



Leading the IT Governance Community

COBIT

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™

Maggio 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.

©1996, 1998, 2000, 2005, 2007 IT Governance Institute (ITGI).

All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system, or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise), without the prior written authorization of ITGI.

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

© 1996, 1998, 2000, 2005, 2007 IT Governance Institute (ITGI). Tutti i diritti sono riservati. Nessuna parte di questa pubblicazione può essere usata, copiata, riprodotta, modificata, distribuita, pubblicata con sistemi video, memorizzata su sistemi di pubblicazione, o trasmessa in qualsiasi forma e con qualsiasi mezzo (elettronico, meccanico, di fotocopiatura, di memorizzazione o di altro tipo), senza la preventiva autorizzazione scritta dell’ITGI.

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 appartenenza 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
Leonardo Nobile, CISA
Alberto Piamonte
Marco Salvato, CISM
Giulio Spreafico, CISA, CISM

Federazione Lombarda BCC
Deloitte
Ing. Alberto Piamonte
KPMG
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.



Capitolo di Milano

Pagina intenzionalmente bianca

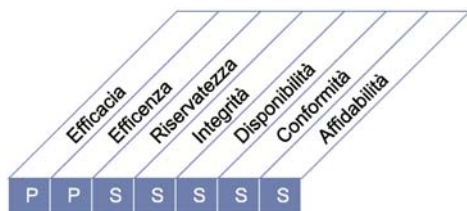
EROGAZIONE ED ASSISTENZA

- DS1** Definire e gestire i livelli di servizio
- DS2** Gestire i servizi di terze parti
- DS3** Gestire le prestazioni e la capacità produttiva
- DS4** Assicurare la continuità di servizio
- DS5** Garantire la sicurezza dei sistemi
- DS6
- DS7
- DS8
- DS9
- DS10
- DS11
- DS12
- DS13

DESCRIZIONE DEL PROCESSO

DS1 Definire e gestire i livelli di servizio

Una comunicazione efficace tra la Direzione IT ed i clienti interni relativamente ai servizi richiesti è resa possibile attraverso un accordo sui servizi IT e sui livelli di servizio e una loro definizione ben documentata. Questo processo comprende anche il monitoraggio e il reporting tempestivo agli stakeholder sul raggiungimento dei livelli di servizio. Questo processo facilita l'allineamento tra i servizi IT e i relativi requisiti aziendali.



Il controllo del processo IT :

Definire e gestire i livelli di servizio

che soddisfa i requisiti aziendali per l'IT di

assicurare l'allineamento fra i servizi chiave IT e la strategia aziendale

ponendo l'attenzione su

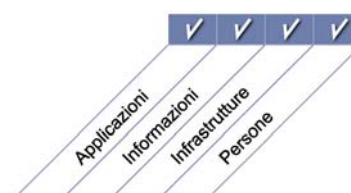
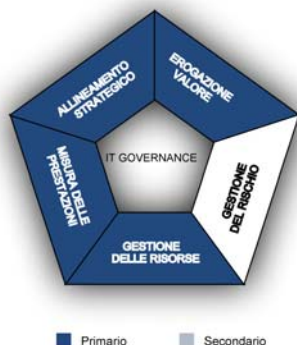
l'identificazione dei requisiti dei servizi, la definizione di accordi sui livelli di servizio e il monitoraggio del perseguimento di questi livelli

è ottenuto tramite

- la formalizzazione degli accordi interni ed esterni, in linea con i requisiti e la capacità di erogazione
- la produzione di relazioni sui livelli di servizio raggiunti (report e livelli conseguiti)
- l'identificazione e la comunicazione alla pianificazione strategica dei nuovi requisiti dei servizi e degli aggiornamenti

e viene misurato tramite

- la percentuale di stakeholder soddisfatti che i servizi erogati abbiano raggiunto i livelli concordati
- il numero di servizi erogati non in catalogo
- il numero di riunioni formali di revisione degli SLA svolte con le altre componenti aziendali nell'arco dell'anno



OBIETTIVI DI CONTROLLO

DS1 Definire e gestire i livelli di servizio

DS1.1 Modello per la gestione dei livelli di servizio

Definire un modello di riferimento che stabilisca un processo formalizzato di gestione dei livelli di servizio fra i clienti ed i fornitori del servizio. Questo modello di riferimento dovrebbe mantenere un allineamento continuo con le priorità e i requisiti aziendali e dovrebbe facilitare la comprensione comune del servizio fra il cliente ed i fornitori. Il modello di riferimento dovrebbe comprendere i processi per la definizione dei requisiti dei servizi e dei servizi stessi, degli accordi sui livelli di servizio (SLA), degli accordi sui livelli operativi (OLA) e delle fonti di finanziamento. Questi attributi dovrebbero essere organizzati in un catalogo dei servizi. Il modello di riferimento dovrebbe definire la struttura organizzativa per la gestione dei livelli di servizio identificando i ruoli, le attività e le responsabilità dei clienti e dei fornitori, sia interni sia esterni.

DS1.2 Definizione dei servizi

Definire i servizi IT basandosi sulle caratteristiche e sui requisiti dei servizi aziendali. Assicurarsi che questi siano organizzati e mantenuti centralmente mediante la realizzazione di un catalogo del portfolio dei servizi.

DS1.3 Accordi sui livelli di servizio

Definire e concordare gli accordi sui livelli di servizio (SLA) per tutti i servizi IT critici basandosi sui requisiti posti dal cliente e sulle potenzialità dell'IT. Gli accordi dovrebbero comprendere: il mandato dei clienti, i requisiti di supporto ai servizi, le metriche qualitative e quantitative per misurare i servizi sottoscritti dagli stakeholder, le condizioni finanziarie e commerciali qualora applicabili, i ruoli e le responsabilità compresa la supervisione degli SLA. Elementi da considerare sono la disponibilità, l'affidabilità, le prestazioni, la capacità di crescita, i livelli di assistenza, il piano di continuità, la sicurezza e i limiti relativamente a nuove richieste.

DS1.4 Accordi sui livelli operativi

Definire i livelli operativi in modo tale da spiegare come i servizi saranno tecnicamente erogati per supportare gli SLA in modo ottimale. Gli OLA dovrebbero descrivere i processi tecnici in termini comprensibili per il fornitore e ciascuno di essi potrebbe supportare diversi SLA.

DS1.5 Monitoraggio e reporting dei livelli di servizio conseguiti

Monitorare sistematicamente i criteri seguiti per la definizione dei livelli di prestazione dei servizi. I report, riguardanti il raggiungimento dei livelli di servizio, dovrebbero essere forniti in un formato comprensibile per gli stakeholder. I controlli statistici dovrebbero essere attivati e analizzati per identificare andamenti positivi e/o negativi di ciascun servizio o dei servizi nel loro complesso.

DS1.6 Revisione degli accordi sui livelli di servizio e dei contratti

Revisionare regolarmente gli accordi sui livelli di servizio e i relativi contratti con i fornitori di servizi, sia interni sia esterni, per assicurarsi che siano efficaci, aggiornati e che i cambiamenti nei requisiti siano stati presi adeguatamente in considerazione.

LINEE GUIDA PER LA GESTIONE

DS1 Definire e gestire i livelli di servizio

Da	Inputs
PO1	Piano strategico per l'IT, piano tattico per l'IT, portafoglio dei servizi IT
PO2	Classificazioni dei dati definite
PO5	Portafoglio dei servizi IT aggiornato
AI2	Pianificazione iniziale degli SLA
AI3	Pianificazione iniziale degli OLA
DS4	Requisiti per i servizi di disaster recovery, inclusi i ruoli e le responsabilità
ME1	Requisiti di performance in input alla pianificazione IT

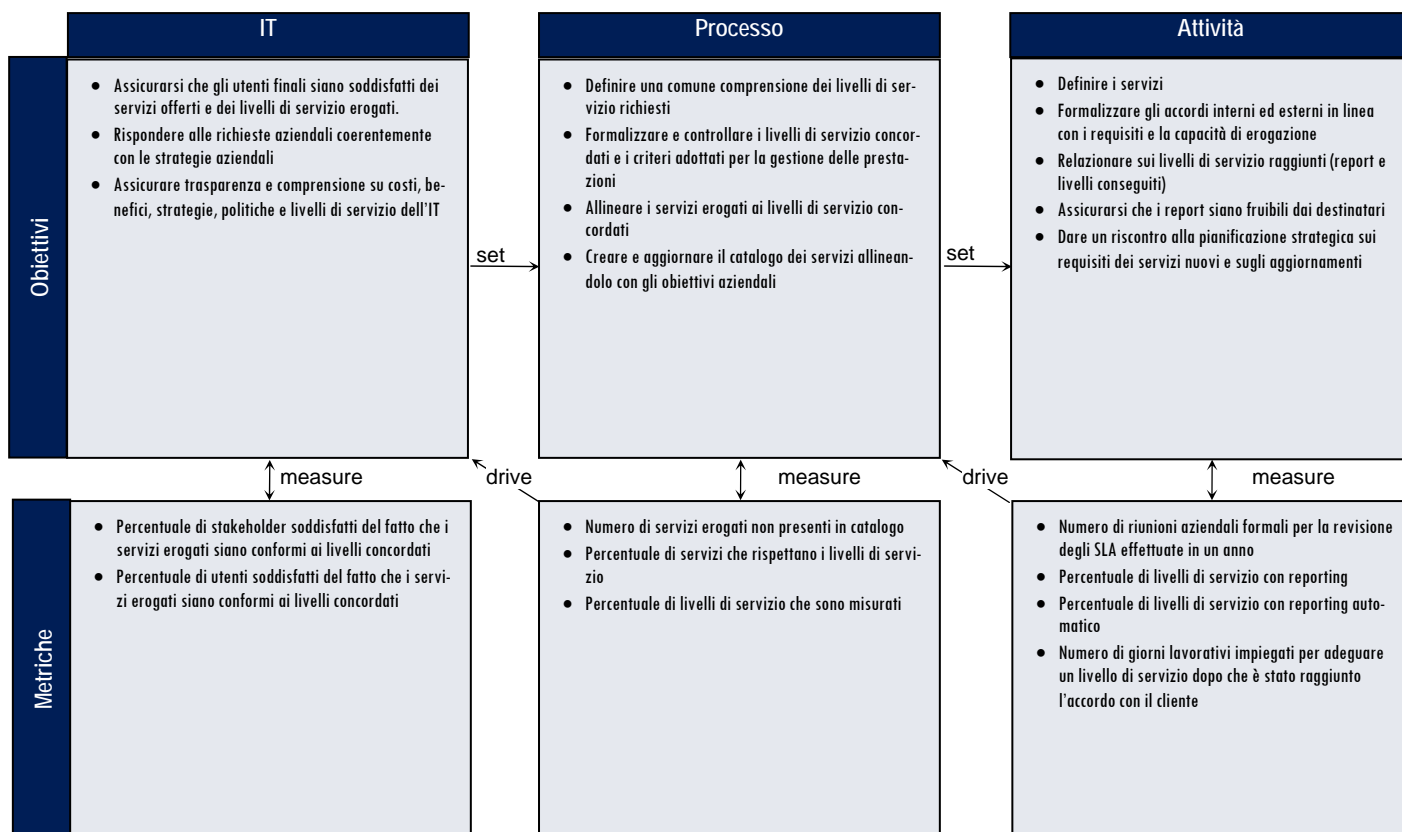
Outputs	a							
Relazione sulla revisione dei contratti	DS2							
Relazione sulle prestazioni dei processi	ME1							
Requisiti nuovi o aggiornati dei servizi	PO1							
SLA	AI1	DS2	DS3	DS4	DS6	DS8	DS13	
OLA	DS4	DS5	DS6	DS7	DS8	DS11	DS13	
Portafoglio dei servizi IT aggiornato	PO1							

RACI Chart

Ruoli

Attività	Amministr. Delegato o DG	Direttore Amministrativo	Direttore Utenti IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architettura IT	Responsabile sviluppo IT	PMO	Conformità, audit, rischio e sicurezza	Service Manager		
Creare un modello di riferimento per definire i servizi IT			C	A	C	C	I	C	C	I	C	R	
Realizzare il catalogo dei servizi IT			I	A	C	C	I	C	C	I	I	R	
Definire accordi sui livelli di servizio (SLA) per i servizi IT critici			I	I	C	C	R	I	R	C	C	A/R	
Definire accordi sui livelli operativi (OLA) per soddisfare gli SLA				I	C	R	I	R	R	C	C	A/R	
Monitorare e rendicontare end-to-end le prestazioni sui livelli di servizio				I	I	R		I	I		I	A/R	
Riesaminare gli SLA e i relativi contratti con i fornitori			I	I	C	R		R	R		C	A/R	
Riesaminare ed aggiornare il catalogo dei servizi IT				I	A	C	C	I	C	C	I	I	R
Creare un piano di miglioramento dei servizi				I	A	I	R	I	R	C	C	I	R

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

DS1 Definire e gestire i livelli di servizio

Il grado di strutturazione del processo *Definire e gestire i livelli di servizio* che soddisfa i requisiti aziendali per l'IT di assicurare l'allineamento fra i servizi chiave IT e la strategia aziendale è:

0 Non esistente quando

La Direzione non ha riconosciuto la necessità di un processo per la definizione dei livelli di servizio. Non sono state assegnate le responsabilità e le attività per il monitoraggio dei livelli di servizio.

1 Iniziale / ad hoc quando

Esiste la consapevolezza della necessità di gestire i livelli di servizio, ma il processo è informale e di natura reattiva. Non sono assegnate le responsabilità e i compiti per la definizione e la gestione dei servizi. Se esistono delle misure delle prestazioni, esse sono solamente qualitative con obiettivi vagamente definiti. I report sono informali, sporadici e approssimativi.

2 Ripetibile ma intuitivo quando

Esistono dei livelli di servizio concordati, ma sono informali e non vengono rivisti. I rapporti sui livelli di servizio sono incompleti e potrebbero essere poco significativi o ambigui per i clienti. I rapporti sui livelli di servizio dipendono dalle capacità e dall'iniziativa di singoli responsabili. È stato designato un coordinatore dei livelli di servizio, con responsabilità definite ma senza sufficiente autorità. Se esiste il processo di conformità dei livelli di servizio concordati, è attivato su base volontaria e non obbligatoriamente.

3 Definito quando

Le responsabilità sono ben definite ma con autorità discrezionale. E' attivo un processo di sviluppo degli accordi sui livelli di servizio con punti di controllo per la valutazione dei livelli di servizio e della soddisfazione dell'utente. Servizi e livelli di servizio sono definiti, documentati e concordati utilizzando un processo standard. Sono identificate le carenze dei livelli di servizio ma le procedure su come superarle sono informali. C'è un chiaro collegamento fra il raggiungimento dei livelli di servizio attesi e i finanziamenti forniti. I livelli di servizio sono concordati ma potrebbero non essere coerenti con le esigenze aziendali.

4 Gestito e misurabile quando

I livelli di servizio sono identificati sempre più nella fase di definizione dei requisiti di sistema e sono compresi nella fase di progettazione dell'ambiente operativo e applicativo. La soddisfazione dell'utente viene misurata e valutata sistematicamente. La misura delle prestazioni considera le esigenze dell'utente piuttosto che solamente gli obiettivi IT. Le misure per valutare i livelli di servizio stanno diventando standardizzate e riflettono le norme industriali. I criteri per definire i livelli di servizio sono basati sulle criticità aziendali e includono disponibilità, affidabilità, prestazioni, crescita di potenzialità, supporto all'utente, pianificazione della continuità e considerazioni sulla sicurezza. Quando non vengono raggiunti i livelli di servizio viene eseguita sistematicamente l'analisi delle cause. Il sistema di reportistica sul monitoraggio dei livelli di servizio diventa sempre più automatizzato. Sono definiti e compresi chiaramente i rischi finanziari e operativi associati al non raggiungimento dei livelli di servizio concordati. Un formale sistema di misurazione è istituito e aggiornato.

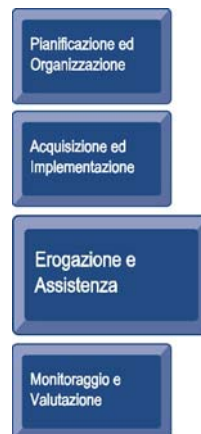
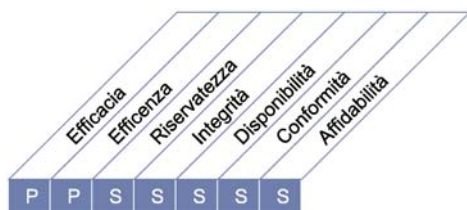
5 Ottimizzato quando

I livelli di servizio vengono di continuo rivisti per assicurare l'allineamento degli obiettivi IT a quelli aziendali, mentre si trae vantaggio dall'innovazione tecnologica includendo il rapporto costi-benefici. Tutti i processi di gestione dei livelli di servizio sono soggetti a continui miglioramenti. I livelli di soddisfazione della clientela sono continuamente monitorati e gestiti. I livelli di servizio attesi riflettono gli specifici obiettivi strategici delle unità aziendali e sono valutati sulla base di criteri industriali. La Direzione IT ha le risorse e la responsabilità necessarie per raggiungere gli obiettivi relativi ai livelli di servizio e la retribuzione è strutturata in modo da prevedere degli incentivi per il raggiungimento di questi obiettivi. L'alta Direzione controlla le metriche di performance quale parte di un processo di miglioramento continuo.

DESCRIZIONE DEL PROCESSO

DS2 Gestire i servizi di terze parti

La necessità di assicurare che i servizi forniti da terze parti (fornitori, rivenditori, partner) siano conformi ai requisiti aziendali comporta l'istituzione di un efficace processo di gestione delle terze parti. Questo processo è attuato sia attraverso l'inserimento negli accordi con le terze parti di una chiara definizione dei ruoli, delle responsabilità e delle aspettative, sia attraverso la revisione ed il monitoraggio di tali accordi per garantirne l'efficacia e la conformità. Un'efficace gestione dei servizi di terze parti minimizza i rischi aziendali associati a mancate o parziali prestazioni dei fornitori.



Il controllo del processo IT :

Gestire i servizi di terze parti

che soddisfa i requisiti aziendali per l'IT di

fornire servizi acquisiti da terze parti soddisfacenti, mantenendosi trasparenti rispetto a benefici, costi e rischi

ponendo l'attenzione su

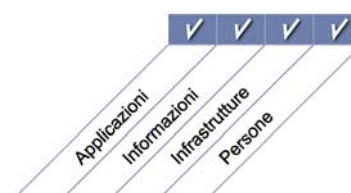
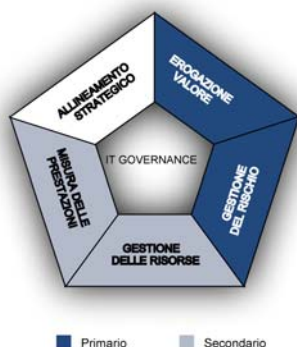
stabilire relazioni e responsabilità bilaterali con qualificate terze parti fornitrici di servizi e monitorare i servizi erogati per verificare ed assicurare il rispetto degli accordi

è ottenuto tramite

- l'identificazione e la classificazione dei fornitori di servizi
- l'identificazione e la mitigazione del rischio relativo ai fornitori
- il controllo e la misura delle prestazioni dei fornitori

e viene misurato tramite

- il numero degli utenti insoddisfatti dei servizi contrattualizzati
- la percentuale dei principali fornitori conformi ai requisiti ed ai livelli di servizio chiaramente definiti
- la percentuale dei principali fornitori sottoposti a monitoraggio



OBIETTIVI DI CONTROLLO

DS2 Gestire i servizi di terze parti

DS2.1 Identificazione delle relazioni con tutti i fornitori

Individuare tutti i fornitori di servizi e classificarli in funzione del tipo di fornitura, importanza e criticità. Mantenere aggiornata la documentazione formale delle caratteristiche tecniche ed organizzative contenenti: ruoli e responsabilità, finalità, erogazioni attese e credenziali dei rappresentanti di questi fornitori.

DS2.2 Gestione delle relazioni con i fornitori

Formalizzare il processo di gestione del rapporto intrattenuto con ciascun fornitore. Il responsabile del rapporto con il fornitore dovrebbe relazionare sui problemi esistenti con i clienti e con il fornitore e assicurare la qualità della relazione basata sulla fiducia reciproca e sulla trasparenza (ad esempio attraverso accordi sui livelli di servizio)

DS2.3 Gestione del rischio relativo ai fornitori

Individuare e mitigare il rischio relativo alla capacità dei fornitori di continuare ad erogare il servizio con: efficacia, sicurezza, efficienza e continuità. Assicurare che i contratti siano in linea con gli standard di mercato e conformi ai requisiti previsti da leggi e norme. La gestione dei rischi dovrebbe inoltre considerare: gli accordi di non divulgazione (NDA- Non Disclosure Agreement), le clausole di garanzia (ad esempio sui sorgenti), la continuità dei fornitori critici, la conformità ai requisiti di sicurezza, la disponibilità di fornitori alternativi, le penali ed i premi, ecc.

DS2.4 Monitoraggio delle prestazioni dei fornitori

Stabilire un processo di monitoraggio dei servizi erogati per assicurare che i fornitori siano conformi agli attuali requisiti aziendali e continuino ad essere aderenti ai contratti ed ai livelli di servizio contrattualizzati e che le prestazioni siano competitive rispetto a fornitori alternativi ed alle condizioni di mercato.

LINEE GUIDA PER LA GESTIONE

DS2 Gestire i servizi di terze parti

Da	Inputs
PO1	Strategia di fornitura IT
P08	Standard di acquisizione
A15	Accordi contrattuali, requisiti di gestione delle relazioni con terze parti
DS1	SLA, resoconto sulla revisione dei contratti
DS4	Requisiti per i servizi di Disaster Recovery, compresi i ruoli e le responsabilità

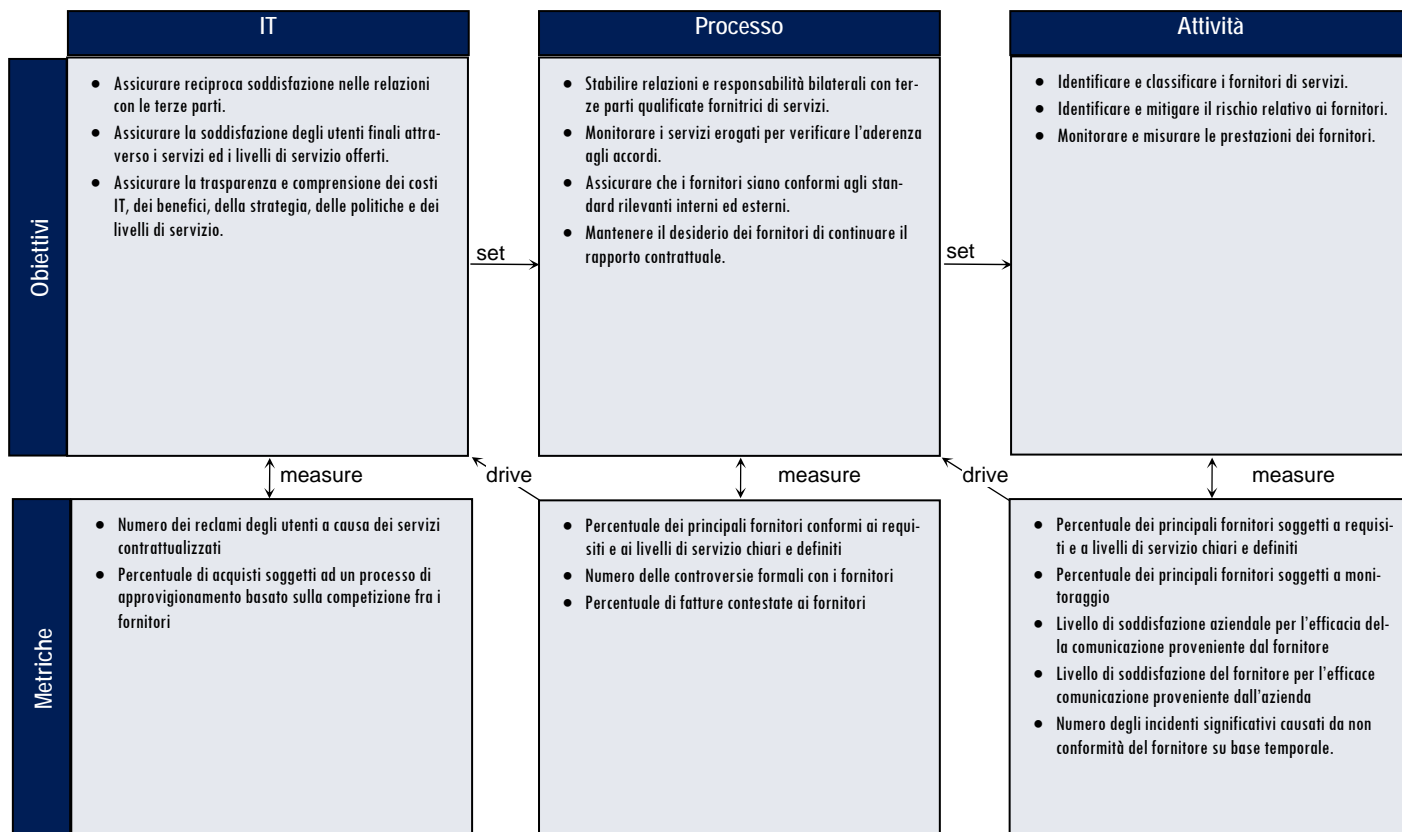
Outputs	a						
Relazione sulle prestazioni dei processi	ME1						
Catalogo dei fornitori	A15						
Rischi relativi ai fornitori	PO9						

RACI Chart

Ruoli

Attività	Amministr. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architettura IT	Responsabile sviluppo IT	Responsabile amminisrativo IT	PMO	Conformità, audit, rischio e sicurezza
Identificare e classificare le caratteristiche dei servizi di terze parti					I	C	R	C	R	A/R	C
Definire e documentare il processo di gestione dei fornitori		C			A	I	R	I	R	R	C
Definire politiche e procedure per la selezione e valutazione dei fornitori		C			A	C	C		C	R	C
Identificare, valutare e mitigare i rischi relativi ai fornitori			I		A		R		R	R	C
Monitorare i servizi erogati dai fornitori					R	A	R		R	R	C
Valutare gli obiettivi a lungo termine del rapporto di fornitura tenendo in considerazione le esigenze di tutti gli stakeholder	C	C	C	A/R	C	C	C	C	C	R	C

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

DS2 Gestire i servizi di terze parti

Il grado di strutturazione del processo *Gestire i servizi di terze parti* che soddisfa i requisiti aziendali per l'IT di fornire servizi acquisiti da terze parti soddisfacenti, mantenendosi trasparenti rispetto a benefici, costi e rischi è:

0 Non esistente quando

Le responsabilità non sono definite. Non ci sono politiche e procedure formali relative ai contratti con le terze parti. I servizi di terze parti non sono né approvati né rivisti dalla Direzione. Non ci sono attività di misurazione e reporting provenienti dalle terze parti. In assenza di obblighi contrattuali di rendicontazione, la Direzione non è informata sulla qualità del servizio fornito.

1 Iniziale / ad hoc quando

La Direzione è consapevole della necessità di disporre di procedure e politiche documentate per la gestione dei servizi di terze parti, inclusi i contratti firmati. Non ci sono condizioni contrattuali standard da usare con i fornitori di servizi. La misurazione del servizio fornito è informale e su base spontanea. Le procedure dipendono dall'esperienza del singolo e dal fornitore (ad esempio: a richiesta).

2 Ripetibile ma intuitivo quando

Il processo di supervisione dei servizi forniti da terze parti, dei rischi associati e dei servizi erogati è informale. Viene firmato un contratto pro forma con indicati i termini e le condizioni standard del fornitore (ad esempio la descrizione dei servizi che devono essere forniti). Sono disponibili dei resoconti sui servizi forniti ma non supportano gli obiettivi aziendali.

3 Definito quando

Esistono delle procedure ben documentate per gestire i servizi di terze parti, con chiari processi che assicurano idonee analisi e trattative con i venditori. Quando un accordo per la fornitura di un servizio viene concluso, la relazione con la terza parte è puramente contrattuale. Nel contratto viene spiegata in dettaglio la natura del servizio che deve essere fornito e comprende i requisiti operativi, legali e di controllo. È assegnata la responsabilità di supervisione dell'erogazione del servizio fornito da terze parti. Le condizioni contrattuali sono basate su modelli standardizzati. Il rischio aziendale associato al servizio fornito dalla terza parte è valutato e sono redatte delle relazioni periodiche.

4 Gestito e misurabile quando

Sono stati stabiliti dei criteri formali e standardizzati che definiscono i termini di incarico, ambito, servizi da erogare o beni da fornire, convenzioni, tempificazione, costi, accordi di fatturazione, responsabilità. Sono assegnate le responsabilità per la gestione sia del contratto sia del fornitore. Sono sistematicamente verificati l'idoneità del venditore, i rischi attinenti e le sue potenzialità operative. I requisiti dei servizi sono definiti e collegati agli obiettivi aziendali. È previsto un processo di revisione delle prestazioni del servizio rispetto ai termini contrattuali, fornendo un contributo alla valutazione attuale e futura dei servizi di terze parti. Un modello di contabilità analitica (attribuzione dei costi ai servizi) è usato nel processo di acquisizione. Tutte le parti interessate sono consapevoli delle aspettative di servizio, di costo, di tempificazione e di controllo. Gli obiettivi e le metriche per la supervisione dei fornitori di servizi sono stati concordati.

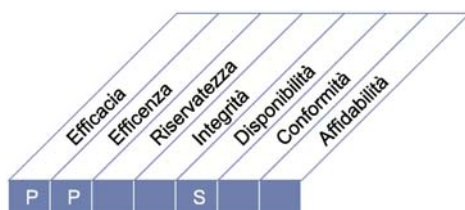
5 Ottimizzato quando

I contratti firmati con terze parti vengono rivisti sistematicamente con scadenze predefinite. La responsabilità per la gestione dei fornitori e della qualità dei servizi forniti è assegnata. Le evidenze di conformità ai contratti in termini operativi, legali e di controllo sono monitorate e vengono imposte eventuali azioni correttive. La terza parte è soggetta ad una periodica revisione indipendente, che fornisce dei feedback sulle prestazioni utilizzati per migliorare i servizi erogati. Le misurazioni variano in risposta ai cambiamenti delle condizioni aziendali. Le misure sono di supporto per la rilevazione tempestiva di eventuali problemi relativi a servizi di terze parti. Il rendiconto finale (predefinito e complessivo rispetto ai servizi forniti) sui livelli di servizio conseguiti è collegato alla remunerazione del fornitore. La direzione, sulla base delle misure ottenute, corregge il processo di selezione dei fornitori e il monitoraggio dei servizi di terze parti.

DESCRIZIONE DEL PROCESSO

DS3 Gestire le prestazioni e la capacità produttiva

La necessità di gestire le prestazioni e la capacità produttiva delle risorse IT richiede un processo di revisione periodica delle prestazioni e della capacità produttiva delle risorse IT. Questo processo include la previsione delle necessità future basata sui requisiti relativi al carico di lavoro, alla memorizzazione e alle emergenze. Questo processo fornisce la garanzia che le risorse informative supportano i requisiti di business e sono continuamente disponibili.



Il controllo del processo IT :

Gestire le prestazioni e la capacità produttiva

che soddisfa i requisiti aziendali per l'IT di

ottimizzare le prestazioni delle infrastrutture, delle risorse e della capacità produttiva dell'IT per soddisfare le esigenze aziendali

ponendo l'attenzione su

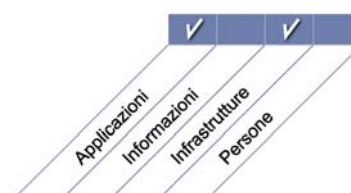
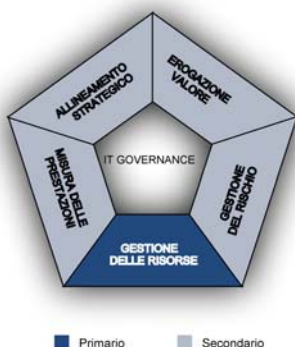
il raggiungimento dei tempi di risposta concordati negli SLA, la minimizzazione dei tempi di fermo e il miglioramento continuo delle prestazioni e della capacità produttiva dell'IT attraverso monitoraggi e misurazioni

è ottenuto tramite

- la pianificazione e fornitura della necessari capacità e disponibilità dei sistemi
- il controllo e la rendicontazione delle prestazioni dei sistemi
- la modellazione e la previsione delle prestazioni dei sistemi

e viene misurato tramite

- il numero di ore perse per utente per mese a causa di una insufficiente pianificazione della capacità produttiva
- la percentuale di picchi dove l'utilizzo eccede l'obiettivo prefissato
- la percentuale di tempi di risposta non conformi agli SLA.



OBIETTIVI DI CONTROLLO

DS3 Gestire le prestazioni e la capacità produttiva

DS3.1 Pianificazione delle prestazioni e della capacità produttiva

Definire un processo di pianificazione per il riesame delle prestazioni e della capacità produttiva delle risorse IT, per assicurare che siano disponibili prestazioni e capacità produttive ad un costo giustificabile, per far fronte ai carichi di lavoro concordati come determinato dagli accordi sui livelli di servizio. La pianificazione della capacità produttiva e delle prestazioni dovrebbe utilizzare appropriate tecniche di modellizzazione per produrre un modello delle performance attuali e previste, della capacità produttiva e del throughput delle risorse IT.

DS3.2 Capacità produttiva e prestazioni attuali

Valutare le attuali capacità produttive e le prestazioni delle risorse IT per determinare se esistono una sufficiente capacità produttiva e una sufficiente performance a fronte dei livelli di servizio concordati.

DS3.3 Capacità produttiva e prestazioni future

Effettuare ad intervalli regolari previsioni sulle prestazioni e sulla capacità produttiva delle risorse IT, per minimizzare il rischio di non fornitura del servizio a causa di una insufficiente capacità produttiva o prestazioni ridotte, e per identificare anche la capacità produttiva in eccesso per un possibile reimpiego. Identificare i trend dei carichi di lavoro e determinare le relative previsioni per contribuire alla pianificazione delle prestazioni e della capacità produttiva.

DS3.4 Disponibilità delle risorse IT

Fornire la capacità produttiva e le performance richieste, prendendo in considerazione aspetti come il normale carico, le emergenze, le esigenze di memorizzazione e il ciclo di vita delle risorse IT. Dovrebbero essere definite delle linee guida per l'assegnazione delle priorità alle attività, la gestione della tolleranza ai guasti e le modalità di allocazione delle risorse. La Direzione dovrebbe assicurare che i piani di emergenza forniscano una adeguata soluzione per la disponibilità, la capacità produttiva e le prestazioni di ciascuna risorsa IT.

DS3.5 Monitoraggio e rapporti

Monitorare continuamente le prestazioni e la capacità produttiva delle risorse IT. I dati raccolti hanno due finalità:

- Mantenere e mettere a punto le prestazioni attuali dell'IT e fornire soluzioni per problematiche come la capacità di resistenza o ripresa (resilience), le emergenze, i carichi di lavoro attuali e previsti, i trend delle esigenze di memorizzazione e l'acquisizione pianificata delle risorse.
- Rendicontare la disponibilità dei servizi erogati all'azienda come richiesto dagli SLA.

Allegare a tutte le eccezioni documentate le raccomandazioni sulle azioni correttive.

LINEE GUIDA PER LA GESTIONE

DS3 Gestire le prestazioni e la capacità produttiva

Da	Inputs
AI2	Specifiche sulla disponibilità, sulla continuità e sul ripristino
AI3	Requisiti di monitoraggio dei sistemi
DS1	SLA

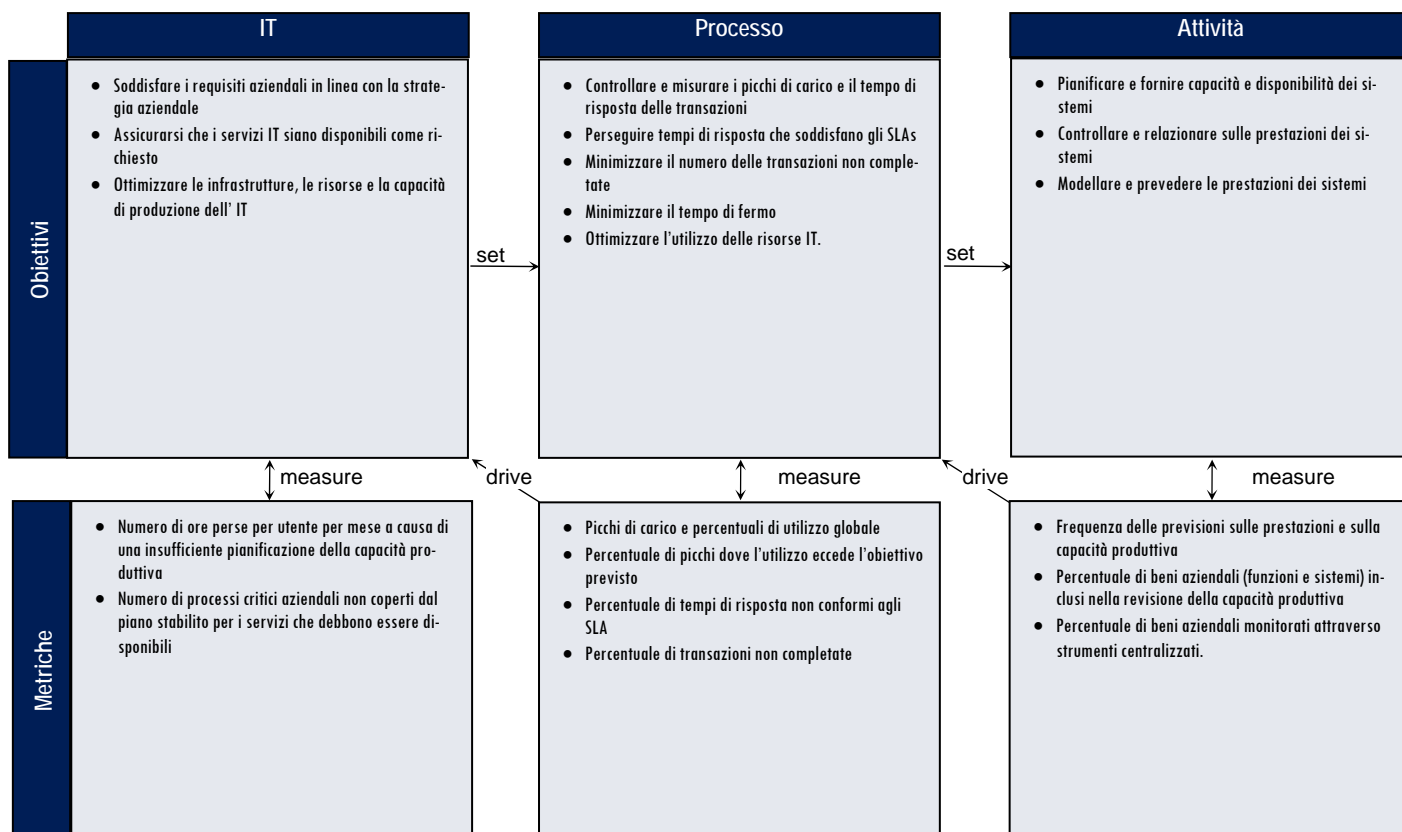
Outputs	a					
Informazioni sulla capacità produttiva e sulle prestazioni	PO2	PO3				
Piani sulle prestazioni e sulla capacità produttiva (requisiti)	PO5	AI1	AI3	ME1		
Cambiamenti richiesti	AI6					
Relazioni sulle prestazioni dei processi	ME1					

RACI Chart

Ruoli

Attività	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architettura IT	Responsabile sviluppo IT	PMO	Continuità, audit, rischio e sicurezza
Stabilire un processo pianificato per la revisione delle prestazioni e della capacità produttiva delle risorse IT				A		R	C	C	C	
Revisionare le prestazioni e le capacità produttive attuali delle risorse IT				C	I	A/R		C	C	C
Condurre una previsione sulle prestazioni e sulle capacità produttive delle risorse IT				C	C	A/R	C	C	C	C
Condurre un'analisi delle differenze (gap analysis) per identificare il divario delle risorse IT				C	I	A/R		R	C	C
Condurre la pianificazione delle emergenze per le potenziali risorse IT non disponibili				C	I	A/R		C	C	I
Costante monitoraggio e resoconto sulla disponibilità, prestazioni e capacità produttiva delle risorse IT				I	I	A/R		I	I	I

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

DS3 Gestire le prestazioni e la capacità produttiva

Il grado di strutturazione del processo *Gestire le prestazioni e la capacità produttiva* che soddisfa i requisiti aziendali per l'IT di *ottimizzare le prestazioni delle infrastrutture, delle risorse e della capacità produttiva dell'IT per soddisfare le esigenze aziendali* è:

0 Non esistente quando

La Direzione non ha rilevato che i processi chiave aziendali possono richiedere prestazioni di alto livello all'IT o che l'azienda globalmente necessita di servizi IT che potrebbero superare la capacità produttiva. Non c'è un processo di pianificazione della capacità produttiva.

1 Iniziale / ad hoc quando

Gli utenti escogitano elaborazioni alternative a causa dei vincoli sulle prestazioni o sulla potenza di elaborazione. C'è poca sensibilità alle esigenze di pianificazione della capacità produttiva e delle prestazioni da parte dei titolari dei processi aziendali. Le azioni intraprese per la gestione delle prestazioni e della potenza di elaborazione sono tipicamente reattive. Il processo di pianificazione della capacità produttiva e delle prestazioni è informale. La comprensione delle capacità produttive e delle prestazioni delle risorse IT attuali e future è limitata.

2 Ripetibile ma intuitivo quando

La Direzione aziendale e IT è consapevole dell'impatto della non gestione delle prestazioni e della capacità produttiva. Le prestazioni necessarie sono generalmente soddisfatte basandosi su sistemi individuali di valutazione e sulle conoscenze dei team di progetto e di assistenza. Possono essere utilizzati singoli strumenti per identificare i problemi legati alle prestazioni e alla potenza elaborativa, ma la consistenza dei risultati dipende dall'esperienza di dipendenti chiave. Non è prevista una valutazione globale delle prestazioni dell'IT né considerazioni relative alle peggiori situazioni o con picchi di carico. È probabile che si manifestino problemi di disponibilità in maniera casuale ed inattesa e che sia richiesto un tempo considerevole per la relativa diagnosi e risoluzione. Tutte le misure sulle performance IT sono basate principalmente sulle necessità dell'IT e non sulle necessità dei clienti.

3 Definito quando

Le richieste di prestazioni e capacità produttive sono definite attraverso il ciclo di vita dei sistemi. Sono definiti i requisiti del servizio e le metriche da utilizzare per misurare le prestazioni operative. Le prestazioni e le capacità produttive future sono modellate attraverso un processo definito. Si possono produrre report che forniscono statistiche sulle prestazioni. I problemi relativi alle prestazioni ed alla capacità produttiva sono ancora probabili e viene impiegato del tempo per correggerli. Nonostante i livelli di servizio siano resi pubblici, gli utenti e i clienti sono talvolta scettici sulle potenzialità del servizio.

4 Gestito e misurabile quando

Sono disponibili strumenti e processi atti a misurare l'utilizzo dei sistemi, le prestazioni e la capacità produttiva e i risultati sono confrontati con gli obiettivi definiti. Sono disponibili informazioni aggiornate che forniscono statistiche standardizzate sulle prestazioni segnalando casi quali insufficienti prestazioni o capacità produttive. Prestazioni insufficienti e problemi sulla capacità produttiva sono affrontati in accordo con standard e procedure definite. Vengono usati strumenti automatizzati per sorvegliare risorse specifiche come spazio su disco, rete, server e gateways di rete. Le statistiche sulle prestazioni e capacità produttive sono documentate utilizzando il linguaggio usato nei processi aziendali affinché gli utenti e i clienti possano comprendere i livelli di servizio IT. Gli utenti sono generalmente soddisfatti delle attuali capacità di servizio e richiedono livelli di disponibilità nuovi e migliorati. Le metriche per misurare le prestazioni e la capacità produttiva dell'IT sono concordati ma possono essere applicati in modo sporadico ed inconsistente.

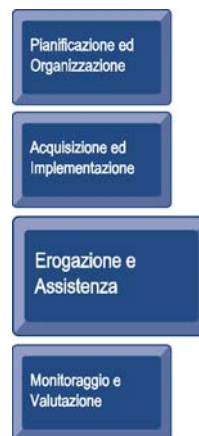
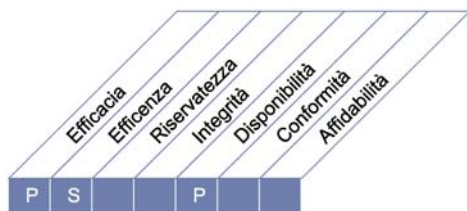
5 Ottimizzato quando

I piani relativi alle prestazioni ed alla potenza sono allineati con le previsioni aziendali. L'infrastruttura IT e le richieste aziendali sono soggette a regolare revisione per assicurare il raggiungimento dell'ottimizzazione della capacità produttiva al più basso costo possibile. Gli strumenti per controllare le risorse IT critiche sono stati standardizzati per tutte le piattaforme e sono collegati ad un unico sistema aziendale di gestione dei problemi. Gli strumenti di monitoraggio rilevano e possono correggere automaticamente i problemi relativi alle prestazioni ed alla capacità produttiva. Gli andamenti vengono rilevati mostrando i problemi di prestazioni incombenti, causati dall'aumento dei volumi del business, permettendo la pianificazione ed evitando incidenti inattesi. Le metriche per misurare le prestazioni e la capacità produttiva IT sono state allineate con le metriche e con gli indicatori di performance di tutti i processi aziendali critici e sono misurate sistematicamente. La Direzione corregge la pianificazione delle prestazioni e della capacità produttiva sulla base dell'analisi di queste misure.

DESCRIZIONE DEL PROCESSO

DS4 Assicurare la continuità del servizio

La necessità di assicurare la continuità dei servizi IT richiede lo sviluppo, la manutenzione ed il test del piano di continuità IT, l'utilizzo di sistemi di archiviazione dei dati per il ripristino del sistema collocati a sufficiente distanza dal sito e l'addestramento periodico al piano di continuità. Un efficace processo di continuità del servizio minimizza la probabilità e l'impatto di una grave interruzione del servizio IT per processi e funzioni aziendali chiave.



Il controllo del processo IT :

Assicurare la continuità del servizio

che soddisfa i requisiti aziendali per l'IT di

Assicurare il minimo impatto sull'azienda in caso di interruzione del servizio IT

ponendo l'attenzione su

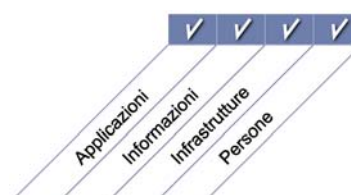
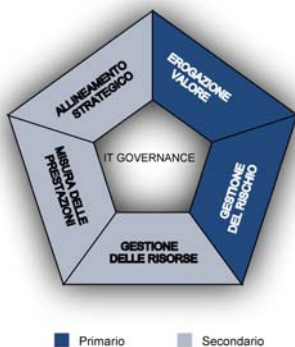
Costruire la capacità di ripresa (resilienza) all'interno della soluzione automatica e sviluppare, aggiornare e testare il piano di continuità IT.

è ottenuto tramite

- Sviluppare, mantenere e migliorare il piano di emergenza IT
- Effettuare l'addestramento sul piano di emergenza IT e testarlo
- Conservare copie del piano di emergenza e dei dati in un'ubicazione remota

e viene misurato tramite

- Numero di ore perse dagli utenti per mese a causa di una interruzione non pianificata
- Numero di processi aziendali critici dipendenti dall'IT non coperti dal piano di continuità IT.



OBIETTIVI DI CONTROLLO

DS4 Assicurare la continuità del servizio

DS4.1 Modello di riferimento della continuità IT

Sviluppare un modello di riferimento per la continuità IT che supporti la gestione della continuità aziendale attraverso un processo coerente. L'obiettivo del modello di riferimento è di aiutare a determinare le richieste di capacità di ripresa delle infrastrutture e guidare lo sviluppo di un piano di Disaster Recovery e un piano di emergenza IT. Il modello di riferimento dovrebbe indirizzare la struttura organizzativa nella gestione della continuità operativa, includendo ruoli, compiti e responsabilità dei fornitori di servizi interni ed esterni, del loro management e dei loro clienti e il processo di pianificazione che crea le regole e le strutture coinvolte nella documentazione, nel test del Disaster Recovery e del piano di emergenza IT. Il piano dovrebbe anche indirizzare aspetti come l'identificazione delle risorse critiche, il controllo ed i rapporti sulla disponibilità delle risorse critiche, i processi alternativi e i principi di salvataggio e ripristino.

DS4.2 Piano di continuità IT

Sviluppare il piano di continuità IT basandosi sulla struttura di riferimento e finalizzandolo alla riduzione dell'impatto o della grave interruzione dei processi e delle funzioni aziendali chiave. I piani dovrebbero essere basati sulla comprensione e valutazione del rischio di potenziali impatti sul business e indirizzare i requisiti sulla capacità di ripresa, sui processi alternativi e sulla capacità di ripristino di tutti i servizi IT critici. I piani dovrebbero trattare i seguenti argomenti: linee guida per l'utilizzo, ruoli e responsabilità, procedure, processi di comunicazione e approccio al test.

DS4.3 Risorse critiche IT

Concentrare l'attenzione sugli elementi più critici del piano di continuità per costruire capacità di ripresa (resilienza) e stabilire delle priorità per le situazioni di ripristino. Evitare di disperdere l'impegno nel ripristino di elementi poco rilevanti e assicurare risposte e ripristini in linea con le priorità aziendali, assicurare allo stesso tempo che i costi siano mantenuti ad un livello accettabile e conformi a regolamenti e requisiti contrattuali. Considerare i fabbisogni di resilienza, di risposta e di ripristino per differenti livelli, p. e. da 1 a 4 ore, da 4 a 24, più di 24 ore e per periodi nei quali vengono svolte operazioni aziendali critiche.

DS4.4 Aggiornamento del piano di continuità IT

Incoraggiare la Direzione IT a definire ed eseguire procedure di controllo dei cambiamenti per assicurare che il piano di continuità IT sia mantenuto aggiornato e rifletta continuamente i requisiti aziendali in essere. Comunicare i cambiamenti nelle procedure e nelle responsabilità in modo chiaro e in maniera tempestiva.

DS4.5 Verifica del piano di continuità IT

Verificare regolarmente il piano di continuità IT per assicurare che i sistemi IT possano essere effettivamente ripristinati, i difetti siano riscontrati e il piano rimanga efficace. Questo richiede un'attenta preparazione, documentazione e relazione sui risultati dei test e, in base ai risultati, l'implementazione di un piano di azione. Comprendere nei test di ripristino le situazioni relative a singole applicazioni, a scenari di test integrato, a test end-to-end, a test integrati con i fornitori.

DS4.6 Addestramento sul piano di continuità IT

Fornire a tutte le parti interessate regolari sessioni di addestramento relativamente alle procedure, ai ruoli e alle responsabilità in caso di incidente o disastro. Verificare e migliorare l'addestramento in accordo con i risultati dei test di emergenza.

DS4.7 Distribuzione del piano di continuità IT

Verificare se esiste e se è operante una strategia di distribuzione del piano per assicurare che il piano sia distribuito in modo appropriato e sicuro, e che sia disponibile alle parti interessate debitamente autorizzate quando e dove necessario. Dovrebbe essere posta attenzione nel rendere i piani accessibili, qualunque sia lo scenario di disastro.

DS4.8 Recupero e ripristino dei servizi IT

Pianificare le azioni che devono essere intraprese nel periodo in cui i servizi IT devono essere recuperati e ripristinati. Questo potrebbe includere l'attivazione di siti alternativi (backup sites), l'attivazione di processi alternativi, la comunicazione di procedure di ripristino alla clientela ed al personale interessato, ecc. Assicurare che l'azienda sia consapevole dei tempi di ripristino e degli investimenti tecnologici necessari per supportare le esigenze di recupero e ripristino aziendali.

DS4.9 Conservazione dei supporti di backup in ubicazione remota

Conservare in un'ubicazione remota tutti i supporti critici di backup, la documentazione e le altre risorse IT necessarie per il ripristino IT e per l'attuazione del piano di continuità aziendale. Determinare il contenuto dei supporti di backup necessari, in collaborazione con i proprietari dei processi aziendali e con il personale IT. La Direzione del servizio di archiviazione remota dovrebbe conformarsi alla politica di classificazione dei dati ed alle pratiche aziendali di archiviazione dei media. La Direzione IT dovrebbe assicurare che le attrezzature dell'ubicazione remota siano periodicamente analizzate, almeno annualmente, sia per quanto riguarda il contenuto che le misure di sicurezza e protezione ambientale. Assicurare la compatibilità dell'hardware e del software per ripristinare i dati archiviati e verificare e aggiornare periodicamente i dati archiviati.

DS4.10 Revisione Post-Ripristino

Determinare se la Direzione IT ha previsto procedure per valutare l'adeguatezza del piano, in riferimento al ripristino della funzione IT a seguito di un disastro, e l'aggiornamento del piano coerentemente alle esigenze emerse nell'attività di ripristino.

LINEE GUIDA PER LA GESTIONE

DS4 Assicurare la continuità del servizio

Da	Inputs
PO2	Classificazione assegnata ai dati
PO9	Valutazione dei rischi
AI2	Specifiche di disponibilità, continuità e ripristino
AI4	Manuali utenti, operativi, di supporto, tecnici e amministrativi
DS1	SLA e OLA

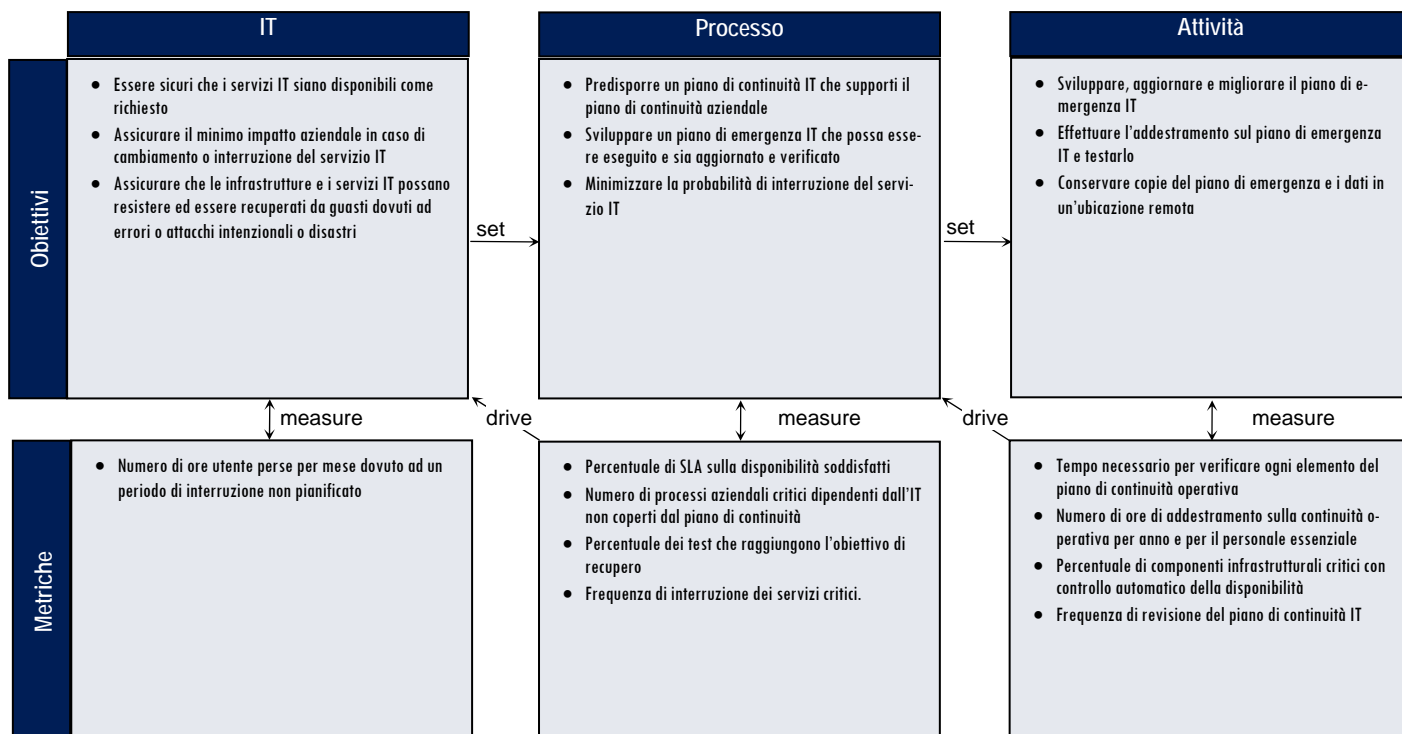
Outputs	a				
Risultati dei test di emergenza	PO9				
Elementi critici di configurazione IT	DS9				
Supporti di memorizzazione e piano di protezione	DS11	DS13			
Soglie di dichiarazione di incidente/disastro	DS8				
Requisiti dei servizi in caso di disastro, compresi ruoli e responsabilità	DS1	DS2			
Relazioni sulle performance dei processi	ME1				

RACI Chart

Ruoli

Attività	Amministratore DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architettura IT	Responsabile sviluppo IT	PMO	Continuità, audit, rischio e sicurezza	
Sviluppare un modello di riferimento per la continuità IT		C	C	A	C	R	R	R	C	C	R
Condurre un'analisi sugli impatti aziendali e la valutazione dei rischi		C	C	C	C	A/R	C	C	C	C	C
Sviluppare e aggiornare un piano di continuità IT	I	C	C	C	I	A/R		C	C	C	C
Identificare e classificare le risorse IT sulla base degli obiettivi di ripristino				C		A/R		C	I	C	I
Definire ed eseguire una procedura di controllo dei cambiamenti per assicurare che il piano di continuità sia aggiornato				I		A/R		R	R	R	I
Testare regolarmente il piano di continuità IT				I	I	A/R		C	C	I	I
Sviluppare un piano di azione come conseguenza dei risultati delle verifiche				C	I	A/R	C	R	R	R	I
Pianificare e condurre l'addestramento sul piano di continuità IT				I	R	A/R		C	R	I	I
Pianificare il recupero ed il ripristino dei servizi IT		I	I	C	C	A/R	C	R	R	R	C
Pianificare e implementare la conservazione e la protezione dei supporti di back up				I		A/R		C	C	I	I
Prevedere procedure per condurre revisioni post ripristino				C	I	A/R		C	C		C

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

DS4 Assicurare la continuità del servizio

Il grado di strutturazione del processo *Assicurare la continuità del servizio* che soddisfa i requisiti aziendali per l'IT di *Assicurare il minimo impatto sull'azienda in caso di interruzione del servizio IT* è:

0 Non esistente quando

Non c'è la comprensione del rischio, delle vulnerabilità e delle minacce all'operatività dell'IT o dell'impatto aziendale derivante dalla perdita dei servizi IT. La continuità del servizio non è considerata degna di attenzione da parte della Direzione.

1 Iniziale / ad hoc quando

Le responsabilità per la continuità del servizio sono informali, e l'autorità per assumere tale responsabilità è limitata. La Direzione sta iniziando a prendere consapevolezza dei rischi correlati e della necessità della continuità del servizio. L'attenzione della Direzione nei confronti dei servizi di continuità è focalizzata sulle risorse infrastrutturali piuttosto che sui servizi IT. Gli utenti stanno escogitando soluzioni alternative in risposta all'interruzione dei servizi. La risposta dell'IT ai grandi disastri è reattiva e impreparata. Le interruzioni pianificate vanno incontro alle esigenze dell'IT ma non considerano i requisiti aziendali.

2 Ripetibile ma intuitivo quando

La responsabilità per assicurare la continuità del servizio è stata assegnata. L'approccio per assicurare la continuità dei servizi è frammentario. Il reporting sulla disponibilità del sistema è sporadica, potrebbe essere incompleta e non tenere conto dell'impatto sul business. Non ci sono documenti sul piano di continuità, sebbene ci sia l'impegno alla disponibilità continua del servizio e siano noti i maggiori principi. Esiste un inventario dei sistemi e dei componenti critici, ma potrebbe non essere affidabile. Stanno emergendo pratiche per la continuità del servizio, ma il successo si basa sull'iniziativa dei singoli.

3 Definito quando

La responsabilità per la gestione della continuità di servizio è univoca. La responsabilità per la pianificazione e la verifica della continuità di servizio è chiaramente definita e assegnata. Il piano di continuità operativa IT è documentato ed è basato sulle criticità del sistema e sull'impatto aziendale. C'è un resoconto periodico sui test per la continuità del servizio. E' lasciata al singolo l'iniziativa di seguire gli standard e addestrarsi per gestire i principali incidenti o disastri. La Direzione comunica costantemente le esigenze da pianificare per la continuità del servizio. Vengono utilizzati componenti ad alta affidabilità e si provvede a ridondare adeguatamente i sistemi. Viene mantenuto aggiornato l'inventario dei sistemi e delle componenti critiche.

4 Gestito e misurabile quando

Le responsabilità e gli standard per la continuità del servizio sono sponsorizzati. E' assegnata la responsabilità per la manutenzione del piano di continuità. Le attività di manutenzione tengono conto dei risultati dei test sulla continuità di servizio, le "buone pratiche" interne ed i cambiamenti all'ambiente IT e aziendali. Vengono raccolti ed analizzati i dati strutturati sulla continuità, si realizzano report e si agisce di conseguenza. Un addestramento formale è obbligatorio per il processo relativo alla continuità di servizio. Le linee guida sulla ridondanza dei sistemi sono costantemente sviluppate. Pratiche di disponibilità e pianificazione della continuità del servizio si influenzano vicendevolmente. Gli incidenti connessi alla sicurezza sono classificati e il percorso di escalation dei problemi è ben conosciuto da tutti gli attori coinvolti. Gli obiettivi e le metriche per la continuità del servizio sono stati sviluppati e concordati ma potrebbero essere misurati in modo non coerente.

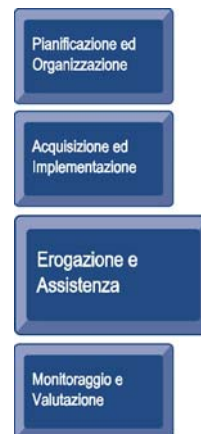
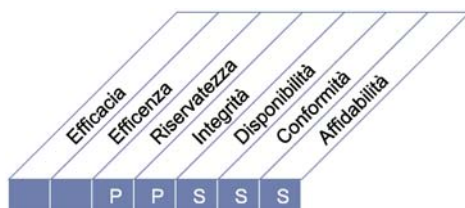
5 Ottimizzato quando

I processi integrati di continuità del servizio tengono conto di valutazioni comparative e delle linee guida esterne. Il piano di continuità IT è integrato con il piano di continuità aziendale e continuamente aggiornato. Requisiti per assicurare la continuità del servizio sono assicurati dai venditori e dai principali fornitori. Vengono effettuati dei test globali sulla continuità di servizio IT ed i risultati sono utilizzati per il processo di manutenzione del piano. La raccolta e l'analisi dei dati viene utilizzata per il continuo miglioramento del processo. È presente un completo allineamento tra le pratiche sulla disponibilità e la pianificazione della continuità di servizio. La Direzione assicura che i disastri o i principali incidenti non accadano a causa di un singolo punto di debolezza (single point of failure). Le pratiche di escalation sono comprese e applicate. Gli obiettivi e le metriche sulla continuità di servizio raggiunti sono misurati in modo sistematico. La Direzione da indicazioni per la ripianificazione della continuità di servizio sulla base delle misure effettuate.

DESCRIZIONE DEL PROCESSO

DS5 Garantire la sicurezza dei sistemi

La necessità di mantenere l'integrità delle informazioni e la protezione delle risorse IT richiede un processo di gestione della sicurezza. Questo processo compendia la definizione e l'aggiornamento dei ruoli e delle responsabilità sulla sicurezza IT, delle politiche, degli standard e delle procedure. La gestione della sicurezza comprende anche il monitoraggio della sicurezza, lo svolgimento di test periodici e l'implementazione delle azioni correttive a fronte di punti di debolezza o incidenti di sicurezza identificati. Una gestione efficace della sicurezza protegge tutte le risorse IT al fine di minimizzare gli impatti aziendali derivanti da vulnerabilità e da incidenti.



Il controllo del processo IT :

Garantire la sicurezza dei sistemi

che soddisfa i requisiti aziendali per l'IT di

salvaguardare l'integrità delle informazioni e dei processi infrastrutturali, minimizzare l'impatto derivante da vulnerabilità e da incidenti

ponendo l'attenzione su

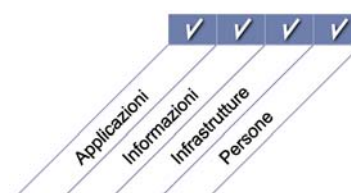
definire le politiche, i piani e le procedure di sicurezza informatica e monitorare, rilevare, relazionare e sistemare le vulnerabilità e gli incidenti di sicurezza

è ottenuto tramite

- Comprendere i requisiti di sicurezza, le vulnerabilità e le minacce
- Gestire l'identità degli utenti e le autorizzazioni in modalità standardizzata
- Testare regolarmente le funzionalità di sicurezza

e viene misurato tramite

- Numero di incidenti che hanno compromesso la reputazione dell'azienda presso il pubblico
- Numero di sistemi dove i requisiti di sicurezza non sono soddisfatti
- Numero di violazioni relative alla segregazione delle funzioni



OBIETTIVI DI CONTROLLO

DS5 Garantire la sicurezza dei sistemi

DS5.1 Gestione della sicurezza IT

Gestire la sicurezza IT al più alto livello aziendale appropriato, così che la gestione degli interventi di sicurezza sia in linea con i fabbisogni aziendali

DS5.2 Piano di sicurezza IT

Tradurre le esigenze aziendali di business, di rischio e di conformità in un piano generale di sicurezza IT, tenendo in considerazione l'infrastruttura IT e la cultura della sicurezza. Assicurarsi che il piano sia realizzato attraverso politiche e procedure di sicurezza insieme ad appropriati investimenti in servizi, personale, software e hardware. Comunicare le politiche e le procedure di sicurezza agli stakeholder e agli utenti.

DS5.3 Gestione delle Identità

Assicurare che tutti gli utenti (interni, esterni o temporanei) e le loro attività sui sistemi IT (applicazioni aziendali, sistemi operativi, sviluppo e manutenzione) siano identificati in modo univoco. Abilitare le identità degli utenti attraverso meccanismi di autenticazione. Assicurare che i diritti di accesso ai sistemi ed ai dati siano in linea con le necessità aziendali, definite e documentate, e le esigenze di lavoro siano coerenti all'identità degli utenti. Assicurarsi che i diritti di accesso siano richiesti dalla Direzione Utente, approvati dal proprietario del sistema e implementati dalla persona responsabile della sicurezza. Mantenere gli identificativi utente e i diritti di accesso in modo centralizzato. Sviluppare tecniche operative e procedure economicamente giustificate e mantenerle aggiornate per definire l'identificazione degli utenti, l'implementazione dell'autenticazione e l'applicazione dei diritti di accesso.

DS5.4 Gestione degli identificativi degli utenti.

Stabilire delle regole per la richiesta, la definizione, il rilascio, la sospensione, la modifica e la revoca degli identificativi utente ed i relativi privilegi attraverso un insieme di procedure per la gestione degli identificativi utente, compresa una procedura di approvazione e concessione dei privilegi di accesso basata sul proprietario dei dati o dei sistemi. Queste procedure dovrebbero essere applicata per tutti gli utenti, inclusi gli amministratori (utenti privilegiati), utenti interni ed esterni, sia per i casi normali sia di emergenza. Diritti e obblighi relativi agli accessi alle informazioni e ai sistemi aziendali dovrebbero essere stabiliti contrattualmente per tutti i tipi di utente. Eseguire una sistematica revisione di tutti gli identificativi ed i relativi privilegi.

DS5.5 Verifica, sorveglianza e monitoraggio della sicurezza

Testare e controllare in modo proattivo l'implementazione della sicurezza IT. La sicurezza IT dovrebbe essere riaccreditata periodicamente per assicurare il mantenimento del livello della sicurezza delle informazioni approvato per l'azienda. Esiste una funzione di registrazione e monitoraggio che consente una rapida prevenzione e/o rilevazione, e conseguentemente una pronta rendicontazione di attività non usuali e/o anormali che potrebbe essere necessario trattare.

DS5.6 Definizione degli incidenti di sicurezza

Definire chiaramente e comunicare le caratteristiche dei potenziali incidenti sulla sicurezza così che possano essere correttamente classificati e trattati dal processo di gestione dei problemi e degli incidenti.

DS5.7 Protezione della tecnologia sulla sicurezza

Rendere la tecnologia collegata alla sicurezza resistente alle manomissioni e non divulgare inutilmente la documentazione sulla sicurezza.

DS5.8 Gestione delle chiavi crittografiche

Verificare che siano definite e messe in atto politiche e procedure per organizzare la generazione, modifica, revoca, distruzione, distribuzione, certificazione, memorizzazione, immissione, uso e archiviazione delle chiavi crittografiche per assicurare la protezione delle chiavi da modifiche e da divulgazioni non autorizzate.

DS5.9 Prevenzione, rilevazione e correzione del software malevolo

Mettere in atto misure preventive, di rilevazione e correzione (specialmente l'aggiornamento delle patch di sicurezza e il controllo dei virus) presso tutta l'organizzazione per proteggere i sistemi informativi e le tecnologie da malware (ad esempio virus, worms, spyware, spam).

DS5.10 Sicurezza della Rete

Utilizzare le tecniche di sicurezza e le relative procedure di gestione (e.g. firewalls, dispositivi di sicurezza, segmentazione della rete e rilevazione delle intrusioni) per autorizzare l'accesso ed il controllo del flusso di informazioni da e per la rete.

DS5.11 Scambio di dati sensibili

Effettuare le transazioni con dati sensibili solo su percorsi di fiducia o ambienti controllati per assicurare l'autenticità del contenuto, la dimostrazione di chi ha avviato la transazione e di chi l'ha ricevuta, e il non ripudio da parte del mittente

Pagina intenzionalmente vuota

LINEE GUIDA PER LA GESTIONE

DS5 Garantire la sicurezza dei sistemi

Da	Inputs
PO2	Architettura delle informazioni; classificazione assegnata ai dati
PO3	Standard tecnologici
PO9	Valutazione dei rischi
AI2	Specifiche su controlli di sicurezza alle applicazioni
DS1	OLA

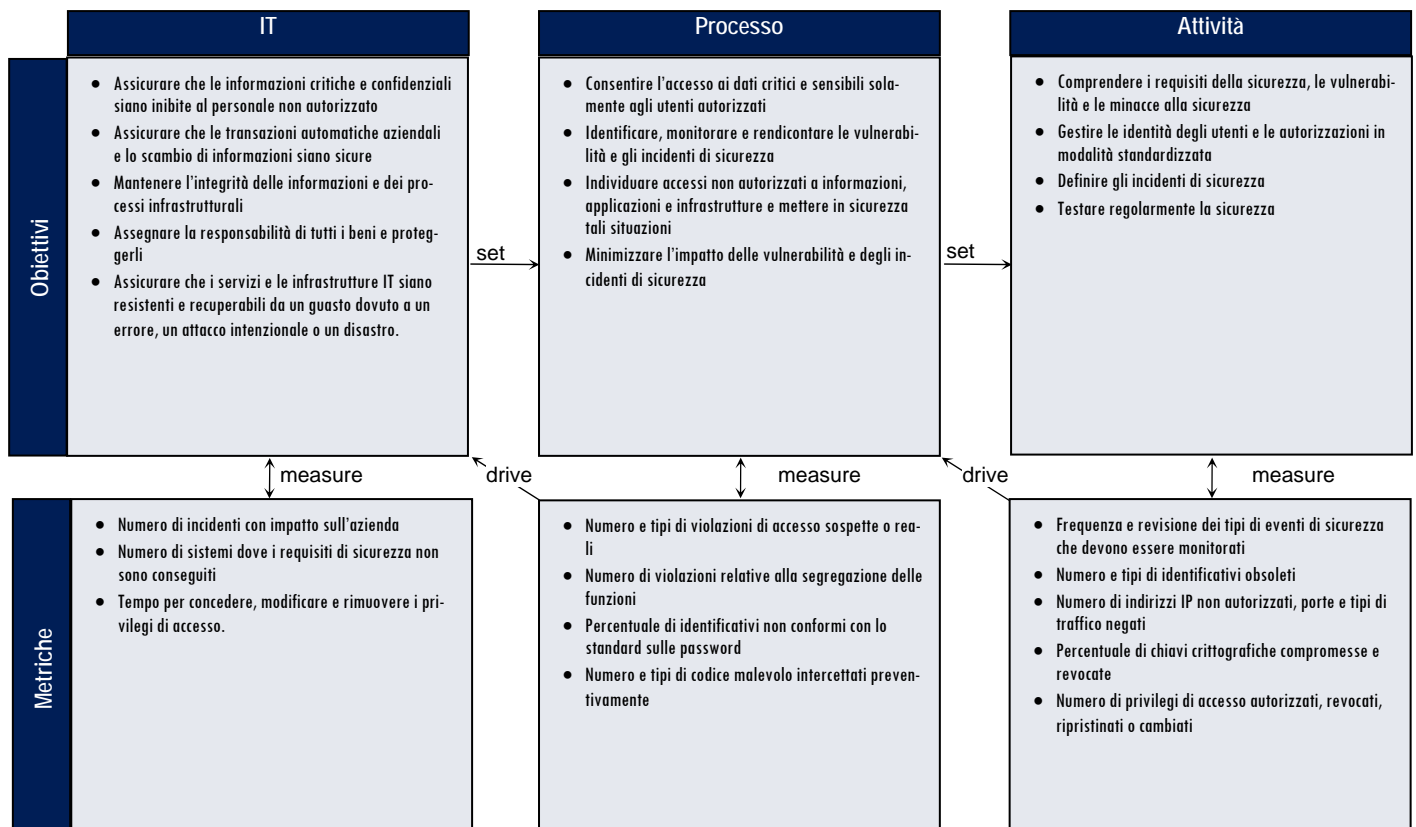
Outputs	a
Definizione degli incidenti di sicurezza	DS8
Requisiti di formazione specifica sulla consapevolezza della sicurezza	DS7
Relazione sulle prestazioni dei processi	ME1
Cambiamenti richiesti sulla sicurezza	AI6
Minacce e vulnerabilità alla sicurezza	PO9
Piani e politiche di sicurezza IT	DS11

RACI Chart

Ruoli

Attività	Anm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architettura IT	Responsabile sviluppo IT	PMO	Conformità, audit, rischio e sicurezza
Definire e aggiornare un piano di sicurezza IT	I	C	C	A	C	C	C	C	I	R
Definire, stabilire e rendere operativo un processo di gestione degli identificativi (account)			I	A	C	R	R	I		C
Monitorare i potenziali e reali incidenti sulla sicurezza				A	I	R	C	C		R
Periodicamente revisionare e convalidare i diritti di accesso e i privilegi degli utenti				I	A	C				R
Definire e aggiornare una procedura per gestire e salvaguardare le chiavi crittografiche				A		R		I		C
Implementare e aggiornare le tecniche e i controlli procedurali per proteggere il flusso di informazioni attraverso la rete				A	C	C	R	R		C
Condurre una regolare valutazione delle vulnerabilità		I		A	I	C	C	C		R

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

DS5 Garantire la sicurezza dei sistemi

Il grado di strutturazione del processo *Garantire la sicurezza dei sistemi* che soddisfa i requisiti aziendali per l'IT di *salvaguardare l'integrità delle informazioni e dei processi infrastrutturali, minimizzare l'impatto derivante da vulnerabilità e da incidenti* è:

0 Non esistente quando

L'azienda non ravvisa la necessità di sicurezza IT. Non sono assegnate le responsabilità per garantire la sicurezza. Non sono implementate misure di supporto per la gestione della sicurezza IT. Non sono previsti report per la sicurezza IT e non ci sono processi di risposta alle falle sulla sicurezza dell'IT. C'è una completa carenza del processo di amministrazione della sicurezza.

1 Iniziale / ad hoc quando

L'organizzazione riconosce la necessità della sicurezza IT. La consapevolezza della sicurezza dipende principalmente dal singolo. La sicurezza IT è indirizzata su base reattiva. La sicurezza IT non viene misurata. Le falle alla sicurezza IT rilevate scatenano la ricerca di un singolo 'colpevole', perché le responsabilità non sono chiare. Le risposte alle falle sulla sicurezza IT sono imprevedibili.

2 Ripetibile ma intuitivo quando

Le responsabilità per la sicurezza IT sono assegnate a un coordinatore senza autorità direttiva e il coordinamento è limitato. La consapevolezza sulla necessità di sicurezza è limitata e frammentaria. Tuttavia le informazioni rilevanti sulla sicurezza IT sono prodotte dai sistemi ma non vengono analizzate. I servizi di terze parti potrebbero non essere indirizzati verso le necessità di sicurezza dell'organizzazione. Si stanno sviluppando delle politiche di sicurezza ma competenze e strumenti sono inadeguati. I report sulla sicurezza IT risultano incompleti, fuorvianti o non pertinenti. È disponibile la formazione per la sicurezza ma intrapresa principalmente su iniziativa individuale. La sicurezza IT è principalmente vista come responsabilità e dominio dell'IT e l'azienda non vede la sicurezza IT all'interno del suo dominio.

3 Definito quando

Esiste una consapevolezza della sicurezza ed è promossa dalla Direzione. Le procedure per la sicurezza IT sono definite e allineate con le politiche di sicurezza IT. Le responsabilità per la sicurezza IT sono assegnate e comprese, ma non sono applicate in modo coerente. Un piano per la sicurezza IT e le soluzioni di sicurezza esistono e sono guidate dall'analisi del rischio. Il reporting sulla sicurezza non è chiaramente focalizzato sull'azienda. Vengono realizzate prove di intrusione ad hoc (es. test di intrusione). La formazione sulla sicurezza è disponibile per l'IT e l'azienda ma è programmata e gestita solo in modo informale.

4 Gestito e misurabile quando

Le responsabilità per la sicurezza IT sono chiaramente assegnate, gestite e applicate. L'analisi del rischio e l'analisi dell'impatto sono opportunamente eseguite. Le politiche e le prassi di sicurezza sono complete con specifici principi di base. L'applicazione di metodi per promuovere la consapevolezza della sicurezza è obbligatoria.

L'identificazione, l'autenticazione e l'autorizzazione dell'utente sono standardizzate. La certificazione della sicurezza è perseguita dallo staff che è responsabile del controllo e della gestione della sicurezza. I test sulla sicurezza sono portati a termine usando processi standard e formalizzati, orientati al miglioramento del livello di sicurezza. I processi della sicurezza IT sono coordinati con la funzione di sicurezza globale dell'organizzazione. Il reporting sulla sicurezza IT è collegato agli obiettivi aziendali. La formazione sulla sicurezza IT è condotta sia sull'azienda che sull'IT. La formazione della sicurezza IT è pianificata e gestita in modo tale da rispondere alle necessità aziendali e ai profili definiti di rischio sulla sicurezza. Gli obiettivi e le metriche per la gestione della sicurezza sono stati definiti ma non ancora misurati.

5 Ottimizzato quando

La sicurezza IT è responsabilità congiunta della Direzione aziendale e di quella IT ed è integrata con gli obiettivi di gestione della sicurezza aziendale. I requisiti della sicurezza IT sono chiaramente definiti, ottimizzati e inclusi in un piano approvato di sicurezza. Gli utenti e i clienti sono sempre più responsabilizzati nella definizione dei requisiti di sicurezza e le funzioni di sicurezza sono integrate con le applicazioni durante le fasi di progettazione. Gli incidenti di sicurezza sono prontamente affrontati con procedure formalizzate di risposta agli incidenti, supportate da strumenti automatici. Accertamenti periodici della sicurezza sono condotti per valutare l'efficacia del piano di sicurezza implementato. Le informazioni sulle minacce e sulle vulnerabilità vengono sistematicamente raccolte e analizzate. Adeguati controlli per mitigare i rischi sono prontamente comunicati e implementati. Test di sicurezza, analisi delle cause degli incidenti relativi alla sicurezza e una proattiva identificazione del rischio sono usati nel processo di miglioramento continuo. I processi e le tecnologie relative alla sicurezza sono integrati nell'organizzazione in modo esteso. Le metriche per la gestione della sicurezza sono raccolte e comunicate. All'interno di un processo di miglioramento continuo, la Direzione usa tali misure per correggere il piano di sicurezza.