



1.1 ITIL e la gestione dei servizi IT

In un mercato in cui il successo delle aziende è in buona parte determinato dalla possibilità di disporre di un'infrastruttura **IT (Information Technology)** realmente funzionale, la capacità di gestione dei servizi IT (**ITSM, IT Service Management**) è sempre più spesso messa a dura prova. Una gestione efficiente dei servizi IT è basata su un sistema strutturato che si avvale delle **best practices** del settore per l'integrazione delle tre componenti dell'ambiente IT: **persone, processi e tecnologie**. Una definizione non sufficientemente chiara di processi IT, ruoli, regole e parametri di valutazione dei servizi rischierebbe infatti di limitare in modo drastico i livelli di efficienza e produttività.

ITIL è il **framework** che più si identifica con l'ITSM (e con il quale è spesso confuso). Esso è un insieme di best practices, quindi di linee guida ispirate dalla pratica, non teoriche, nella gestione dei servizi IT. Consiste in una serie di pubblicazioni che forniscono indicazione sull'erogazione di servizi IT di qualità e sui processi e mezzi necessari a supportarli, schematizzando processi di riferimento per strutturare le attività di IT e le interazioni dello staff di IT con i clienti e gli utenti.

Secondo ITIL i tre obiettivi dell'IT Service Management sono i seguenti:

- allineare i servizi IT con i bisogni correnti e futuri del business e dei clienti;
- migliorare la qualità dei servizi IT erogati;
- ridurre i costi fissi di erogazione dei servizi.

La filosofia ITIL adotta un approccio orientato ai processi, che quindi si può utilizzare indifferentemente in organizzazioni grandi o piccole. L'adozione di ITIL conduce ad un approccio sistematico e professionale nella gestione dei servizi IT, che quindi porta con sé diversi benefici:

- costi ridotti;
- miglioramento dei servizi IT mediante l'uso di best practice provate e diffuse;
- miglioramento della soddisfazione dei clienti in seguito all'approccio più professionale nell'erogazione dei servizi;
- miglioramento della produttività;
- migliore utilizzo di competenze ed esperienza;
- miglioramento nell'erogazione dei servizi di terze parti mediante gli standard per la gestione dei servizi in appalto.

ITIL si evolve sin dal 1989, anno in cui le prime pubblicazioni furono rilasciate da un'agenzia del governo britannico per l'uso negli uffici della propria pubblica amministrazione. È stato in seguito globalmente accettato dalle industrie IT come standard de facto per la gestione dei servizi informatici (rivolti sia a clienti finali, sia a utenti interni). È quindi stato adottato da centinaia di aziende ed organizzazioni in tutto il mondo (fra cui, ad esempio: Microsoft, IBM, Barclays Bank, HSBC, British Airways, Hewlett Packard). Attualmente ITIL è arrivato alla sua terza versione (ITIL v3), i cui volumi sono stati pubblicati nel Giugno 2007.

1.2 Cenni a ITIL v1

Il concetto di ITIL è nato negli anni '80, quando il governo britannico ritenne che la qualità dei servizi IT della pubblica amministrazione non era sufficiente. Per ovviare al problema, la Central Computer and Telecommunication Agency (CCTA), oggi chiamata Office of Government Commerce (OGC), fu incaricata di occuparsi di sviluppare delle linee guida per un uso delle risorse IT efficiente e finanziariamente "responsabile".

Quella da tutti chiamata ITIL v1, non fu altro che la prima versione di queste linee guida. Fu intitolata "Government Information Technology Infrastructure Method" (GITM) e negli anni si è espansa fino a 31 volumi. Naturalmente questa versione era abbastanza diversa dall'ITIL odierno, anche se concettualmente si avvicinava molto, e si concentrava, non in modo diretto, sulle due fasi di supporto e fornitura di servizi informatici.

Molti dei principali concetti sulla gestione del servizio non erano stati creati all'interno del progetto originale del CCTA che sviluppava ITIL, infatti IBM rivendica che i suoi "Yellow Books" ("A Management System for the Information Business") ne siano stati un precursore. Alcune pubblicazioni IBM e commenti degli stessi autori di ITIL hanno chiarito che i "Yellow Books" diedero un significativo contributo alla parte di Service Support di ITIL mentre il volume sul Service Delivery non ne era stato influenzato nella stessa misura.

Durante gli anni '80 la diffusione di ITIL rimase parzialmente limitata alla Gran Bretagna ed agli addetti ai lavori; il vero boom iniziò a metà degli anni '90, quando molte grandi aziende ne iniziarono l'adozione.

1.3 Il framework ITIL v2

L'aumento esponenziale in ITIL v1 del numero di volumi pubblicati (i quali ricoprivano ognuno una specifica pratica all'interno della gestione dei servizi IT) rese ITIL non più accessibile (ed abbordabile) a coloro che desideravano esplorarlo. Una delle aspirazioni del progetto per la seconda versione (ITIL v2) fu proprio quella di consolidare i lavori in insiemi logici in grado di raggruppare le linee guida correlate nei diversi aspetti della gestione dei sistemi, delle applicazioni e dei servizi IT.

La principale caratteristica della seconda versione di ITIL è stata pertanto la netta suddivisione dei processi di gestione dei servizi IT in alcune aree principali, presentate in una collezione di 8 volumi:

- l'area **Service Support** (supporto ai servizi IT);
- l'area **Service Delivery** (fornitura dei servizi IT);
- l'area **ICT Infrastructure Management** (gestione dell'infrastruttura IT);
- l'area **Security Management** (gestione della sicurezza);
- l'area **The Business Perspective** (la prospettiva aziendale);
- l'area **Application Management** (gestione delle applicazioni);
- l'area **Software Asset Management** (gestione del software);
- l'area **Planning to Implement Service Management** (pianificazione per sviluppare la gestione dei servizi).

Dei volumi elencati, i primi due sono stati sostanzialmente i più seguiti e studiati: non a caso sono comunemente indicati mediante il colore delle copertine (“Blue Book” per il volume sul Service Support, “Red Book” per quello sul Service Delivery).

Service Support

La parte di Service Support di ITIL si occupa della gestione giornaliera delle attività di IT Service Management. Essa è focalizzata soprattutto sugli utenti dei servizi IT, con l'obiettivo di garantire flessibilità e stabilità nell'accesso ai servizi appropriati che supportano il business aziendale. Gli utenti considerati sono quelli interni, appartenenti cioè all'organizzazione o dipartimento IT, e quelli esterni, cioè i clienti (altri dipartimenti dell'azienda o clienti esterni veri e propri).

Il Service Support definisce e indirizza i seguenti processi:

- **Service Desk;**
- **Incident Management;**
- **Problem Management;**
- **Change Management;**
- **Release Management;**
- **Configuration Management.**

Service Desk

L'interfaccia unica (*single point of contact*) verso gli utenti per tutti i servizi IT è costituita dal **Service Desk**. Il Service Desk segue sia le chiamate da clienti esterni, sia le chiamate che hanno avuto origine all'interno dell'organizzazione o dipartimento IT. È da esso che partono le richieste di supporto da parte degli utenti:

- richieste di modifiche;
- necessità di aggiornamenti;
- segnalazioni di difficoltà o problemi.

In generale il Service Desk ha quindi a che fare con il concetto di **incidente**. In ITIL il termine **incident** (incidente) indica un qualunque evento che non fa parte delle operazioni standard di un servizio e che causa, o potrebbe causare, un'interruzione o un peggioramento della qualità del servizio stesso. In particolare viene usata una definizione larga di incidente, così che tutte le chiamate possano essere considerate incidenti: in tal modo anche le richieste di servizi o aggiornamenti (*Service Requests*) sono considerate incidenti.

I Service Desk tradizionali (*Call Center* e *Help Desk*) tendono a essere non strutturati: spesso supportano solo parte dei servizi IT e molte volte non sono responsabili di tutto il ciclo di vita degli incidenti (che possono essere passati ad altri gruppi, in seguito a valutazioni errate della criticità). Con ITIL invece gli obiettivi del Service Desk sono quelli di:

- porsi come l'interfaccia unica con gli utenti per tutti i servizi IT;
- fornire risposte più veloci e di miglior qualità;
- migliorare la gestione dell'infrastruttura e controllo;
- utilizzare meglio le risorse di supporto all'IT e aumentare la produttività del personale;
- utilizzare maggiore informazione significativa per le decisioni;
- gestire tutto il ciclo di vita dell'incidente o della richiesta.

Di conseguenza il Service Desk ha racchiuso in sé il compito di ridurre il carico di lavoro degli altri dipartimenti IT, eliminando le interruzioni portate da questioni irrilevanti o a cui è facile rispondere. Il Service Desk agisce quindi come filtro, lasciando passare le chiamate alla seconda e terza linea di supporto solo quando è necessario. In più costituisce un ottimo strumento sia per mantenere i contatti con gli utenti (interni ed esterni) che per monitorare la soddisfazione del cliente.

Il Service Desk ha a che fare per sua natura con diverse attività degli altri processi ITIL:

- il processo di Incident Management, che controlla come una parte degli incidenti vengano registrati e monitorati dal Service Desk, includendo il coordinamento delle attività di terze parti coinvolte nella gestione dell'incidente;
- i processi di Release Management e Change Management, se coinvolto durante l'installazione di software o hardware;
- il processo di Configuration Management, se, quando si registra un incidente, il Service Desk verifica i dettagli del chiamante e le loro risorse IT;
- il processo di Service Level Management, appartenente all'area Service Delivery, nel caso il Service Desk non sia autorizzato ad accogliere una richiesta o incidente.

Gli obiettivi del Service Desk sono raggiunti tramite l'implementazione delle sue funzioni più comuni, che includono:

- ricezione delle chiamate (per la segnalazione di richieste o incidenti);
- tenere traccia degli incidenti segnalati (registrazione e classificazione);
- definire le priorità degli incidenti;
- effettuare attività di comunicazione per gli altri processi ITIL coinvolti;
- tenere informati gli utenti interessati dello stato e progresso delle segnalazioni;
- monitorare il processo di evasione della richiesta di supporto, rispettando le **SLA (Service Level Agreement)**;
- riferire al Management, ai manager del processo e agli utenti sulle performance del Service Desk.

In generale sono diversi i benefici portati dall'introduzione di un Service Desk secondo il framework ITIL:

- miglior servizio agli utenti finali;
- miglior accessibilità al servizio (un Service Desk unico per tutti i servizi IT);
- migliore comunicazione interna nel dipartimento IT e con gli utenti;
- maggiore focalizzazione sulle esigenze degli utenti;
- migliore comprensione delle dinamiche di supporto (ed una maggiore comprensione degli impatti);
- maggiore produttività delle risorse umane;

Incident Management

L'obiettivo del processo di **Incident Management**, secondo i documenti ufficiali di ITIL, è di ripristinare le operazioni normali di servizio il più velocemente possibile con la minima interruzione di servizio, assicurando che i migliori livelli di servizio e disponibilità siano mantenuti. Per questo gli incidenti vengono registrati, classificati e assegnati agli specialisti appropriati, il progresso dell'incidente viene monitorato, e gli incidenti risolti vengono chiusi. Di conseguenza l'Incident Management diventa essenziale per gli altri processi ITIL anche come fornitore di informazioni sugli errori dell'infrastruttura.

È ovvio che esiste una forte relazione tra il processo di Incident Management e il Service Desk: è da quest'ultimo che arrivano le richieste di supporto, ovvero gli incidenti. Può inoltre essere coinvolto anche il processo di Change Management nel caso la risoluzione di un incidente richieda la modifica dell'infrastruttura (l'incidente si traduce in una **RFC, Request For Change**). Infine è necessario per ciascun incidente informare il processo di Problem Management della presenza di un nuovo *problema* (la causa ignota alla base dell'incidente).

Dato che possono essere trattati più incidenti allo stesso tempo, diventa fondamentale implementare un meccanismo di **priorità**, per determinare l'ordine nel quale gli incidenti devono essere risolti. Innanzitutto esiste una discriminazione tra incidenti veri e propri e richieste di servizio (Service Requests), che può incidere in modo più o meno importante sulle priorità assegnate. L'assegnazione delle priorità è effettuata dal Service Desk, in consultazione con l'utente e in accordo con le SLA. Per una definizione obiettiva della priorità devono essere discussi con l'utente i seguenti criteri:

- **impatto** dell'incidente, cioè l'estensione delle deviazioni dal normale livello di servizio (in termini di numero di utenti e/o processi di business coinvolti);
- **urgenza** dell'incidente, cioè il ritardo accettabile dall'utente e/o dal processo di business.

La priorità è pertanto determinata sulla base dell'urgenza e dell'impatto, e per ciascuna priorità si assegna una certa quantità di risorse. Nel caso di incidenti con la stessa priorità, l'ordine può essere determinato in base allo sforzo richiesto: potrebbe essere data la precedenza a incidenti facilmente risolvibili. La priorità potrà essere ovviamente modificata, ad esempio nel caso di passaggio dell'incidente a un livello diverso di supporto oppure di variazioni nell'impatto o nell'urgenza.

Gli incidenti sono trattati mediante un meccanismo ad **escalation**: se un incidente non può essere risolto nel livello di supporto corrente, allora dovranno essere assegnate nuove risorse. L'assegnazione di nuove risorse può essere effettuata in due modi:

- escalation **funzionale** (orizzontale), con la permanenza nello stesso livello di supporto ma con il coinvolgimento di nuovo personale e/o risorse per risolvere l'incidente;
- escalation **gerarchica** (verticale), cioè il passaggio ad un livello di supporto più alto.

L'Incident Management ha il compito e obiettivo di riservare in anticipo la capacità per un'escalation funzionale, in modo da cercare di evitare un'escalation gerarchica. In generale il supporto di *first-line* (conosciuto anche come *tier-1*) è offerto dal Service Desk stesso, il *second-line* attraverso i dipartimenti di gestione, il *third-line* dagli sviluppatori di software e il *fourth-line* dai fornitori.

Il processo di Incident Management implica quindi una serie di attività da eseguire:

- individuazione dell'incidente e registrazione;
- classificazione dell'incidente e supporto iniziale (identificazione delle cause, assegnazione priorità, segnalazione al Problem Management);
- analisi e diagnosi dell'incidente;
- soluzione e ripristino;
- chiusura dell'incidente;
- classificazione dell'appartenenza dell'incidente (**ownership**), monitoraggio e gestione della comunicazione.

Tutti i punti sono sequenziali, ad eccezione dell'ultimo che deve essere svolto durante l'intero ciclo di vita del processo.

Si possono individuare alcuni benefici relativi all'introduzione del Service Management:

- minore impatto degli incidenti a cause di una più veloce risoluzione;
- identificazione proattiva di possibili miglioramenti all'infrastruttura;
- disponibilità di informazione significativa per poter redigere e valutare i livelli di servizio;
- migliore utilizzazione dello staff;
- eliminazione di incidenti persi;
- aumento della soddisfazione di clienti e utenti;
- meno interruzioni sul lavoro sia allo staff IT che agli utenti.

Problem Management

L'obiettivo del processo di Incident Management è quello di intraprendere le necessarie misure in caso di un incidente, fermando le sue attività dopo avere completato il ripristino delle operazioni normali di servizio. Ciò significa che non sempre la causa dell'incidente viene scoperta, e quindi l'incidente potrebbe in futuro accadere nuovamente. È qui che entra in gioco il processo di **Problem Management**: il suo compito è di analizzare l'infrastruttura e le registrazioni degli incidenti (l'*Incident Database*) per identificare le **cause** degli attuali e dei potenziali errori nella fornitura dei servizi. Un **problema** è pertanto la causa sconosciuta e sottostante (errore sconosciuto) di uno o più incidenti esistenti o potenziali, è rappresenta perciò una situazione non desiderabile.

Il Problem Management ha ovviamente bisogno di un processo di Incident Management ben implementato che fornisca gli input di cui ha bisogno (cioè gli incidenti) in forma strutturata ed analizzabile. D'altra parte la differenza con l'Incident Management è evidente. Mentre l'Incident Management è focalizzato all'utente, il Problem Management è focalizzato all'infrastruttura nel lungo termine. Nel primo caso l'obiettivo è ripristinare (spesso con correzioni temporanee) il servizio il più velocemente possibile. Nel secondo caso l'obiettivo è individuare le cause degli incidenti e trovare soluzioni permanenti, riservando più importanza alla risoluzione dei problemi piuttosto che alla rapidità

L'identificazione delle cause può essere più o meno complicata, a seconda delle caratteristiche dell'infrastruttura, che può essere complessa e distribuita, e delle relazioni fra gli incidenti, che potrebbero non essere ovvie. In ogni caso, una volta che la causa sottostante è stata determinata, il problema diventa un **errore conosciuto (known error)**. Il Problem Management tiene traccia di tutte le informazioni relative agli errori conosciuti mediante un apposito database (**KeDB, Known error Database**). A questo punto si potrebbe emettere una *Request For Change* (RFC), ossia una richiesta di modifica all'infrastruttura per eliminare l'errore.

Come tutti gli altri processi, anche il Problem Management è caratterizzato da alcune fasi principali:

- il controllo del problema, cioè l'identificazione delle cause principali che hanno provocato il problema;
- il controllo dell'errore, cioè l'identificazione degli errori e la conseguente modifica all'infrastruttura al fine da evitare il ripresentarsi degli incidenti associati al problema.
- la prevenzione dei problemi, cioè l'identificazione dei problemi prima che generino incidenti (il cosiddetto Problem Management pro-attivo).

I benefici del Problem Management sono i seguenti:

- miglioramento della qualità del servizio IT;
- riduzione del volume degli incidenti e prevenzione;
- risoluzione permanente dei problemi;
- possibilità di creare documentazione sulle soluzioni temporanee per gli errori;

Change Management

Il processo di **Change Management** mira a gestire i cambiamenti apportati all'infrastruttura IT, limitando di conseguenza gli incidenti provocati dai cambiamenti stessi. Al giorno d'oggi, infatti, il rapido sviluppo della tecnologia IT e del mercato porta alla necessità di cambiamenti e modifiche alle infrastrutture di organizzazioni o dipartimenti IT. Perciò, gli incidenti che interessano l'infrastruttura IT sono spesso correlati o addirittura provocati dai cambiamenti. Le cause sono molteplici: ad esempio mancanza di risorse,

preparazione insufficiente, analisi errate degli impatti sull'infrastruttura o problemi di testing. Se non esistesse un'adeguata gestione dei cambiamenti, l'infrastruttura IT rischierebbe di cadere in un ciclo senza controllo, con l'introduzione di ulteriori cambiamenti per correggere errori provocati da cambiamenti precedenti: ciò contribuirebbe a far crescere sempre più il numero di incidenti.

L'obiettivo del Change Management è di assicurare che siano usati i metodi e le procedure standard e allo stesso tempo che i cambiamenti vengano condotti velocemente, con il minor impatto sull'infrastruttura (in termini di qualità del servizio). Inoltre deve essere consentita la rintracciabilità dei cambiamenti apportati, in modo che risulti facile capire cosa si è modificato.

Per l'implementazione del Change Management è necessario svolgere le seguenti attività:

- filtraggio e accettazione dei cambiamenti, che analizza l'infrastruttura e riconosce i cambiamenti da mettere in atto;
- valutazione dell'impatto e della risorsa, che esamina l'impatto del cambiamento sull'organizzazione e sull'infrastruttura, effettua uno studio di costi, benefici e rischi, e analizza le risorse necessarie per effettuare il cambiamento;
- approvazione del cambiamento;
- programmazione del cambiamento (se approvato);
- implementazione del cambiamento (se approvato).

Prima ancora di essere filtrato e accettato, ogni cambiamento deve essere opportunamente registrato e descritto in una RFC. Il processo di autorizzazione di ogni RFC deve essere effettuato da un comitato che abbia il giusto livello di autorità, secondo il cambiamento previsto. Normalmente le decisioni sono prese dal **Change Advisory Board (CAB)** che può includere:

- il *Change Manager* (il proprietario del processo di Change Management);
- lo staff IT dell'area interessata dal cambiamento;
- utenti interni e/o esterni;
- fornitori;
- esperti e tecnici.

Tuttavia esistono dei cambiamenti che non devono seguire il normale iter di approvazione. Si distinguono infatti degli **standard changes**, che prevedono un'approvazione automatica e che si adattano a cambiamenti molto comuni e ripetitivi (ad esempio la creazione di account) e **model changes**, che prevedono modalità specifiche e/o semplificate che meglio si adattano al tipo di cambiamento (ad esempio nel caso di *bug fixing*).

L'adozione di un buon processo di Change Management porta diversi benefici:

- riduzione dell'impatto negativo dei cambiamenti sull'infrastruttura e la qualità dei servizi IT;
- migliori stime dei costi dei cambiamenti proposti;
- pochi cambiamenti vengono ripristinati per tornare alla situazione precedente;
- miglioramento della produttività dell'utente attraverso un più stabile e migliore servizio IT;
- incremento dell'abilità di introdurre cambiamenti frequente senza creare un ambiente IT instabile.

Release Management

I cambiamenti all'infrastruttura IT costituiscono la normalità in un ambiente IT complesso e distribuito. Il rilascio e l'implementazione di modifiche deve quindi essere attentamente pianificato. Una **release** (definita nella RFC che la implementa) è un set di nuovi e/o modificati **Configuration Items**, cioè componenti dell'infrastruttura che sono stati testati e introdotti in un ambiente. In particolare un Configuration Item è un'unità di configurazione (elemento dell'infrastruttura IT) che può essere gestita individualmente. Un

insieme di Configuration Item include in genere: computer, software, componenti attivi e passivi di rete, server, router, processori centrali, documentazione, procedure, servizi e tutti gli altri componenti IT che devono essere controllati.

Il **Release Management** indirizza ad un approccio di progetto pianificato per l'implementazione di cambiamenti nell'infrastruttura e servizi IT. Il Release Management assicura inoltre la qualità dell'ambiente di produzione, attraverso l'uso di procedure formali e di verifiche quando si implementano nuove versioni. Il Release Management ha quindi a che fare con l'implementazione dei cambiamenti, a contrario del Change Management che si occupa della verifica e valutazione.

Il Release Management lavora a stretto contatto con il database di gestione delle configurazioni (**CMDB, Configuration Management Database**). Il CMDB è un deposito (*repository*) di informazioni relative a tutti i componenti (i Configuration Item) di un sistema informativo (comprese le relazioni tra essi): nel contesto ITIL è la configurazione dei componenti (hardware e software) dell'infrastruttura IT e le relazioni fra loro. L'obiettivo del CMDB è quello di tenere traccia delle relazioni tra i componenti e della loro configurazione: ciò avviene per ogni Configuration Items mediante descrizioni tecniche e attributi di appartenenza e di relazioni con altri Items. Per assicurare che il comune CMDB sia aggiornato con ogni rilascio, il Release Management deve interfacciarsi in modo opportuno con i processi di Change Management e di Configuration Management. Infatti, una delle poche raccomandazioni di ITIL in termini di priorità di implementazione dei processi è quello di implementare i processi di Configuration, Change e Release Management insieme, e possibilmente di avere una funzione centralizzata per gestirli.

Il Release Management, oltre che con il CMDB, deve poi lavorare con altre due componenti:

- la **Definitive Software Library (DSL)**, che contiene tutte le copie master (originali) di tutti i software in produzione, utilizzata e/o aggiornata con ogni release;
- la **Definitive Hardware Store (DHS)**, un'area dove vengono mantenuti i ricambi per l'hardware; le parti del DHS devono essere tracciate nel CMDB e mantenute allo stesso livello dell'hardware in produzione.

È quindi possibile dare un elenco degli obiettivi del Release Management:

- pianificare, coordinare e implementare software e hardware;
- progettare e implementare procedure efficienti per effettuare cambiamenti all'infrastruttura IT;
- assicurare che l'hardware e il software relativo ai cambiamenti sia tracciabile (via CMDB, DSL e DHS) e sicuro, e che vengano installate solo versioni corrette, autorizzate, e testate;
- comunicare con gli utenti e tenere in considerazione le loro aspettative durante la pianificazione e l'implementazione (*roll-out*) di nuove release;
- determinare la composizione e la pianificazione di un roll-out, collaborando con il Change Management;
- implementare le release di nuovo software e hardware nell'infrastruttura operativa, sotto il controllo del Change Management, e supportati dal Configuration Management;
- assicurare che le copie originali del software siano archiviate nella DSL, che il CMDB sia aggiornato e nel DHS vengano inseriti i ricambi per l'hardware.

Le attività del Release Management possono essere semplicemente riassunte nella figura 1. Esse riguardano:

- disegno e manutenzione delle politiche di release;
- pianificazione delle release;
- design, costruzione e configurazione delle release;
- accettazione delle release;
- pianificazione dell'implementazione;
- testing delle release;

- comunicazione e training sulla nuova release;
- valutazione dell'hardware e del software della release (prima e dopo l'implementazione);
- manutenzione di copie di sicurezza del software utilizzato;
- rilascio, distribuzione ed installazione dell'hardware e/o software delle release.

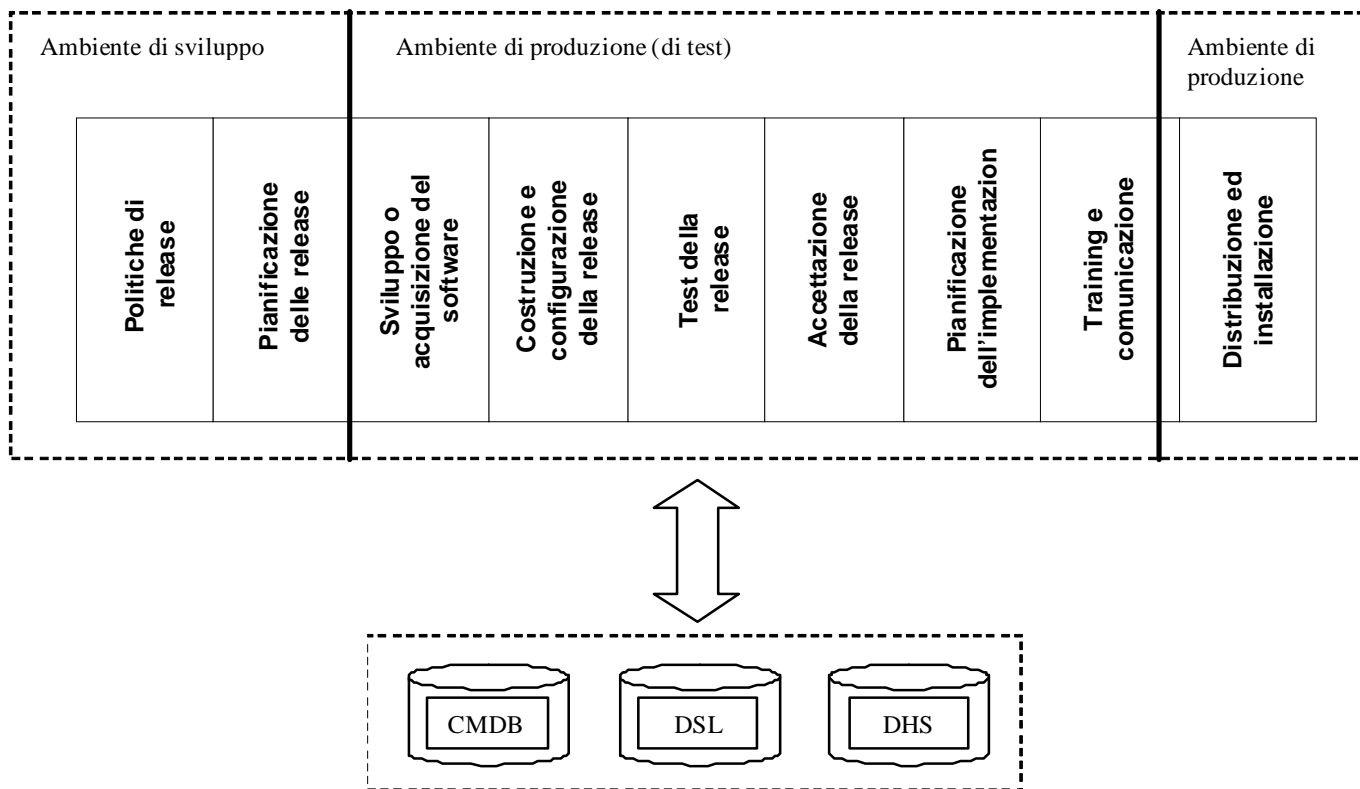


Figura 1: Attività del Release Management

Le release possono essere di tre differenti categorie:

- release del software principale e aggiornamento dell'hardware;
- release di software minore e aggiornamento dell'hardware;
- emergenza del software e miglioramento dell'hardware.

Allo stesso tempo le release possono essere implementate in diversi modi, a seconda della necessità:

- **full release;**
- **delta release;**
- **package release.**

Nella *full release* il vantaggio è che tutti i componenti vengono costruiti, distribuiti e implementati insieme, lo svantaggio è nell'aumento di tempo, sforzo e risorse computazionali. La *delta release* include solo quei Configuration Item all'interno dell'unità di release che sono stati appena modificati o che sono nuovi dall'ultima release. Bisogna decidere quando la delta release è più appropriata e preferibile ad una totale. Infine, se per fornire lunghi periodi di stabilità per l'ambiente attivo si vuole ridurre il numero delle release, si possono raggruppare release individuali per formare un pacchetto. L'utilizzo del *package release* può ridurre la probabilità che software vecchi o incompatibili siano erroneamente tenuti in uso. Può inoltre

incoraggiare le organizzazioni ad assicurare che tutti i cambiamenti che devono essere fatti allo stesso tempo e in diversi sistemi siano fatti effettivamente allo stesso tempo.

I benefici dell'implementare il Release Management includono i seguenti:

- migliore qualità dei servizi rilasciati come risultato di una maggiore percentuale di release con successo;
- miglior utilizzo delle risorse;
- certezza che l'hardware e il software rilasciato in produzione sia di qualità nota, riducendo in tal modo le possibilità che software illegale, errato o non autorizzato sia in uso.

Configuration Management

Ogni organizzazione o dipartimento IT possiede informazione sulla sua infrastruttura e servizi IT: tali informazioni devono però essere tenute aggiornate. Il processo di **Configuration Management** mira a fornire un modello logico dell'infrastruttura attraverso l'identificazione, il controllo, la gestione e la verifica di tutte le versioni di componenti dell'infrastruttura IT, ossia i *Configuration Item*. Inoltre si devono includere anche i dettagli su come i Configuration Item siano connessi l'uno con l'altro. Il Configuration Management verifica quindi se i cambiamenti nell'infrastruttura IT sono stati registrati correttamente, incluse le relazioni fra Configuration Item, e monitora lo stato dei componenti IT, per assicurare che abbia una accurata immagine delle versioni di Configuration Item esistenti. In aggiunta, il Configuration Management può anche essere utilizzato per archiviare e controllare i dettagli sugli utenti, interni e esterni, e sullo staff IT.

Un elemento chiave è naturalmente il CMDB, dove è tenuta traccia di tutti i Configuration Item e delle relazioni fra essi. Un CMDB potrebbe consistere, nella sua forma più basilare, in un insieme di fogli di form o di un set di fogli di calcolo. Tuttavia è fortemente consigliata l'integrazione, con l'uso di database ed eventualmente di tool automatici di monitoraggio dell'infrastruttura.

Il Configuration Management punta quindi ad aiutare la gestione del valore economico dei servizi IT (una combinazione di requisiti del cliente, qualità e costi) attraverso il mantenimento di un modello logico dell'infrastruttura e dei servizi IT, fornendo informazioni su di loro agli altri processi. Gli obiettivi del Configuration Management includono quindi:

- mantenere affidabile la descrizione dei Configuration Item, tracciando i beni appartenenti all'infrastruttura IT;
- fornire accurate informazioni e documentazione per supportare gli altri processi;
- verificare i dati rispetto all'infrastruttura e correggere eventuali discrepanze.

Riveste in particolare una notevole importanza l'interfaccia del Configuration Management verso tutti gli altri processi di Service Support, nei quali esso è spesso coinvolto (ad esempio tramite accessi al CMDB per l'analisi e diagnosi di incidenti e problemi o le necessità di gestione, modifica o inserimento di Configuration Item).

Il Configuration Management persegue i suoi obiettivi mediante una serie di attività e procedure da seguire:

- **pianificazione** del processo di Configuration Management, con la definizione (per il periodo di tempo scelto) di strategie, politiche, obiettivi, ruoli, responsabilità, relazioni con altri processi, attività e procedure;
- **identificazione** delle strutture di configurazione per tutti i Configuration Item e registrazione nel CMDB;

- **controllo** dei Configuration Item per assicurare che solo quelli autorizzati siano presenti nell'infrastruttura e per garantire che nessun Configuration Item venga aggiunto, modificato, rimosso o riposizionato senza l'appropriata documentazione;
- **monitoraggio** dei Configuration Item durante il loro ciclo di vita, mantenendo per ciascuno i dati correnti e storici così da consentire di tenere traccia dei propri stati;
- **verifica** mediante la revisione dei processi di Configuration Management per verificare l'esistenza fisica dei Configuration Item, per verificare che siano correttamente immessi nel CMDB.

In generale l'implementazione e l'utilizzo di un buon processo di Configuration Management consente di:

- fornire informazioni accurate sull'infrastruttura in generale e sui singoli Configuration Item e la relativa documentazione a supporto degli altri processi;
- permettere il tracciamento di componenti di alto valore finanziario;
- contribuire alla pianificazione finanziaria attraverso la quantificazione delle varie risorse afferenti all'infrastruttura IT;
- rendere visibili i cambiamenti al software;
- aiutare a pianificare le release;
- contribuire ad una corretta pianificazione delle esigenze;
- fornire dati di andamento al Problem Management (ad esempio indicando quali sono i componenti coinvolti in più incidenti).

Service Delivery

La parte di Service Delivery di ITIL si occupa della pianificazione di lungo termine della fornitura di servizi IT e del miglioramento degli stessi.

I processi utilizzati a tale scopo sono i seguenti:

- **Service Level Management**
- **Capacity Management;**
- **IT Service Continuity Management;**
- **Availability Management;**
- **Financial Management.**

Service Level Management

Il **Service Level Management** è un processo di gestione della qualità dei servizi IT reso operativo attraverso un ciclo di negoziazione, definizione e gestione dei livelli di servizio e di supporto operativo, che può tradursi in azioni mirate ad eliminare o migliorare i servizi scarsi o mediocri. I livelli di servizio sono documentati nelle **SLA (Service Level Agreement)**, mentre i livelli di supporto operativo sono documentati nelle **OLA (Operational Level Agreement)**.

Gli accordi sul livello di servizio (SLA) sono generalmente stipulati con un contratto tra il fornitore e il cliente, nel quale vi è una descrizione dettagliata e non ambigua del servizio IT e dei suoi componenti, nonché una specifica di come il servizio debba essere erogato per mantenere gli obiettivi concordati. I livelli operativi (OLA), invece, sono accordi, variabili a seconda dei bisogni e delle condizioni, tra i gruppi interni

di supporto (ad esempio il Service Desk), stipulati al fine di garantire la qualità del lavoro (in termini di rispetto delle SLA stipulate).

Ovviamente cliente e fornitore hanno interessi diversi:

- il cliente è incoraggiato a documentare e definire le proprie necessità (inizialmente descritte nei documenti di Service Level Requirement, SLR);
- il fornitore è incoraggiato a focalizzarsi su queste necessità e ad assumersi le responsabilità.

Le attività da eseguire come obiettivo del Service Level Management sono quindi le seguenti:

- produzione, revisione e manutenzione del catalogo dei servizi IT (Service Catalogue);
- quantificazione dei servizi IT;
- definizione degli obiettivi interni ed esterni dei livelli di servizio (negoziazione con i clienti);
- raggiungimenti dei livelli concordati;
- miglioramento con continuità dei livelli di servizio, attraverso programmi specifici (*Service Improvement Program, SIP*);
- revisione degli accordi e dei contratti, per verificare che siano sempre allineati con le necessità.

In generale l'introduzione del Service Level Management può portare i seguenti benefici:

- le incomprensioni tra fornitori di servizi e clienti sono minimizzate, in modo tale che i servizi IT sono progettati in modo mirato a soddisfare le aspettative come definite nelle SLR;
- le performance dei servizi possono essere misurate e valutate;
- diminuzione delle possibilità di rottura dei servizi;
- diminuzione dei tempi e dello sforzo speso dallo staff IT per risolvere i problemi;
- chiarezza delle responsabilità e dei ruoli nell'erogazione di un servizio;
- soddisfazione dei clienti e chiara visione delle aspettative;
- possibilità di usare le SLA come base per la trattativa di tariffazione di un servizio.

Capacity Management

Il processo di **Capacity Management** si pone l'obiettivo di assicurare il miglior utilizzo dell'infrastruttura IT al fine di soddisfare efficacemente le necessità aziendali. Ciò deve avvenire attraverso la comprensione di come i servizi IT verranno utilizzati e correlando le risorse IT (hardware, software, telecomunicazioni) per l'erogazione di questi servizi ai livelli concordati nel processo di Service Level Management.

Il Capacity Management si interessa pertanto della gestione dei servizi da un punto di vista quantitativo. In generale il processo comprende i seguenti elementi:

- comprensione della domanda di servizi attuale e previsione dei bisogni e delle richieste futuri (con la creazione di nuove capacità);
- comprensione di come l'infrastruttura è utilizzata e di come dovrebbe esserlo;
- stabilire le operazioni necessarie che l'azienda deve mettere in atto e prevedere le infrastrutture essenziali;
- capacità di influenzare la domanda di servizi e risorse IT;
- produrre e aggiornare un piano (**Capacity Plan**) che consideri tutte le necessità dell'azienda.

L'implementazione del Capacity Management deve essere in ogni caso allineata con la *business strategy* (strategia aziendale) e con i *business plan* (piani aziendali) a tutti i livelli attraverso tre macro-aree:

- **Business Capacity Management**, relativo all'operatività dell'azienda; si focalizza sulla previsione, modellizzazione, dimensionamento e documentazione dei futuri requisiti aziendali;

- **Service Capacity Management**, relativo ai servizi erogati; si focalizza sulla gestione (con monitoraggio, analisi e ottimizzazione) dei servizi IT erogati;
- **Resource Capacity Management**, relativo alle risorse IT. Si focalizza sulla gestione (con monitoraggio, analisi e ottimizzazione) delle risorse dell'infrastruttura IT.

Per poter gestire correttamente il processo può essere utile implementare e gestire un database, il **Capacity Management Database**, sorgente di tutti i report del Capacity Management. Naturalmente non è necessario che sia un database unico, ma può essere distribuito in più ubicazioni fisiche e può relazionare dati molto diversi ed eterogenei tra loro.

Le attività del Capacity Management, nelle aree di servizi e risorse, sono riassunte nella figura 2. Il monitoraggio consente di verificare in modo continuativo l'utilizzo delle risorse e i livelli dei servizi. In caso di superamento delle soglie stabilite, contestualmente, o in modo sequenziale, il monitoraggio e l'analisi devono produrre delle eccezioni sul livello di servizio (*Service Level Exception*) e sull'utilizzo della risorsa (*Resource Utilization Exception*). La fase di ottimizzazione cercherà di gestire tali eccezioni, con la progettazione di modifiche alle capacità dell'infrastruttura da realizzare poi nella fase di implementazioni. Esempi di superamento di soglie sull'utilizzo delle risorse (che incidono poi sul livello di servizio) possono essere il superamento della soglia di utilizzo di CPU o memoria, o di richiesta di operazioni I/O; l'ottimizzazione potrà ad esempio tradursi in un miglior bilanciamento del lavoro e di traffico sul disco.

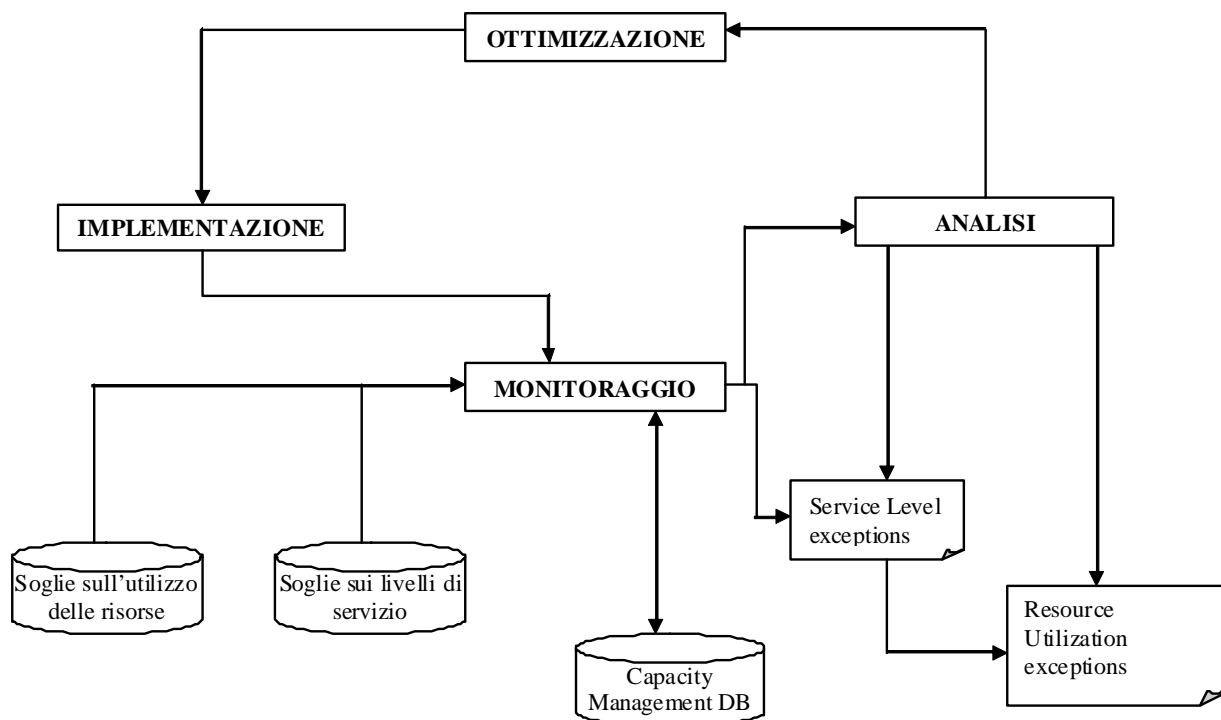


Figura 2: Attività del Capacity Management

I benefici portati dalla corretta implementazione del Capacity Management sono ovvi:

- miglior capacità di mantenere i livelli di servizio concordati;
- miglior utilizzo delle capacità dell'infrastruttura;
- possibilità di anticipare i cambiamenti.

IT Service Continuity Management

Il processo di **IT Service Continuity Management (ITSCM)** ha a che fare con il concetto di **disastro (failing)**. Per disastro si intende un evento che influenza in modo fortemente negativo un servizio o un sistema e che richiede uno sforzo significativo per ripristinare l'originale livello di performance: di conseguenza è molto più serio di un incidente, poiché il più delle volte causa un'interruzione del business (cioè dei servizi offerti). Esistono vari tipi di disastri:

- calamità naturali;
- atti di vandalismo;
- black-out su larga scala;
- guasti hardware;
- errori umani o tecnici;
- frodi, sabotaggi, estorsioni e spionaggio;
- attacchi terroristici;
- virus e attacchi informatici (generalmente attacchi Denial Of Service).

Nel passato il processo di gestione delle emergenze era principalmente reattivo (entrava in azione solo a disastro avvenuto). L'ITSCM cerca invece di intervenire in anticipo, prima che si verifichino i disastri, enfatizzando invece la prevenzione. Per questo l'obiettivo del processo è quello di evitare i rischi identificati e di pianificare (con piani di continuità, **Business Continuity Plan**) in anticipo il *recovery* almeno dei servizi chiave, al fine di supportare la continuità funzionale dell'organizzazione ad un livello specificato entro un certo lotto di circostanze preventivate.

I compiti dell'ITSCM sono perciò i seguenti:

- riduzione della vulnerabilità dell'organizzazione;
- riduzione dei rischi identificati;
- pianificazione del recovery dei servizi chiave;
- eventuale trasferimento del rischio a terze parti;
- riduzione della minaccia di potenziali disastri;
- identificazione dei ruoli e delle responsabilità.

In realtà, l'ITSCM costituisce una parte integrante del più ampio processo di **Business Continuity Management (BCM)**. Il BCM è il processo che si occupa della gestione dei rischi dell'azienda in generale e della continuità nel caso i rischi dovessero materializzarsi. L'ITSCM costituisce quindi la parte del BCM focalizzata al settore IT dell'azienda. Per questo ciascun piano intrapreso dall'ITSCM deve essere coerente con la restante parte del processo di BCM.

Le attività dell'ITSCM come parte integrante del BCM sono rappresentate in figura 3. Da essa si può notare come vi siano quattro fasi principali:

- impostazione del BCM, analizzando tutti i fattori da prendere in considerazione;
- analisi dei requisiti, per valutare l'efficacia delle varie strategie;
- implementazione delle strategie studiate, con una prima fase di testing;

- mantenimento delle strategie (gestione), si assicura che tutto quello che è stato fatto venga mantenuto correttamente (addestramento personale, revisione, testing, controllo, monitoraggio, assicurazione dei livelli di qualità).

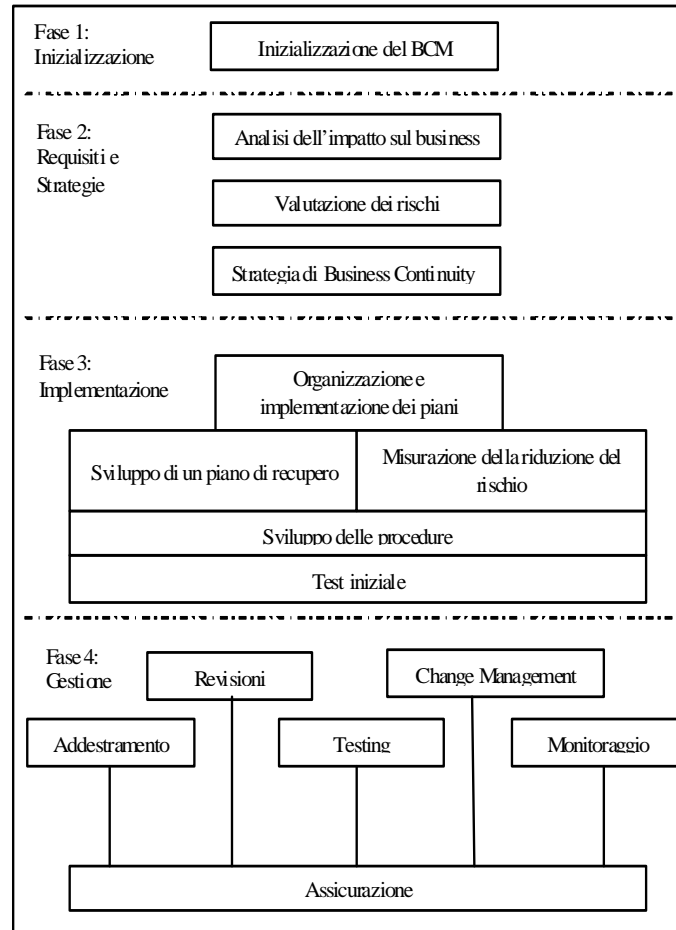


Figura 3: Attività del IT Service Continuity Management

Le interazioni con altri processi sono fondamentali per le finalità dell'ITSCM. In particolare l'ITSCM interagisce con i processi:

- Availability Management, implementando misure di riduzione del rischio in modo da aumentare l'availability dei servizi;
- Service Level Management, definendo i livelli di ITSCM;
- Change Management, assicurandosi che l'ITSCM sia sempre in linea con l'infrastruttura corrente;
- Service Desk e Incident Management, nell'utilizzo di dati storici.

I benefici dell'ITSCM sono i seguenti:

- assicura che l'organizzazione passi più o meno indenne da disastri o avvenimenti simili, almeno nei servizi IT chiave;
- riduce la vulnerabilità dell'organizzazione ai rischi identificati;
- produce piani di recovery a supporto del BCM.

Availability Management

Il processo di **Availability Management** ha lo scopo di assicurare un livello di **availability (disponibilità)** adeguato nell'erogazione dei servizi IT. L'availability è la capacità di un servizio IT o di un componente di un servizio IT di esplicare le proprie funzioni in un determinato periodo di tempo. Poche ore di non funzionamento dell'infrastruttura IT (di componenti hardware o software) possono portare, in seguito all'indisponibilità dei servizi, a un serio impatto sull'immagine aziendale, provocando in certi casi (ad esempio nei siti Internet) una fuga di clienti.

L'Availability Management deve quindi ottimizzare la capacità dell'infrastruttura IT, dei servizi e dei supporti, in modo da creare disponibilità ad un livello molto sostenuto da un punto di vista qualitativo e al tempo stesso economica, che permetta di soddisfare adeguatamente gli obiettivi aziendali. È pertanto necessario determinare i bisogni di disponibilità dell'azienda e confrontarli con la capacità dell'infrastruttura IT, dei servizi e dei supporti. In particolare, il processo deve considerare il problema della disponibilità da due punti di vista:

- il punto di vista dell'infrastruttura (componenti hardware o software non funzionanti);
- il punto di vista del servizio (l'applicazione non risponde), e quindi dell'utente finale.

I due concetti sono simili, ma l'impatto e la misurazione dei due è diversa (ad esempio un servizio potrebbe rimanere disponibile anche se dei componenti non lo sono).

Le attività di un processo di Availability Management, sono normalmente le seguenti:

- determinazione dei requisiti di disponibilità dell'organizzazione o dipartimento IT;
- produzione del piano delle disponibilità (**Availability Plan**);
- ottimizzazione della disponibilità ed analisi e monitoraggio degli elementi chiave;
- raccolta ed analisi dei dati relativi alla disponibilità;
- verifica del raggiungimento dei livelli minimi di disponibilità, specificati nella SLA o nelle OLA;
- determinazione di azioni correttive (**Corrective Actions**) per gestire il **downtime** (tempo di indisponibilità) di un servizio.

Tutte le attività dovrebbero comunque tenere in conto alcuni principi:

- l'Availability Management è essenziale per ottenere un alto grado di soddisfazione del cliente (la disponibilità e l'affidabilità determinano come i clienti percepiscono il servizio fornito);
- potranno sempre accadere dei guasti, malgrado un alto grado di disponibilità, tuttavia con un buon processo di Availability Management è possibile mantenere intatta la soddisfazione dei clienti gestendo correttamente i problemi.

In relazione al processo e alle sue attività vanno poi considerati diversi elementi. Alcuni di essi sono:

- i requisiti aziendali;
- i costi necessari e consentiti per mantenere un livello specifico di disponibilità;
- la ridondanza dei componenti chiave dell'infrastruttura IT;
- l'affidabilità dell'infrastruttura IT;
- la complessità dell'infrastruttura IT;
- la qualità delle procedure operative relative all'infrastruttura IT

In conclusione, un processo di Availability Management va pianificato in modo adeguato e attento ai bisogni dell'azienda attraverso la stesura, secondo precisi criteri, dell'Availability Plan. Sono molteplici i modi per migliorare il processo e molto differenti possono essere gli strumenti utilizzati.

Financial Management

Il processo di **Financial Management** ha come scopo quello di studiare e gestire i costi dell'infrastruttura IT e fornire una base finanziaria stabile per le decisioni aziendali relative all'area IT attraverso l'identificazione e l'analisi dei costi per l'erogazione dei servizi e, dove possibile, recuperando i costi in una giusta maniera.

Un processo di Financial Management si occupa quindi di:

- effettuare la contabilità di gestione dell'area IT;
- assistere nella riduzione dei costi di gestione nel lungo termine;
- identificare i costi reali dei servizi IT;
- formare una base per le decisioni di business;
- identificare come i servizi IT forniscano valore aggiunto all'azienda;
- valutare il **ROI (Return On Investment)**, cioè l'indice di redditività del capitale investito;
- valutare il **TCO (Total Cost of Ownership)**, cioè il costo totale di proprietà o possesso di apparecchiatura IT;
- assistere nell'influenzare il comportamento degli utenti (ad esempio incentivando l'uso di risorse non critiche).

La gestione finanziaria è divisa in tre fasi (rappresentate in figura 4):

- **budgeting;**
- **IT accounting;**
- **charging;**

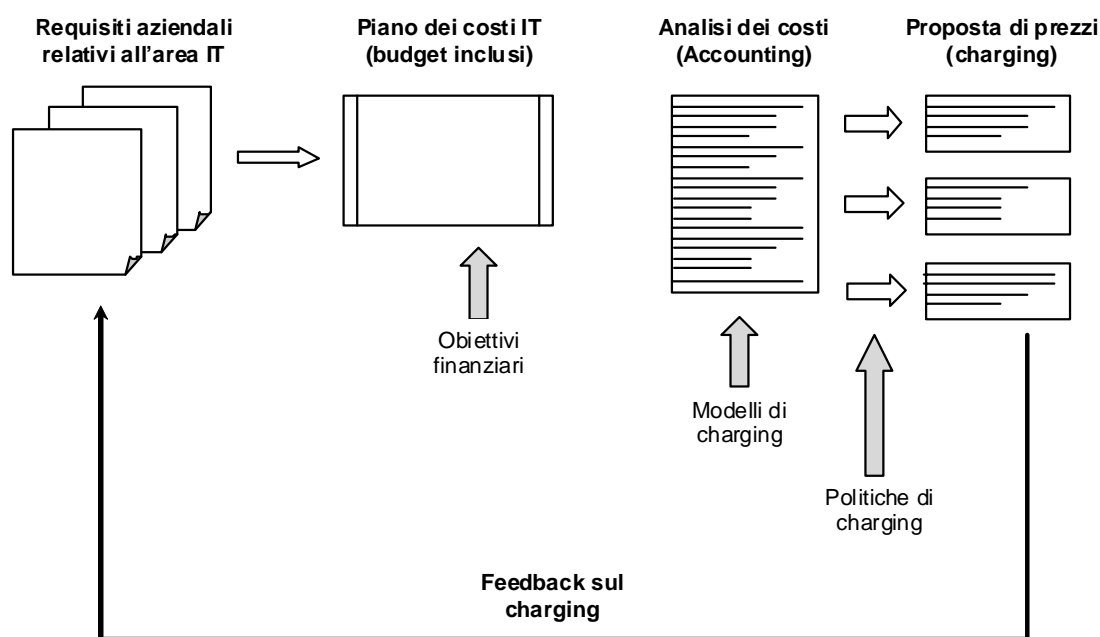


Figura 4: Fasi principali del Financial Management

Nella fase di *budgeting* si effettua il preventivo, il controllo e il monitoraggio dei costi, in rapporto al bisogno espresso dall'utenza, alle direzioni strategiche aziendali e al piano strategico dell'area IT. Consiste

in un periodo di tempo (generalmente annuale) di previsione e di un successivo monitoraggio giornaliero delle spese in rapporto con le aspettative preventivate. Nella fase di *IT accounting* viene effettuata una descrizione dettagliata sul denaro speso per la gestione dei servizi IT, motivando, in termini amministrativi e di controllo di gestione, la natura della spesa IT identificando le dimensioni d'analisi d'interesse (ad esempio per tipo di servizio e per attività). Infine, nella fase di *charging* si permette all'organizzazione di recuperare i costi della fornitura dei servizi; ciò può avvenire con diversi modelli, ad esempio:

- *cost recovery*, in cui il prezzo del servizio è uguale al costo;
- *cost recovery + markup*, in cui il prezzo è uguale al costo più un ricarico (markup);
- *market rate*, in cui il prezzo è quello di mercato, quindi non collegato al costo reale sostenuto (e si spera sia comunque superiore ad esso).

Ovviamente i costi possono ovviamente essere di diversa categoria. In particolare possono essere:

- capitali o operativi;
- diretti o indiretti;
- fissi o variabili.

ICT Infrastructure Management

Il volume dedicato all'**ICT Infrastructure Management** descrive le best practices per la definizione dei requisiti, la pianificazione, il design lo sviluppo, la gestione operativa e il supporto tecnico di un'infrastruttura **ICT** (*Information and Communication Technology*).

I processi descritti sono i seguenti:

- **ICT Design and Planning;**
- **ICT Deployment;**
- **ICT Operations;**
- **ICT Technical Support.**

Spesso, e sbagliando, si crede che questi processi, che costituiscono un approccio ad un ciclo di vita, siano implicitamente considerati e coperti dal Service Management.

Il processo **ICT Design and Planning** offre delle linee guida per il design e l'implementazione di processi di gestione dell'infrastruttura ICT che soddisfino i requisiti dell'azienda. Tra gli aspetti esaminati vi sono la fornitura di nuove soluzioni ICT, a seguito di richieste (**SOR, Statements of Requirement**) o offerte (**ITT, Invitations to Tender**), e il supporto dal punto di vista dell'infrastruttura ICT dei cambiamenti di strategia aziendale. Gli output di questo processo sono:

- strategie, politiche e piani ICT;
- descrizione e gestione dell'architettura ICT;
- studi di fattibilità, prendendo in considerazione richieste (SOR) e offerte (ITT);
- studi di business case.

Il processo **ICT Deployment** offre delle linee guida sull'implementazione di processi di gestione dell'infrastruttura ICT così come pianificati. Si focalizza sull'integrazione con il processo di Release Management e con le fasi di testing.

Il processo **ICT Operations** si occupa della gestione giornaliera dell'infrastruttura. È spesso confuso con il processo di Incident Management: è invece più tecnico e si interessa non solo degli incidenti segnalati dagli utenti, ma anche degli eventi generati o segnalati dall'infrastruttura stessa; lavora comunque a stretto contatto con l'Incident Management e con il Service Desk. Ciascuna operazione deve essere eseguita in base a processi documentati e procedure specifiche, ad esempio: gestione degli output, Job Scheduling, Backup and Restore, monitoraggio e gestione rispettivamente di rete, sistema, database e memoria. L'insieme delle operazioni deve assicurare:

- un'infrastruttura ICT stabile e sicura;
- una libreria di documentazione (**Operational Documentation Library, ODL**) aggiornata;
- un log di eventi operativi;
- la gestione dei sistemi di monitoraggio dell'infrastruttura.

Il processo di **ICT Technical Support** si occupa di supportare altri processi, sia di Service Management che di Infrastructure Management, offrendo alcuni aspetti specialistici quali:

- valutazione delle tecnologie;
- valutazione di richieste e offerte;
- dimostrazioni e ingegnerizzazione;
- disponibilità di specialisti e tecnici esperti;
- creazione di documentazione.

Security Management

L'interesse verso la sicurezza delle informazioni si è incrementato negli anni a causa della crescita dell'utilizzo di Internet e quindi all'aumento del rischio di intrusioni. Per questo motivo l'area di **Security Management** fornisce una serie di linee guida che mirano a controllare la fornitura delle *informazioni* e a prevenire un utilizzo non autorizzato di esse.

I requisiti sulla sicurezza devono essere indicati nella SLA dei servizi forniti, e il Security Management deve assicurare che gli aspetti di sicurezza siano stati forniti al livello concordato in ogni momento. Pertanto, gli obiettivi del Security Management sono i seguenti:

- rispettare i requisiti di sicurezza indicati nelle SLA e altri ulteriori requisiti esterni, specificati in altri contratti, dalla legge o da imposizioni politiche;
- fornire un livello base di sicurezza, indipendente dai requisiti esterni.

The Business Perspective

L'area di **Business Perspective** si propone di affrontare alcuni dei temi spesso incontrati nella comprensione di come debba avvenire la fornitura di servizi IT. In pratica supporta le funzionalità IT a comprendere come possano contribuire al raggiungimento degli obiettivi di business e come il loro ruolo possa essere utilizzato per massimizzare i risultati aziendali.

Si può quindi considerare quest'area come un insieme di linee guida che consentono un corretto approccio ai temi dell'**IT Governance** (governo dei sistemi informativi), i cui temi principali sono:

- assicurare che gli investimenti IT generino valore per l'azienda;
- gestire e limitare i rischi associati all'IT.

Questi obiettivi possono essere raggiunti definendo e realizzando una struttura organizzativa con ruoli e responsabilità ben chiari per quanto riguarda i temi correlati ai sistemi informativi (sicurezza, processi aziendali, infrastruttura, analisi dei rischi, applicazioni) e cercando di allineare il più possibile l'infrastruttura e i servizi IT ai requisiti dell'azienda.

Application Management

L'**Application Management** descrive come gestire le applicazioni durante tutte le fasi del ciclo di vita, assicurando l'allineamento ai progetti e alle strategie aziendali. Per ogni fase del ciclo di vita sono pertanto fornite delle linee guida che danno una descrizione ad alto livello delle responsabilità e dei *task* da attuare. Viene quindi fornita una sorta di *roadmap* che aziende o dipartimenti IT possono seguire nel rilascio di nuovo software.

Sebbene l'Application Management sembri molto vicino al processo di Release Management, in realtà va molto oltre, arrivando a coprire il processo di sviluppo software pressoché nella sua interezza: può quindi essere considerato a tutti gli effetti un processo di ingegneria del software.

Alcuni benefici dell'Application Management sono:

- la possibilità di focalizzarsi non solo sul software stesso, ma anche alla sua integrazione con l'infrastruttura esistente e con l'azienda;
- la possibilità di collegare i requisiti aziendali con i requisiti del software, permettendo così controlli di qualità basati non solo sulla funzionalità del software ma anche sulla base del valore aggiunto portato da esso all'azienda.

Software Asset Management

L'area di **Software Asset Management** consiste in una serie di best practices riguardanti l'integrazione di *persone, processi e tecnologie* al fine di tenere traccia, valutare e monitorare le licenze software (gli *asset*) e il loro uso. L'obiettivo dei processi di quest'area è quello di ridurre le spese IT, diminuire l'overhead nell'uso delle risorse umane e ridurre i rischi dovuti al possesso e alla gestione del software.

Le attività principali sono le seguenti:

- manutenzione delle licenze software (garantire la conformità);
- monitoraggio dell'utilizzo delle risorse software (tramite un inventario);
- uso di politiche e procedure standard per l'implementazione, configurazione, utilizzo e ritiro di software.

In realtà il Software Asset Management è la componente software dell'area più generale di **IT Asset Management**, che include anche la gestione dei beni hardware. Ovviamente la gestione della parte software deve essere contemporaneamente accompagnata da una corretta gestione della parte hardware.

Planning to Implement Service Management

L'area **Planning to Implement Service Management** è in pratica una guida all'implementazione di ITIL. Il suo scopo è fornire una spiegazione sui passi necessari per identificare come un'organizzazione potrebbe ottenere benefici da ITIL, e come regolarsi per raccogliere questi benefici.

In particolare esamina i fattori e i compiti coinvolti nella pianificazione, nell'implementazione e nel miglioramento dei processi di Service Management all'interno di un'organizzazione. Inoltre indirizza i fattori legati ai cambiamenti culturali e organizzativi, lo sviluppo di una visione e di una strategia e il più adeguato metodo di approccio.

Cenni a ITIL v3

ITIL v3 è parte di un processo teso a migliorare le best practices ITIL, conservando in ogni caso una parte molto significativa di ITIL v2. Il processo che sta portando ad una definizione di ITIL v3 è basato su consultazioni pubbliche e contribuzioni dagli esperti del settore e dalla comunità di ITSM a livello internazionale.

ITIL v3, rappresenta una evoluzione di ITIL, ma non una rivoluzione, dal momento che l'interfaccia tra la versione corrente 2 e la nuova non introduce ulteriori complicazioni e risulta facilmente usufruibile. Nonostante ciò, il punto di maggior distacco dalla versione precedente è l'introduzione del concetto di lifecycle dei servizi.

Altri cambiamenti sono i seguenti:

- Si chiarisce l'integrazione tra la strategia di business e la strategia di fornitura dei servizi IT;
- Si introduce il concetto di Return On Investment (ROI) nel frame work, migliora inoltre la misurazione del valore prodotto;
- Vengono aggiunti modelli di transizione per l'adozione di innovazioni nei servizi IT;
- Nasce il concetto di Service Management Knowledge Base che traduce i dati registrati in "organizational intelligence";
- Maggiori dettagli vengono dati per contesti di IT Service Management specifici a particolari settori.

Sostanzialmente, i "core books" di ITIL v3, rilasciati il 30 Maggio 2007, sono i seguenti:

- Service Strategies;
- Service Design;
- Service Transition;
- Service Operations;
- Continuous Service Improvement.

Le prime quattro voci dell'elenco riorganizzano sostanzialmente la struttura di ITIL v2, cambiandone la forma, ma non la sostanza; è interessante invece spendere due parole sull'ultima voce, che riguarda il Continuous Service Improvement (o CSI). Quest'ultimo copre gli aspetti relativi al continuo miglioramento dei servizi offerti. I suoi obiettivi includono:

- Rivedere ed analizzare i Service Level Achievement;
- Identificare ed implementare attività di miglioramento della qualità dei Servizi IT e migliorare l'efficienza e l'efficacia dei processi ITSM;
- Migliorare l'efficienza nei costi (cost effectiveness) della fornitura dei servizi IT.

Critiche a ITIL

Nonostante i numerosi vantaggi, citati nei processi visti, ITIL porta con se anche alcuni potenziali problemi:

- l'introduzione di nuove metodologie può comportare un lungo periodo di formazione e uno sforzo iniziale significativo, che richiede un cambiamento culturale nell'azienda;
- i miglioramenti nella fornitura dei servizi e le riduzioni dei costi potrebbero non essere sufficientemente visibili;
- un'implementazione di successo richiede il coinvolgimento e l'affidamento del personale di tutti i livelli aziendali;
- se non si investe sufficientemente negli strumenti di supporto, i processi potrebbero non essere eseguiti correttamente ed il servizio in generale non sarà migliorato.

Ovviamente questi problemi possono essere facilmente superati, in quanto ITIL è stato sviluppato guardando ai vantaggi. Molte delle best practices suggeriscono poi di puntare a prevenire alcune problemi o, dove occorre, ad aiutare a risolverli.

ITIL è inoltre criticato essenzialmente per due motivi:

- la percezione di esso come un *frame work*, ossia di una metodologia per la gestione dell'IT;
- la tendenza ad essere considerato quasi una religione.

In realtà ITIL non è altro che un insieme di *best practices*, non è una metodologia formale e scientifica, per cui discostarsi da esso non vuol dire necessariamente sbagliare. Occorre pertanto applicare in modo critico ciò che è realmente applicabile e utile in una organizzazione IT.

Casi applicativi

Esempio di successo

Lo scenario è quello di una grande catena di abbigliamento in rapida crescita: dopo aver studiato lo schema ITIL e analizzato la situazione aziendale (processi, obiettivi, stato dell'azienda ecc.) si decide di implementarne i processi per supportare più efficacemente tale crescita.

In precedenza il personale IT era ostacolato da strumenti poco efficienti per la gestione dell'infrastruttura IT. Di conseguenza le attività aziendali erano spesso penalizzate da interruzioni di servizio non volute, ritardi nei ripristini e numerosi incidenti. Inoltre erano disponibili quantità minime di informazioni per determinare l'impatto delle interruzioni sull'attività aziendali, tenere sotto controllo i beni IT, aggiornare il software, stimare le risorse richieste e implementare nuove funzionalità.

L'implementazione di ITIL è pertanto avvenuta a partire dal Service Desk, con la sostituzione del precedente sistema con uno nuovo che implementasse i processi ITIL per la gestione degli incidenti, dei problemi, dei cambiamenti e delle configurazioni. A questo punto si sono prese in considerazione diverse opzioni, tra cui:

- implementare ITIL internamente;
- acquistare una soluzione ITIL esterna, in grado di fornire le funzionalità richieste.

L'azienda decide quindi di optare per una soluzione esterna. Tale decisione si è scontrata però con una certa resistenza interna, dovuta alla convinzione di parte dei dipendenti e dei manager che un pacchetto applicativo non avrebbe soddisfatto le esigenze. Per questo motivo, dopo una preparazione (*training*) iniziale sulle nuove modalità di gestione dell'area IT, i responsabili del progetto chiedono, per un certo periodo successivo all'implementazione, di elencare tutte le funzioni identificate come mancanti. Il personale abbandona però dopo poco tempo questa linea, essendo diventato molto più semplice aderire ai processi implementati e favorendo in tal modo la rapidità del progetto.

In sole dieci settimane l'azienda è quindi riuscita a implementare una suite integrata di applicazioni di gestione dei servizi IT, in grado di supportare un Service Desk conforme alle linee guida di ITIL, un insieme di processi per la gestione degli incidenti, dei problemi e dei cambiamenti e il CMDB sottostante. In una fase successiva l'azienda ha poi provveduto all'estensione dell'adozione di ITIL implementando i processi di Service Delivery.

I vantaggi per l'azienda sono stati rilevanti:

- riduzione di 1.8 milioni di dollari del budget di spesa annuale;
- oltre 1 milione di dollari di utile dovuto all'accelerazione nell'apertura di nuovi negozi;
- oltre 500 mila dollari di risparmio sui contratti di licenza;
- oltre 200 mila dollari di risparmio nelle trattative con i fornitori di hardware;
- capacità di tenere sotto controllo i beni IT e di ridurre i costi di manutenzione;
- riduzione del 10% delle spese di esercizio dell'area IT;
- capacità di offrire nuovi servizi ai clienti più rapidamente, con livelli di servizio superiori.

Esempio di insuccesso

In questo caso lo scenario è dato da un'azienda internazionale di telecomunicazioni, con più di 6500 dipendenti e fatturato annuo di 4 miliardi di dollari. L'organizzazione si è evoluta molto velocemente, attraverso la fornitura di nuovi servizi ai clienti e alla rapida introduzione di nuove tecnologie. Inoltre sono state anche effettuate diverse acquisizioni di altri gruppi, senza però alcun consolidamento, mantenendo pressoché intatte le singole aree IT. Di conseguenza, l'infrastruttura globale risulta molto grande, complessa e diversificata, senza alcun controllo centralizzato e con bassa comunicatività.

L'azienda decide quindi di affidarsi allo schema ITIL, dopo alcuni tentativi precedenti frenati dai ritmi di crescita. Viene quindi creata una squadra di 12 esperti ITIL (per la maggior parte nuove assunzioni), separandola, gestionalmente e funzionalmente, dal resto dell'area IT.

Dopo circa un anno di analisi, la squadra ITIL introduce il progetto, che risulta abbastanza completo in quanto sono state seguite tutte le linee guida e si è cercato di personalizzare i processi per l'azienda. Al momento dell'attuazione del piano si rende però evidente come esso sia incompatibile con il funzionamento dell'organizzazione, con la sua complessità e con la sua infrastruttura non standardizzata.

Tutto ciò è dovuto principalmente al fatto che la squadra ITIL si è isolata nell'effettuare il progetto, lasciando in disparte lo staff IT. Sono quindi emersi numerosi problemi di comunicazione tra le due parti, tanto da impedire una comprensione di base sulle metodologie ITIL e conducendo a modelli ideali incompatibili con i workflow reali. Inoltre nel frattempo l'azienda ha continuato a crescere, con l'aggiunta di nuovi servizi di telefonia e l'acquisizione di un'altra società. Si è quindi deciso di effettuare una semplice revisione dell'area IT, bloccando così l'iniziativa del passaggio a ITIL.

In realtà l'azienda è tuttavia riuscita ad applicare lo schema ITIL alcuni mesi più tardi, dopo aver ricavato requisiti dettagliati sul funzionamento dell'infrastruttura e sui workflow e tramite una stretta collaborazione tra gli attuatori dello schema e l'intero staff IT. Si è quindi riusciti in tal modo a trovare un equilibrio tra la teoria, proposta da ITIL, e la pratica, in termini di funzionamento dell'azienda.

Bibliografia

Introduzione a ITIL e generalità:

- <http://www.iti-officialsite.com/home/home.asp>
- <http://www.iti-itsm-world.com/>
- <http://www.iti.org/en/>
- <http://www.itsmf.it>
- <http://www.iti.org.uk>
- <http://it.sun.com/servicessolutions/iti/>
- http://www.lineadp.it/01NET/HP/0.1254.1_ART_72533.00.html?lw=10001

Descrizione di ITIL nelle sue aree e processi:

- <http://www.iti-italia.com/iti.htm> (riferimento di base)
- <http://en.wikipedia.org/wiki/ITIL>
- [http://en.wikipedia.org/wiki/Incident_Management_\(ITSM\)](http://en.wikipedia.org/wiki/Incident_Management_(ITSM))
- [http://en.wikipedia.org/wiki/Change_Management_\(ITSM\)](http://en.wikipedia.org/wiki/Change_Management_(ITSM))
- http://en.wikipedia.org/wiki/Release_Management
- [http://en.wikipedia.org/wiki/Configuration_Management_\(ITSM\)](http://en.wikipedia.org/wiki/Configuration_Management_(ITSM))
- http://en.wikipedia.org/wiki/Capacity_management
- http://en.wikipedia.org/wiki/ITIL_Planning_to_implement_service_management
- http://en.wikipedia.org/wiki/ITIL_Security_Management
- <http://www.itlibrary.org/>
- <http://www.itil-survival.com/>
- home.dei.polimi.it/violante/1/iti.pdf
- www.unc.edu/remedy/presentations/iti_study_guide.pdf

Argomento delle best practice in generale:

- <http://www.best-management-practice.com>
- http://en.wikipedia.org/wiki/Best_practice

Implementazione di ITIL:

- <http://www.bmc.com>
- <http://www.networkworld.com/topics/ITIL.html>

Storia di ITIL, benefici e critiche

- www.compaid.com/caiinternet/ezine/the_iti_story.pdf

ITIL v3

- http://images.globalknowledge.com/wwwimages/whitepaperpdf/WP_ITILv3.pdf
- akmeev.ru/images/itilv3_overview.pdf

PC LINK S.a.s
Italia