità con politiche, standard e procedure	A	R	C	I	C		I	I	I	I	I	R
Risolvere i rilievi individuati dalle valutazioni indipendenti ed assicurare l'implementazione da parte della direzione dei suggerimenti concordati	A	R	C	I	C		I	I	I	I	I	R
Produrre un report sull'IT governance	A	C	C	C	R	C	I	I	I	I	I	C

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

ME4 Istituire l'IT Governance

Il grado di strutturazione del processo *istituire l'IT Governance* che soddisfa i requisiti aziendali per l'IT di *integrare l'IT governance con gli obiettivi di corporate governante e di conformità con leggi, regolamenti e contratti* è:

0 Non esistente quando

C'è una completa mancanza di qualsiasi processo riconoscibile di IT governance. L'azienda non si è ancora resa conto che c'è un problema che deve essere affrontato e di conseguenza non c'è comunicazione riguardo al problema.

1 Iniziale / ad hoc quando

C'è la consapevolezza che le problematiche di IT governance esistono e devono essere considerate. Sono presenti approcci ad hoc attuati su base individuale o su casi specifici. L'approccio della Direzione è di tipo reattivo, esiste solo una comunicazione sporadica e non coerente sui problemi e sugli approcci necessari per affrontarli. La Direzione riceve soltanto indicazioni approssimative circa il contributo fornito dall'IT alla performance aziendale. Il management affronta e risolve gli incidenti che hanno causato qualche perdita o problemi di immagine all'azienda solo con un approccio reattivo.

2 Ripetibile ma intuitivo quando

Esiste consapevolezza in merito alle problematiche legate al governo dell'IT. Le attività di IT governance, e gli indicatori di prestazione, fra cui la pianificazione, l'erogazione e i processi di monitoraggio dell'IT sono in fase di sviluppo. L'identificazione dei processi IT da migliorare è effettuata sulla base di decisioni individuali. La Direzione ha identificato metodi e tecniche di valutazione elementari; il processo non è tuttavia ancora stato applicato all'intera azienda. La comunicazione degli standard e delle responsabilità di governo viene lasciata ai singoli, i quali guidano i processi di governance all'interno di vari progetti e processi IT. I processi, gli strumenti e le metriche dell'IT governance sono limitati e possono non essere utilizzati appieno per una mancanza di conoscenza delle loro caratteristiche.

3 Definito quando

L'importanza e la necessità dell'IT governance sono comprese dal management e comunicate all'organizzazione. E' sviluppato un insieme di indicatori di base per l'IT governance, dove i collegamenti fra le misure dei risultati e i parametri delle prestazioni sono definiti e documentati. Le procedure sono standardizzate e documentate. La Direzione ha comunicato le procedure standardizzate e sono definite delle procedure di formazione. Sono identificati gli strumenti per supportare il monitoraggio dell'IT governance. Sono stati sviluppati dei cruscotti, parte integrante delle Balanced Business Scorecard in ambito IT. Tuttavia è lasciato al singolo di dedicarsi alla formazione, seguire gli standard ed applicarli. I processi possono essere monitorati, ma mentre molto viene fatto sulla base dell'iniziativa personale per gestire le deviazioni, queste ultime sono difficilmente identificate dalla Direzione.

4 Gestito e misurabile quando

Esiste consapevolezza delle problematiche legate all'IT governance a tutti i livelli. Il cliente dei servizi forniti dall'IT è chiaramente identificato e le responsabilità sono definite e monitorate tramite accordi sui livelli di servizio. Le responsabilità sono chiaramente definite e la responsabilità del processo è stata attribuita. I processi IT e l'IT governance sono allineati ed integrati con la strategia aziendale e la strategia IT. I miglioramenti dei processi IT sono basati principalmente su di un approccio di natura quantitativa ed è possibile misurare e monitorare la conformità con le procedure e le metriche di processo. Tutti gli stakeholder del processo sono consapevoli dei rischi, dell'importanza dell'IT e delle opportunità che essa è in grado di offrire. La Direzione ha definito i livelli di tolleranza con riferimento ai quali devono essere strutturati i processi. C'è un limitato, principalmente tattico, uso della tecnologia, basato su tecniche mature e strumenti standard consolidati. L'IT governance è stata integrata nella pianificazione operativa e strategica e nei processi di monitoraggio. Gli indicatori di prestazione relativi a tutte le attività di IT Governance sono stati identificati e tracciati consentendo miglioramenti estesi a tutta la realtà aziendale. La responsabilità generale delle prestazioni dei processi chiave è chiara e il management è premiato sulla base delle misure chiave di prestazione.

5 Ottimizzato quando

Esiste una comprensione avanzata ed orientata al futuro delle problematiche di IT Governance e delle relative soluzioni. Addestramento e comunicazione sono supportati da concetti e tecniche di "leading edge". I processi sono stati portati ad un livello coerente con le migliori pratiche di settore sulla base dei risultati di un'attività di miglioramento continuo e di raffronto con altre realtà aziendali in relazione al modello di strutturazione dei processi IT. La realizzazione delle politiche IT ha condotto ad una struttura organizzativa, organico del personale e processi IT che sono rapidi ad adattarsi e a supportare pienamente i requisiti di IT governance. Le cause di tutti i problemi e di tutte le discrepanze sono analizzate e si dà corso ad azioni correttive efficaci. L'IT è usato in modo coerente, integrato ed ottimizzato, tale da automatizzare i flussi di lavoro e fornire strumenti per migliorare qualità ed efficacia. I rischi come i benefici dei processi IT sono definiti, bilanciati e comunicati a tutta l'azienda. Si fa leva su esperti esterni e i benchmark sono usati come riferimento. Il monitoraggio, l'auto-valutazione e la comunicazione delle aspettative di governance pervadono tutta l'azienda e c'è un uso ottimale della tecnologia a supporto di attività di misurazione, analisi, comunicazione e formazione. Il governo dell'impresa ed il governo dell'IT sono collegati strategicamente, facendo leva su tecnologia, risorse umane e finanziarie per aumentare il vantaggio competitivo dell'azienda. Le attività di IT governance sono integrate con i processi di governance dell'impresa.