

UNIVERSITA' DEGLI STUDI DI PADOVA

Laurea Magistrale in Computer Science

IT Service Management

A.a. 2022/23

Poloni Alessandro, mat. 2097424

Greggio Marta, mat. 2096579

Noro Matteo, mat. 2091681

Indice

Indice.....	1
1. SOMMARIO.....	2
2. ANALISI DELLO SCENARIO.....	3
3. ANALISI DELL'INCIDENTE.....	4
3.1 PROBLEMI RISCONTRATI.....	4
3.2 SOLUZIONI PROPOSTE.....	5
4. ITIL 4.....	7
4.1 ITIL practices coinvolte nello scenario.....	8
4.2 I sette principi ITIL 4.....	13
5. PIANO EVOLUTIVO.....	16
5.1 ANALISI DELLE FIGURE AZIENDALI.....	17
5.2 DEFINIZIONE DEI NUOVI PROCESSI.....	18
5.1.1 Processo di IT Asset Management.....	18
5.1.2 Processo di Supplier Management.....	21
5.1.3 Processo di Availability Management.....	28
5.1.4 Processo di Incident Management.....	30
5.3 IMPLEMENTAZIONE DEL CAMBIAMENTO.....	33
5.3.1 Piano di rollout.....	37

1. SOMMARIO

Il presente documento si pone l'obiettivo di produrre un *evolutionary plan* che permetta di correggere e migliorare gli attuali processi dell'azienda in esame.

Il piano si basa su un'analisi di ciò che è andato storto e, di conseguenza, quali processi dovrebbero essere revisionati.

Viene poi proposto un redesign di questi ultimi, definendo inoltre i ruoli delle figure coinvolte usando una matrice RACI, chiudendo con un piano di rollout per i nuovi processi.

2. ANALISI DELLO SCENARIO

Il caso di studio riguarda una banca specializzata in servizi bancari individuali che sta affrontando sfide legate all'espansione delle proprie operazioni in altri paesi e che ha recentemente ampliato le sue operazioni all'estero, attraverso l'acquisizione di banche e partnership con altre istituzioni finanziarie.

La strategia aziendale è orientata all'espansione e il comitato esecutivo ha fissato degli obiettivi da raggiungere entro un determinato periodo, in cui integrare e automatizzare le operazioni aziendali e informatiche, sempre considerando eventuali vincoli legislativi, normativi e finanziari.

L'attuale struttura dell'azienda è la seguente:

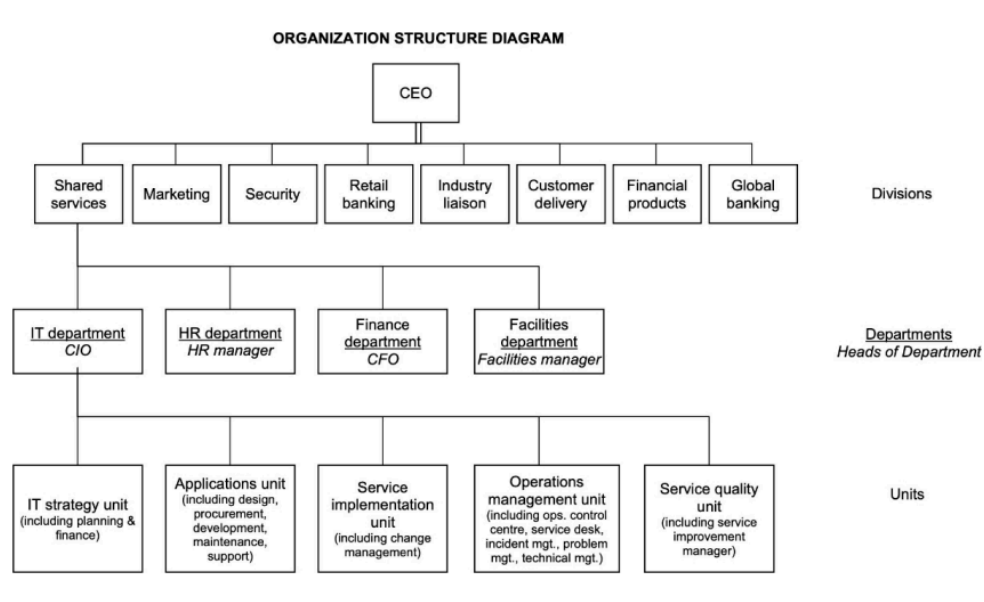


Figura 1: Organigramma aziendale.

Ci sono otto divisioni principali che riferiscono direttamente al *CEO*: l'unione di queste forma il consiglio direttivo.

Le otto divisioni principali si suddividono in cinque bancarie e tre non bancarie, tra cui *shared services*. Questa è a sua volta divisa in 4 dipartimenti, tra i quali l'*IT department*.

Quest'ultimo, guidato dal CIO, si compone di cinque unità, ognuna diretta da un manager.

Fra queste unità troviamo il *Service Desk*, compreso nella *Operations management unit*.

3. ANALISI DELL'INCIDENTE

L'incidente e i problemi riscontrati sorgono da una richiesta pervenuta al servizio di Service Desk da parte di un utente finale. Quest'ultimo si è correttamente rivolto al Service Desk il quale, dopo aver informato che ci sarebbero voluti 5 giorni lavorativi al fine della sostituzione, ha inoltrato la richiesta al gruppo di assistenza appropriato.

In maniera reattiva all'accaduto, l'assegnatario del gruppo di assistenza ha effettuato un ordine al fornitore esterno responsabile di tutti i servizi desktop. Dopo due giorni, il fornitore esterno ha avvisato il gruppo di assistenza che i monitor sono esauriti e che ci vorrà quindi una settimana e mezza prima di poterne fornire uno nuovo.

Questo ritardo costituisce il punto di errore dell'intero processo in quanto il Service Desk, come stabilito dallo SLA, aveva garantito la risoluzione del problema entro 5 giorni lavorativi.

Il ritardo e la mancanza di forniture di scorta hanno determinato quindi un potenziale rallentamento nel normale svolgimento delle attività lavorative dell'utente.

In particolare, siamo di fronte ad una violazione del Service Level Agreement (SLA), ovvero un accordo tra il fornitore di servizi ed il cliente, che delinea il livello di servizio atteso. Il documento include, per esempio, i tempi di risposta, i tempi di risoluzione del problema ed eventuali metriche di performance (KPI) garantendo così che entrambe le parti coinvolte siano d'accordo.

3.1 PROBLEMI RISCONTRATI

In primo luogo, l'incidente ha influito negativamente sul regolare workflow dell'utente coinvolto, che ha infatti espresso fin da subito il disagio causato dal monitor guasto.

L'impatto sul workflow non è specificato, ma naturalmente potrebbe comportare rallentamenti di portata ben più ampia fino all'intera interruzione di un servizio.

Esaminando la situazione organizzativa della banca, si delineano diverse prospettive del problema.

Innanzitutto, la manutenzione hardware IT all'interno della sede principale è interamente appaltata ad un singolo fornitore, il quale nello scorso anno non è risultato profittevole.

Affidare la manutenzione ad un singolo fornitore esterno risulta rischioso, in quanto in caso di disagi o ritardi nei servizi erogati, come avvenuto per il monitor, l'azienda non dispone di alternative.

Inoltre, emerge un chiaro problema di comunicazione, forse dovuto alla recente acquisizione di aziende estere. Infatti, succede che il Support Group effettua un ordine al fornitore senza sapere se ci fosse la disponibilità di un monitor.

Questo problema porta ad una terza considerazione: visto che la banca dispone di un software per il controllo delle scorte, perché il Support Group non lo ha consultato prima di effettuare l'ordine?

3.2 SOLUZIONI PROPOSTE

Come già menzionato, affidare l'approvvigionamento di dispositivi hardware IT ad un solo fornitore è una scelta rischiosa.

La banca dovrebbe poter contare su almeno due fornitori, diversificati tra di loro, in modo da mitigare il rischio di esaurimento scorte e garantire un approvvigionamento stabile e continuo di materiale IT in caso di necessità.

Inoltre, in linea con i piani di espansione, sarebbe opportuno valutare una lista di fornitori localizzati per ogni paese, in modo da ottimizzare i processi correlati.

Come già detto, la risposta al problema è stata reattiva: si è rilevato che le scorte erano esaurite soltanto alla richiesta esplicita dell'utente coinvolto.

Questo approccio apre a possibilità di miglioramento, incorporando invece delle misure proattive, che mirano a prevenire o anticipare il problema.

Per esempio, il gruppo di assistenza avrebbe potuto affidarsi al software di controllo scorte adottato dalla banca per controllare la disponibilità di monitor in tempo reale prima di effettuare l'ordine.

Questa operazione avrebbe aiutato il gruppo di supporto a stabilire immediatamente le tempistiche entro le quali il monitor sarebbe stato sostituito. Invece, effettuando l'ordine al fornitore, queste si sono allungate di due giorni.

Una soluzione efficace includerebbe un meccanismo di notifica al personale da parte del software di controllo scorte quando queste si stanno esaurendo, abbinato ad un processo automatizzato che ordini automaticamente dei nuovi monitor in modo da prevenire disagi o ritardi nel servizio e rispettare gli SLA concordati.

Inoltre, un processo di valutazione continua dei fornitori potrebbe migliorare gli accordi con questi, in modo da rendere più profittevole ed efficiente l'approvvigionamento di risorse secondo un criterio di affidabilità. In questo caso, consci della scarsa redditività del fornitore di attrezzature IT, l'azienda avrebbe potuto agire in modo proattivo cambiando a priori il fornitore di riferimento.

4. ITIL 4

ITIL 4 è un framework che ha l'obiettivo di creare valore per i clienti finali sotto forma di servizi IT.

Questo fornisce basi pratiche e flessibili per supportare le organizzazioni nel percorso di trasformazione digitale, promuove una visione olistica nell'erogazione di prodotti e servizi, sottolinea l'importanza della collaborazione e garantisce qualità ed efficienza.

Gli elementi chiave di ITIL 4 sono il Service Value System (SVS) e le quattro dimensioni.

Il Service Value System facilita l'integrazione e il coordinamento delle diverse componenti e attività di un'organizzazione in modo da rendere quest'ultima affidabile, ed è formato da cinque componenti fondamentali:

1. *Service Value Chain (SVC)*;
2. [ITIL practices](#);
3. [Guiding principles](#);
4. *Governance*;
5. *Continual improvement*.

Le quattro dimensioni, invece, devono essere prese in considerazione da ciascun componente della SVS in modo da assicurare un approccio olistico e ben bilanciato alla gestione dei servizi IT. Le quattro dimensioni sono:

- *Organizations and people*: si riferisce all'aspetto umano, ovvero le persone che svolgono e gestiscono il lavoro. Le organizzazioni devono considerare come le persone lavorano insieme per creare valore. Questo include la cultura organizzativa, la struttura, le competenze, e la capacità di adattarsi al cambiamento;
- *Information and technology*: concerne le tecnologie usate nella gestione dei servizi IT, per esempio gli strumenti e le basi di conoscenza, oltre che della gestione delle informazioni che le aziende generano, immagazzinano, gestiscono e utilizzano nella fornitura di un servizio IT;
- *Partners and Suppliers*: riguarda le relazioni con altre organizzazioni che sono coinvolte nella progettazione, sviluppo, consegna e miglioramento dei servizi.

Questo può includere fornitori, partner commerciali, organizzazioni esterne e altre parti che contribuiscono alla fornitura di servizi;

- *Value streams and processes*: fornisce una definizione di tutte le attività, flussi di lavoro e processi necessari per raggiungere gli obiettivi di business. Esamina anche l'interazione dei diversi componenti del business e come sono coinvolti nel processo di creazione del valore.

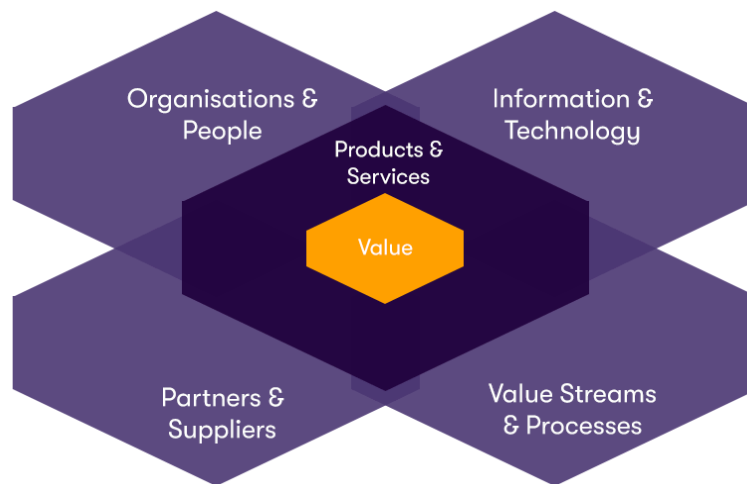


Figura 2: Le quattro dimensioni ITIL.

4.1 ITIL practices coinvolte nello scenario

Le pratiche ITIL sono linee guida raccomandate per completare certi compiti e raggiungere certi obiettivi.

Sono organizzate in tre categorie che coprono diverse aree della gestione dei servizi: pratiche di gestione generale (*General management practices*), Pratiche di gestione dei servizi (*Service Management Practices*) e Pratiche della gestione tecnica (*Technical Management Practices*).

L'obiettivo è di favorire una gestione sistematica e orientata al miglioramento continuo, garantendo al contempo l'allineamento dei servizi IT con gli obiettivi strategici dell'organizzazione.

Ogni processo è un insieme strutturato di attività finalizzato al raggiungimento di uno specifico obiettivo.

Nella versione 4 di ITIL sono presenti 34 *practices* ognuna delle quali è rappresentata da un *manager*.

Dopo aver identificato i problemi nello scenario presentato nel [capitolo precedente](#), procediamo a mapparli con le pratiche ITIL 4, suddivise per categoria.

Si riportano solo le pratiche ITIL coinvolte nel caso di studio. La ridefinizione dei suddetti processi verrà implementata nel capitolo successivo, alla sezione [5.1 Definizione dei nuovi processi](#).

Pratiche di gestione generale

- **Continual Improvement:** è un'attività organizzativa ricorrente che serve ad assicurare che l'organizzazione sia allineata con le aspettative degli stakeholders. In particolare, possiamo dire che fornisce una guida al miglioramento tramite un approccio iterativo.
- **Measurement and Reporting Management:** questa pratica aiuta ad identificare eventuali problematiche ricorrenti, comprende le attività di definizione e monitoraggio dei KPI e degli SLA per mantenere gli standard di servizio concordati.

Nel nostro caso va considerata, visto che si verifica la necessità di ridefinire alcuni indicatori di performance.

- **Risk Management:** nel nostro caso, il processo di *Risk management* deve essere tenuto in considerazione. Per esempio, prima di ridefinire i processi di *availability* ed *IT Asset Management*, è importante valutare gli effettivi rischi nel caso di esaurimento scorte, in modo da fornire una proposta di cambiamento documentata.
- **Knowledge Management:** il mantenimento di una *knowledge base* per raccogliere le lezioni apprese dagli incidenti, e dalle soluzioni annesse, è essenziale per riferimenti e miglioramenti futuri. Questo processo non andrà ridefinito ma sarà naturalmente partecipe per la sua natura.
- **Supplier Management:** esso è finalizzato ad assicurare che i contratti con i fornitori supportino i bisogni della banca. Un sottoprocesso di questa pratica consiste nella valutazione di possibili nuovi fornitori e relativi contratti. Ciò avviene in accordo con il *Supplier strategy*, che stabilisce le linee guida per l'approvvigionamento di servizi e beni e, in genere, include i criteri per la selezione di fornitori idonei.

- **Availability Management e IT Asset Management:** questi due processi sono interdipendenti. Il primo riguarda la gestione e il raggiungimento dei requisiti di disponibilità concordati come stabilito nello SLA, il secondo si occupa della gestione efficiente delle apparecchiature IT durante il loro ciclo di vita. Garantisce che le risorse vengano distribuite, gestite, aggiornate e smaltite.

È necessario ridefinire questi processi affinché non si verifichino altri problemi di esaurimento scorte e conseguente interruzione del servizio.

- **Service Desk:** riteniamo che il Service Desk abbia agito correttamente, quindi non è necessario revisionare il processo relativo. Tuttavia, è bene sottolineare come, nel caso in cui si verifichi un incidente, il Service Desk sia responsabile non solo dell'assegnazione del ticket al gruppo di supporto adeguato, ma anche della segnalazione all' *Incident manager* e dell'eventuale comunicazione con l'utente e con il proprio manager nel caso di rottura del SLA.

Questa pratica viene comunemente chiamata *escalation gerarchica* e garantisce che l'inconveniente sia risolto nel più breve tempo possibile.

Di seguito riportiamo il workflow del servizio di Service Desk, a riprova del fatto che abbia agito correttamente.

Nel nostro caso, il Service Desk elabora la richiesta e fornisce immediatamente all'utente un feedback con le tempistiche di risoluzione.

Quando l'utente informa il Service Desk agent di non poter aspettare i 5 giorni comunicati, la richiesta viene rivalutata e inoltrata al gruppo di supporto per una risoluzione più tempestiva.

In assenza di istruzioni chiare su come procedere, il support group effettua un ordine al fornitore, affidandosi ai 5 giorni definiti nello SLA per il rifornimento. Questo rappresenta un'ulteriore escalation, data l'impossibilità di evadere la richiesta con le risorse disponibili.

Concludendo, il Service Desk ha agito correttamente e non è necessario rivedere il processo. Tuttavia, l'incidente avvenuto apre le possibilità di miglioramento sia per il processo di Incident Management sia per la gestione dei fornitori.

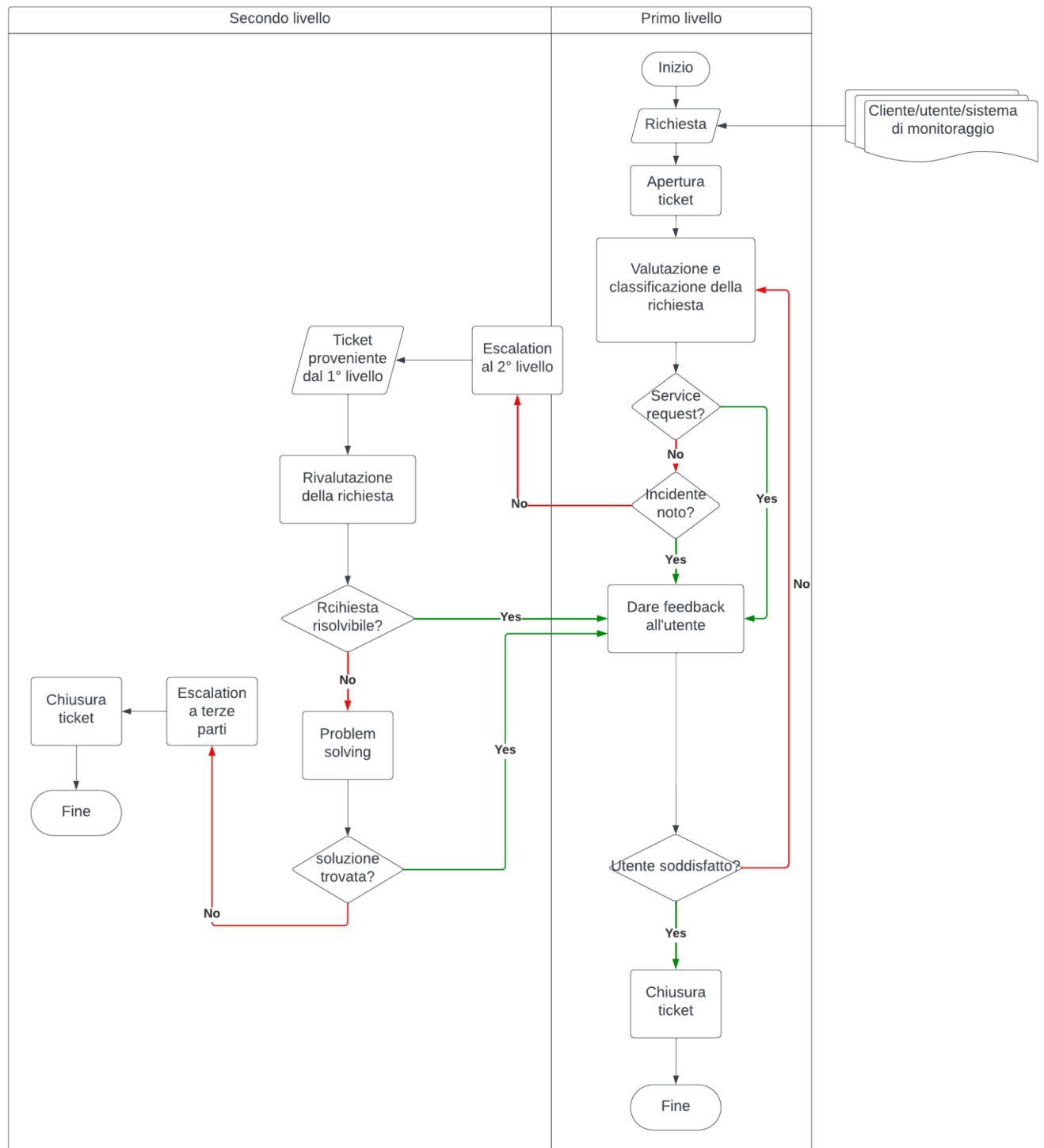


Figura 3: Flowchart del Service Desk.

- **Incident Management:** questa pratica è dedicata alla gestione efficiente e tempestiva degli incidenti che si verificano. L'obiettivo è quello di ripristinare il normale funzionamento del servizio minimizzando l'impatto negativo.

Dal testo di riferimento, si legge che il processo di *Incident Management* è ben consolidato ed efficace, ma riteniamo necessario apportare alcune modifiche affinché il gruppo di assistenza sappia come procedere nel caso di una richiesta di sostituzione monitor.

Inoltre, essendo questo processo strettamente legato alle pratiche di *Problem management* e *Change management*, è importante che all' *Incident manager* venga segnalato l'inconveniente al fine di inserire tutti i dettagli nell'incident report.

- **Problem Management:** a differenza dell'*Incident Management* che si occupa di gestire le singole segnalazioni dell'utente, questa pratica spinge ad adottare una risoluzione proattiva anziché reattiva. Nel nostro caso, questa pratica sta alla base del nostro approccio di ridefinizione dei processi, e va ridefinita visto che attualmente il *Problem management team* tende ad essere solamente reattivo.
- **Change Enablement Management:** data la necessità di ridefinire alcuni processi, il *Change enablement manager* è cruciale per garantire che i cambiamenti all'ambiente IT siano pianificati, autorizzati e implementati in modo controllato e conforme.

Egli infatti, non solo deve valutare ed approvare le richieste di cambiamenti, ma si deve anche occupare di implementare la proposta e monitorarla per garantire che abbia avuto gli effetti desiderati.

Inoltre, si legge dal testo che 'non esiste un processo formale di valutazione del cambiamento', quindi è necessario definire delle metriche per avere un quadro chiaro dell'efficacia dei cambiamenti apportati, oltre che consentire di identificare aree che necessitano di miglioramenti.

È bene tenere a mente che le pratiche di *Change enablement management* e *Release management* lavorano a stretto contatto: una volta stilato e approvato il piano di cambiamento, il *release manager* ha il compito di programmarlo ed implementarlo.

4.2 I sette principi ITIL 4

Analizzeremo lo scenario sotto i sette diversi principi ITIL, i quali costituiscono una guida per la gestione dei processi e promuovono il miglioramento continuo a tutti i livelli.

1. Focus on Value - Focalizzarsi sul valore

Questo principio sottolinea l'importanza di concentrarsi sul valore per il cliente e per tutti gli *stakeholders* coinvolti.

Tutte le attività e i servizi erogati dall'azienda dovrebbero essere orientati a fornire valore al cliente e all'organizzazione nel loro complesso.

Il valore non è solo inteso come finanziario, infatti questo principio mira ad incoraggiare l'esperienza complessiva del consumatore.

Nella ridefinizione delle pratiche ITIL individuate, cercheremo sempre di evidenziare qual è il valore apportato da ogni processo, in termini di benefici per business e per il corretto svolgimento delle operazioni.

2. Start Where You Are - Partire da dove ci si trova

Questo principio suggerisce di utilizzare i punti di forza degli attuali processi e servizi come base di partenza.

Tenere a mente questo principio ci aiuterà a trovare soluzioni partendo dalle risorse, dai dati e dalle pratiche già disponibili.

3. Progress Iteratively with Feedback - Avanzare iterativamente raccogliendo feedback

Questo principio invita ad implementare progressi gradualmente ed iterativi, e raccogliere feedback per assicurarsi che la direzione presa sia giusta e in linea con gli obiettivi.

Proveremo a presentare soluzioni gradualmente, evitando di affrontare tutto in un'unica fase.

4. Collaborate and Promote Visibility - Collaborare e promuovere la visibilità

Questo principio sottolinea l'importanza della collaborazione e della visibilità tra i vari team e le divisioni.

Infatti, persone abituate a lavorare nei cosiddetti silos sono molto competenti in specifiche attività, ma quando le circostanze cambiano si trovano in svantaggio. Al contrario, quando la collaborazione è pratica quotidiana, tutti ne traggono beneficio.

Naturalmente, affinché la collaborazione sia efficace, è necessario essere trasparenti: tutte le parti coinvolte devono essere al corrente di come stiano procedendo le cose, in modo che sia più semplice collaborare.

Ridefinendo i vari processi, cercheremo di evidenziare sempre quali sono le figure coinvolte e le loro responsabilità, in modo da promuovere la collaborazione.

5. Think and Work Holistically - Pensare e lavorare in modo olistico

Questo principio invita a considerare il sistema nel suo complesso, collegando le diverse attività tra di loro e comprendendo come ogni parte influenzi il sistema. In questo modo, infatti, si riduce il rischio di produrre soluzioni isolate e viene invece promosso un approccio integrato.

Non considereremo mai una pratica come indipendente e a sé stante: considerando anche il principio *Collaborate and promote visibility*, cercheremo di interconnettere i vari processi affinché si tengano in considerazione tutti i punti di vista.

6. Keep it Simple and Practical - Mantenere semplicità e praticità

Questo principio incoraggia a evitare la complessità e a mantenere le cose semplici e pratiche. L'obiettivo è semplificare i processi, le procedure e le attività senza compromettere l'efficacia.

Si cerca dunque di evitare inutili complessità nei processi progettati e di snellire i flussi di lavoro utilizzando il minor numero di step, semplificare la documentazione e garantendo la praticità nelle operazioni quotidiane.

Tenendo in considerazione questa linea guida, insieme ai principi *Start where you are* e *Progress iteratively*, cercheremo di produrre soluzioni semplici che contribuiscono alla creazione di valore.

7. Optimize and Automate - Ottimizzare e automatizzare

Questo principio ci invita a cercare costantemente modi per ottimizzare i processi esistenti e ad adottare soluzioni automatizzate ove possibile.

In caso si riveli possibile adottare soluzioni automatizzate, cercheremo di implementarle per ridurre al minimo l'utilizzo di risorse umane in queste task, in modo che queste possano dedicarsi ad altri processi.

5. PIANO EVOLUTIVO

Si presenta l'opportunità di migliorare i processi incorporando misure più proattive, come per esempio la verifica dell'applicazione di controllo delle scorte prima di effettuare un ordine al fornitore. Ciò potrebbe aiutare il gruppo di supporto a valutare rapidamente la disponibilità degli articoli ed a evitare ritardi causati dalle scorte.

L'incidente relativo alla sostituzione del monitor ha evidenziato che altri processi, anche se non direttamente coinvolti, possono influire sulla tempestività e sull'efficienza complessiva.

Pertanto, durante la revisione dei processi identificati, si terrà conto delle interazioni con processi correlati, come: *Change enablement*, *Problem management*, *Risk management*, *Knowledge management*, *Monitoring and event management*, *Portfolio management*, *Financial management*, *Service validation and testing*, *Measurement and reporting* per garantire una soluzione integrata e completa.

Questo approccio olistico assicura che le modifiche apportate ai processi principali siano coerenti con l'intero panorama operativo e che gli utenti finali possano beneficiare di un servizio migliorato in termini di tempi di risposta e disponibilità degli asset.

Si consideri inoltre che, per ogni processo ridefinito, si sono sempre tenuti in considerazione i 7 principi ITIL, rendendolo noto in maniera più o meno esplicita. Lo stesso ragionamento avviene anche per le 4 dimensioni, che saranno sempre insite nelle definizioni dei nuovi processi per il significato stesso di queste.

Si è quindi tentato di sviluppare i ragionamenti focalizzandosi sempre sull'importanza del valore per gli stakeholder coinvolti, partendo da un'analisi dei processi e servizi attuali per seguire una implementazione graduale e iterativa secondo gli obiettivi.

La collaborazione fra i vari team e il pensiero olistico sono quindi considerati affinché la collaborazione sia sempre efficace verificando tutte le influenze nel sistema e nelle attività.

Infine, si è tentato di sviluppare il tutto evitando le complessità, rendendo in modo chiaro e semplice gli sviluppi necessari per snellire il flusso di lavoro.

5.1 ANALISI DELLE FIGURE AZIENDALI

Si parte da un'analisi delle figure aziendali principali verificando il coinvolgimento o meno di queste e dei processi correlati nell'incidente:

- **Business Relationship manager:** è la figura che favorisce una relazione produttiva tra l'azienda ed i suoi partner commerciali. È verosimilmente coinvolta nell'accaduto in quanto l'errore si è verificato anche nella comunicazione fra le due parti;
- **Capacity manager,** ovvero la figura che garantisce la disponibilità e l'utilizzo ottimale delle risorse, è anch'esso responsabile in quanto non è stato in grado di rilevare l'assenza dell'apparecchiatura da sostituire;
- **Chief Financial Officer,** ovvero il responsabile delle iniziative finanziarie di un'azienda. Essendo una delle figure chiave della cosiddetta area AFC (Amministrazione, Finanza e Controllo), deve essere coinvolto nella pianificazione finanziaria a lungo termine e nel processo di budgeting;
- **End user,** in questo caso colui che ha richiesto la sostituzione del monitor, non ha responsabilità;
- Il **fornitore esterno** è responsabile di quanto accaduto, poiché non è stato in grado di fornire quanto stabilito dal SLA;
- L'**Incident manager,** ed il relativo processo coinvolto, non è direttamente responsabile al momento ma deve essere coinvolto a seguito dell'incidente accaduto;
- L'**IT financial manager,** cui processo correlato si occupa di fornire una gestione finanziaria delle risorse IT, considerando i fattori di qualità e rischio. Le analisi che ne derivano aiutano a creare una strategia ottimizzata e parametrata delle risorse IT. È quindi coinvolto nell'accaduto in quanto partecipa alla gestione delle risorse IT;
- Il **Service Desk manager,** responsabile della funzione di Service Desk, è coinvolto nell'accaduto ma il servizio correlato ha agito in modo corretto garantendo all'end user che il problema sarebbe stato risolto secondo un tempo breve stabilito, veicolando quindi le informazioni necessarie al gruppo di assistenza appropriato;
- Il **Service Level manager** ha il ruolo di garantire che gli SLA vengano rispettati e gestire eventuali violazioni in modo appropriato. In collaborazione con i team operativi,

nello scenario proposto il *service level manager* contribuisce a definire azioni correttive per risolvere la violazione e prevenire che si verifichi in futuro.

- Il **Service Request manager** non è coinvolto a seguito della richiesta di avere un nuovo terminale, in quanto l'accaduto comporta un' interruzione del servizio che chiama in causa l'ala dell'Incident Management;
- Il **Supplier manager**, il cui processo gestisce i fornitori per garantire la massima efficienza, è coinvolto in quanto il fornitore di monitor si è dimostrato inaffidabile e quindi probabilmente responsabile anch'esso nell'incidente, consci inoltre della già poca redditività del fornitore di apparecchiature IT.

5.2 DEFINIZIONE DEI NUOVI PROCESSI

5.1.1 Processo di IT Asset Management

Questa pratica si occupa di identificare e gestire gli asset IT all'interno dell'organizzazione. L'obiettivo è di garantire che hardware, software e altri elementi che contribuiscono a fornire servizi IT siano correttamente registrati e controllati.

Tra le varie attività di cui l'IT Asset manager è responsabile, troviamo proprio il supporto alla risoluzione di incidenti e il ritiro degli asset obsoleti.

Nello scenario proposto, l'IT Asset manager deve venire avvisato dal Support Group, in modo da procedere con il ritiro e la sostituzione del monitor guasto, con l'aggiornamento del controllo scorte ed eventuale ordine al fornitore (vedere pratica di *Availability Management*) e con la stesura di un report.

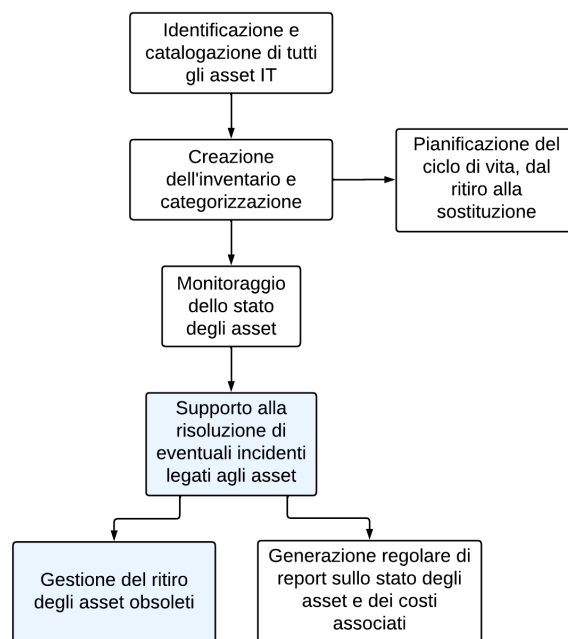


Figura 4: Flowchart della pratica di IT Asset Management.

Il pilastro su cui si basa l'intero processo di IT Asset Management è la catalogazione accurata degli asset: è necessario raccogliere le informazioni essenziali come il numero di serie, la data di acquisizione, il modello e l'ubicazione in modo da identificare e tracciare gli asset in modo univoco e affidabile.

Segue una naturale implementazione di un software automatizzato per il rilevamento delle risorse per mantenere un inventario accurato e sempre aggiornato, con annesso database di gestione della configurazione.

In accordo con la policy aziendale per cui è preferibile, quando possibile, acquistare software *off-the-shelf* piuttosto che svilupparne uno internamente, si consiglia l'adozione del software IBM Control Desk, che aiuta a gestire e ottimizzare le risorse IT aziendali, compresi hardware, software, contratti e licenze.

Tale applicativo ha un costo di circa €300 per licenza singola, al quale si deve aggiungere il costo delle attività di formazione.

Inoltre, è necessario seguire un approccio strategico che comprenda anche la categorizzazione degli asset. Questa consente di suddividere le risorse in categorie significative, riflettendo le loro criticità e l'importanza per le operazioni quotidiane.

Una categorizzazione accurata fornisce una base solida per migliorare la sicurezza: possiamo per esempio suddividere le risorse in base alla sensibilità dei dati che gestiscono, in modo da applicare misure di protezione più rigorose per gli elementi critici.

Grazie alla categorizzazione, anche il ciclo di vita diventa più gestibile: è possibile pianificare in modo proattivo il ritiro, l'aggiornamento o la sostituzione in modo da ridurre i rischi operativi e i costi associati ad incidenti.

Nella tabella di seguito vediamo un esempio di categorizzazione degli asset:

Categoria	Descrizione
Hardware	server, laptop, monitor, workstations, stampanti, dispositivi di archiviazione, etc
Software e licenze software	sistemi operativi, applicazioni aziendali, applicazioni di produttività, software di gestione, licenze, etc.
Risorse di rete	router, VPN, switch, etc.
Sicurezza	firewall, antivirus, strumenti di rilevamento minacce

Tabella 1: Categorizzazione degli asset.

Nel caso del monitor in questione, diremo che questo appartiene alla categoria *hardware*.

Vengono inoltre definiti i seguenti criteri per la classificazione degli asset:

- **Criticità operativa (CO):** si riferisce all'importanza nel mantenimento e nell'esecuzione delle attività operative quotidiane;
- **Sensibilità dei dati (SD):** è una valutazione del livello di riservatezza e importanza delle informazioni contenute nell'asset in questione;
- **Rilevanza per il business (RB):** indica quanto sia critico o importante per gli obiettivi strategici e operativi dell'organizzazione;
- **Impatto finanziario (IF):** rappresenta la stima del costo economico associato alla perdita dell'asset o della sua compromissione. Vengono considerati anche gli effetti collaterali indiretti.

Per ogni criterio viene assegnato un punteggio da 1 a 5, dove 1 indica ‘bassa importanza’ mentre 5 è indice di ‘alta importanza’.

Questa valutazione funge da ulteriore criterio di categorizzazione e permette di adottare misure adeguate in base al punteggio ottenuto per ogni criterio, concentrando le risorse nelle aree più critiche. Per esempio, un asset con un alto punteggio per la criticità operativa necessita di maggiore attenzione, che si concretizza in attività di manutenzione più frequenti e mirate.

Di seguito, la matrice RACI della pratica, che individua le figure responsabili del processo.

Attività	IT Asset manager	Incident manager	Fornitore esterno	Divisione sicurezza
Rilevazione asset	R/A	-	-	-
Catalogazione asset	R/A	-	-	C
Monitoraggio stato asset	R/A	-	-	-
Ritiro asset	R/A	-	-	-
Report su stato degli asset	R/A	-	-	-
Supporto incidenti	R/A	C	-	-
Pianificazione manutenzione	C/A	-	R	I

Tabella 2: RACI matrix per la pratica di IT Asset Management.

5.1.2 Processo di Supplier Management

Nel processo di *Supplier Management* è comune utilizzare diverse valutazioni e criteri per valutare i fornitori. La valutazione dei fornitori è una pratica fondamentale: aiuta ad identificare e mitigare i rischi associati alle forniture, monitora e garantisce che i prodotti siano conformi agli standard di qualità richiesti e consente di identificare opportunità di risparmio.

A tal fine, introduciamo i seguenti indicatori chiave di prestazione (KPIs). Ognuno di essi consente di individuare un punteggio utilizzabile in seguito per determinare l'affidabilità del fornitore.

- **On time delivery (OTD):** percentuale di consegne effettuate entro i termini previsti, di seguito indicato con *otd*.

$$otd = \frac{\text{ordini puntuali}}{\text{totale ordini}} * 100$$

$otd \geq 95\%$	5 punti
$90\% \leq otd < 95\%$	4 punti
$85\% \leq otd < 90\%$	3 punti
$70\% \leq otd < 85\%$	2 punti
$otd < 70\%$	1 punto

Tabella 3: Valori di riferimento per la metrica On time delivery.

- **Perfect order rate (POR) :** la percentuale di ordini consegnati senza errori, come prodotti errati, discrepanze di quantità o danni, di seguito indicato con *por*.

$$por = \frac{\text{ordini corretti}}{\text{totale ordini}} * 100$$

$por \geq 98\%$	5 punti
$94\% \leq por < 98\%$	4 punti
$90\% \leq por < 94\%$	3 punti
$85\% \leq por < 90\%$	2 punti
$por < 85\%$	1 punto

Tabella 4: Valori di riferimento per la metrica Perfect order rate.

Lead time: tempo medio necessario al fornitore per evadere un ordine dalla ricezione alla consegna, di seguito indicato con *lt*;

$lt < 2g$	5 punti
$2g \leq lt < 5g$	4 punti
$5g \leq lt < 10g$	3 punti

$10g \leq lt < 30g$	2 punti
$lt \geq 30g$	1 punto

Tabella 5: Valori di riferimento per la metrica Lead time.

- **Responsività:** velocità ed efficacia con cui il fornitore risponde alle richieste e ai problemi, di seguito indicata con r ;

$r < 6h$	5 punti
$6h < r < 12h$	4 punti
$12h < r < 24h$	3 punti
$24h < r < 72h$	2 punti
$r > 72h$	1 punto

Tabella 6: Valori di riferimento per la metrica Responsività.

- **Margine di redditività annuale:** percentuale di profitto ottenuta da un fornitore rispetto al totale delle entrate annue, di seguito indicato con mra ;

$$mra = \frac{\text{profitto netto}}{\text{ricavi totali}} * 100$$

$mra \geq 15\%$	5 punti
$10\% \leq mra < 15\%$	4 punti
$5\% \leq mra < 10\%$	3 punti
$1\% \leq mra < 5\%$	2 punti
$mra < 1\%$	1 punto

Tabella 7: Valori di riferimento per la metrica Margine di redditività annuale.

Un semplice rapporto ci permette anche di dare un voto su base decimale, espresso come *voto* dato il *punteggio* ottenuto:

$$voto : 10 = punteggio : 25$$

Per il principio di *Continual Improvement*, queste valutazioni verranno aggiornate su base annuale in modo da raccogliere feedback e monitorare l'efficacia del nuovo processo.

Un ulteriore strumento che può aiutare nella valutazione dei fornitori è la *matrice di Kraljick*, che prevede la classificazione di prodotti o servizi offerti dai fornitori in base al loro rischio di approvvigionamento (*supply risk*) e all'impatto sui profitti (*profit impact*). Questo strumento aiuta a pianificare gli approcci di gestione degli acquisti e ad allocare le risorse nel modo più efficiente, in base al profilo di ciascuna categoria d'acquisto.

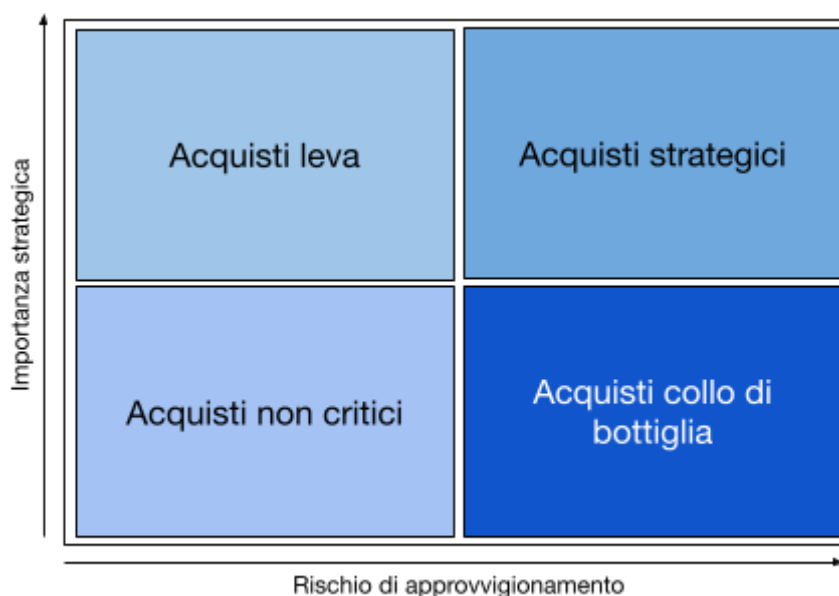


Figura 5: Matrice di Kraljick.

Inoltre, dal testo di riferimento si legge che “tutta la manutenzione dell'hardware IT all'interno della sede centrale è affidata a un unico fornitore che non è stato redditizio nell'ultimo esercizio”. Questo solleva un problema circa l'affidamento ad un solo fornitore senza la valutazione o la consulenza di un'alternativa.

Questo dettaglio contribuisce in larga misura alla violazione del SLA: se ci fosse stato un fornitore alternativo, l'azienda avrebbe potuto riferirsi a quest'ultimo per una risoluzione più celere del problema. Infatti, fare affidamento ad un fornitore unico espone la banca a un

rischio maggiore di interruzione dell'attività.

Va introdotta quindi una matrice dove si manifestano due o più fornitori, su base territoriale, per ogni fornitura IT necessaria: questa stratificazione permette di avere sempre una panoramica completa di tutti i *Suppliers*.

Questa matrice deve coesistere con la valutazione dei fornitori secondo le metriche descritte sopra, in modo che risalti sempre il *Supplier* migliore secondo i criteri stabiliti.

	Monitor		Mouse		Tastiere		Server		...
Italia	Az1	Az3	Az1	Az2	Az2	Az3	Az4	Az1	...
Svizzera	Az1	Az4	Az1	Az2	Az2	Az3	Az4	Az1	...
Germania	Az5	Az1	Az1	Az3	Az2	Az1	Az1	Az3	...
...

Tabella 8: Esempio di matrice fornitura/area geografica.

Applicando la dimensione ITIL *Information and technology*, è consigliabile implementare un software di *Supplier Relationship Management* (SRM), che consente di archiviare e centralizzare tutti i dati dei fornitori, tra cui ad esempio i KPI precedentemente descritti, e tenere sotto controllo gli ordini di acquisto ed i contratti.

Il mercato offre molteplici soluzioni *off-the-shelf*: in accordo con la policy aziendale, suggeriamo l'utilizzo di *ProcureWare*, una delle soluzioni software più diffuse, la cui licenza base *enterprise* ha un costo di circa €11.600 e comprende l'eventuale formazione del personale, essenziale per garantire che tutti i membri del team siano a conoscenza delle linee guida per implementare il cambiamento in modo efficace.

Infine, volendo definire più nel dettaglio il processo di Supplier Management, abbiamo identificato le attività principali da eseguire e le relative figure coinvolte.

Attività	Supplier manager	Utente finale	Risk manager	CFO
Identificazione fornitori	R/A	-	-	-
Selezione dei fornitori	R/A	-	-	-
Negoziiazione contratti	R/A	-	-	I
Monitoraggio delle prestazioni e valutazione dei fornitori	R/A	C	-	-
Gestione del rischio fornitore	C	-	R/A	-
Raccolta feedback	R/A	C	-	-

Tabella 9: RACI matrix della pratica di Supplier Management.

Gli output di questo processo sono i report sulle prestazioni dei fornitori, in base alle metriche descritte sopra, e tutta la documentazione relativa all'identificazione e alla selezione.

Nel caso del fornitore in analisi, valutandolo con le metriche proposte, ci si accorge subito di come si possa prevenire in futuro una situazione simile a quella che ha causato il problema con il fornitore di monitor.

Nel dettaglio, assumiamo che il fornitore in questione ottenga il seguente punteggio:

On time delivery (OTD)	3
Perfect order rate (POR)	3
Lead Time	1
Responsività	2
Margine di redditività annuale	2
TOTALE	11

Tabella 10: Valutazioni del fornitore in base alle metriche proposte.

Notando come il massimo punteggio raggiungibile sia 25, il valore ottenuto risulta ben al di sotto di un buon risultato.

Esprimendo su base decimale, si ottiene un *voto* = 4.4

Questo è un indicatore di allarme per l'azienda, che preventivamente dovrebbe valutare un fornitore migliore per l'anno che segue.

Volendo categorizzare il monitor in base alla matrice di *Kraljic* descritta sopra, questo risulta essere un 'acquisto non critico' in quanto materiale a bassa importanza strategica e di facile approvvigionamento. Tale classificazione suggerisce di automatizzare e standardizzare quanto più possibile il processo di approvvigionamento, come verrà successivamente proposto nella ridefinizione del processo di *Availability Management*.

5.1.3 Processo di Availability Management

Il processo di Availability Management è essenziale per garantire un elevato livello di produttività, minimizzando il downtime dovuto alla rottura dei monitor.

Il processo va ridefinito in modo da garantire che tutte le richieste di sostituzione monitor siano evacuate entro i tempi definiti dallo SLA.

- Assumiamo che la frequenza di rottura media sia di 2 monitor al mese.
- Assumiamo che la banca effettui un ordine al fornitore primario ogni 6 mesi per riempire la capacità imposta del magazzino.
- Assumiamo che la soglia minima sia di 5 monitor, in modo da garantire eventuale copertura per mediamente 2 mesi.
- Assumiamo che nel caso in cui si scenda sotto la soglia minima, la banca effettui un ordine per riportare in magazzino alla capacità massima imposta.

Dunque, la capacità massima del magazzino sarà di $2 * 6 = 12$ monitor, a cui aggiungiamo una scorta di 3 monitor, per un totale di 15.

- Il budget iniziale ammonta a €1500. Infatti, il prezzo medio di un monitor da ufficio si aggira intorno ai €100 e la banca necessita di 15 monitor per il primo approvvigionamento. Vista la natura dell'azienda, questa viene considerata una somma adeguata.
- Il prezzo medio semestrale è di €1000. Infatti, ricordando la frequenza media di rottura di 2 monitor al mese, si raggiungerebbe il 5° mese scendendo sotto la soglia di 5 scorte in magazzino, facendo scattare in automatico un riordino di 10 monitor per un costo totale di €1000 ogni sei mesi.

Questo dato verrà fornito al *Change enablement management* per una successiva valutazione e approvazione.

Questo nuovo processo richiede l'adozione di un *inventory management software* che, in base a quanto descritto, è già in dotazione alla banca ma nella gestione dell'incidente non è stato consultato a dovere.

Per il principio ITIL *Start where you are*, assumiamo che tale applicativo sia già sufficiente a soddisfare le richieste del processo, senza quindi necessità di acquistare un nuovo software ERP di terze parti o di avviare uno sviluppo interno.

Per quanto riguarda la dimensione *'People'* invece, i due team responsabili sono il Support Group, che si occupa di controllare la disponibilità dei monitor, e il gruppo di gestione degli asset IT che ha la responsabilità di aggiornare l'inventario, come vedremo nel prossimo processo.

Attività	Availability manager	Support group	IT financial manager	IT Asset manager	CFO
Controllo scorte magazzino	A/I	R	I	I	-
Approvazione del budget per ordinare nuovi monitors	C	-	A/R	-	I
Aggiornamento software di controllo scorte	C	I	-	A/R	-

Tabella 11: RACI matrix per la pratica di Availability Management.

5.1.4 Processo di Incident Management

Abbiamo assunto che il software di controllo in dotazione alla banca sia già sufficiente per la corretta implementazione del processo di Availability Management.

Tuttavia, il gruppo di supporto non lo ha consultato prima di effettuare un ordine al fornitore primario, quindi va ridefinito il processo con il quale si gestiscono problemi di questo tipo.

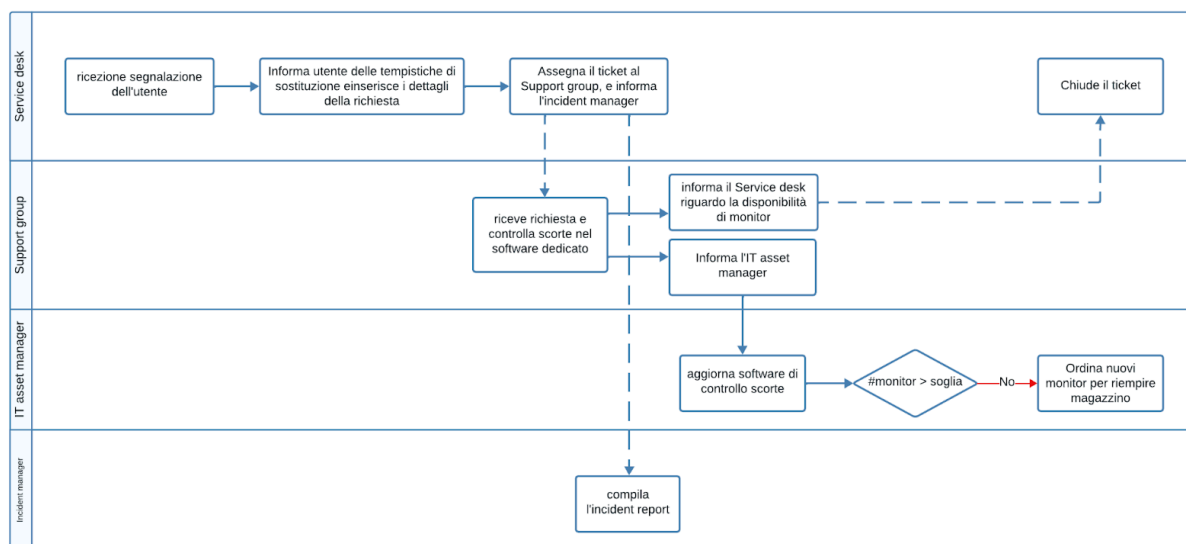


Figura 6: Flowchart della pratica di Incident Management.

Come si vede dal diagramma, questo processo in realtà è interdipendente con altre pratiche ITIL e diverse figure vengono coinvolte per garantire una corretta risoluzione del problema.

Le persone o i team direttamente coinvolti sono:

- il *Service Desk agent* che si occupa della comunicazione con l'utente e ha il compito di inoltrare la richiesta di supporto al gruppo adeguato e di informare l'incident manager dell'inconveniente;
- il *gruppo di supporto*, che è responsabile del controllo scorte per dare informazioni al Service Desk e deve anche informare l'IT Asset manager;
- l'*IT Asset manager* che ha il compito di aggiornare il software di controllo scorte dopo aver sostituito il monitor, ed effettuare un nuovo ordine nel caso in cui le scorte siano sotto la soglia minima di magazzino;
- l'*incident manager*, che ha il compito di compilare il report e monitorare la gestione dell'incidente affinché questa sia efficace e avvenga entro i tempi stabiliti dallo SLA.

Attività	Service Desk agent	Support group	End user	Incident manager	IT Asset manager
Compilazione <i>Incident report</i>	C	I	C	R/A	I
Prima comunicazione all'utente	R/A	C	I	-	-
Verifica scorte tramite software di controllo	-	R/A	-	-	-
Verifica dell'inventario	I	C	-	-	R/A
Aggiornamento del software di controllo	-	C	-	-	R/A
Notifica finale all'utente	R	I	I	I	I

Tabella 12: RACI matrix per la pratica di Incident Management.

Data la forte correlazione tra i processi di *Incident Management* e *Problem management*, anche il problem manager dovrà essere informato dell'incidente avvenuto, in modo da consultare il report e analizzare la causa alla radice per prevenirne la ricorrenza.

In questo modo, l'approccio adottato è proattivo anziché reattivo.

Dal testo si legge che la banca ha già a disposizione degli strumenti di rilevamento automatico di errori e che la pratica di *Incident Management* è ben consolidata ed efficace.

Assumiamo dunque che esista anche un '*Known error database*' (KEDB) dove documentare e gestire gli incidenti, riportando le relative soluzioni. Assumiamo che non sia ancora presente una soluzione a breve termine per l'inconveniente registrato dall'utente.

È quindi necessario registrarlo, aggiungendo al database la seguente entry:

Titolo del problema	Monitor esauriti
ID Known Error	#id
Data	gg/mm/aaaa
Descrizione del problema	Un utente ha segnalato un problema con il monitor del proprio computer. Non sono disponibili monitor per la sostituzione tempestiva.
Radice del problema	Non è presente una scorta in magazzino.

Soluzione temporanea	Ordinare al fornitore un nuovo monitor.
Soluzione permanente	-

Tabella 13: Esempio di entry nel KEDB per l'incidente dello scenario.

È bene notare come, se fosse presente un'azione correttiva definitiva, il problema 'monitor esauriti' non dovrebbe più ripresentarsi.

Dobbiamo infine assumere che il *problem manager* consulti il database e, in collaborazione con il team adeguato, fornisca una soluzione permanente.

In questo caso, la soluzione proposta è descritta sopra nel processo di Availability Management.

5.3 IMPLEMENTAZIONE DEL CAMBIAMENTO

La gestione del cambiamento è una parte cruciale per assicurarsi che i cambiamenti proposti siano implementati correttamente e richiede una pianificazione e un coordinamento attenti.

Dal documento in analisi, inoltre, si evince come il processo di cambiamento non sia ben consolidato in quanto non esiste un passaggio formale di valutazione dei cambiamenti. Vanno quindi riviste in parte le modalità che coinvolgono il cambiamento, ridefinendo il flusso, come mostrato in [Figura 7](#).

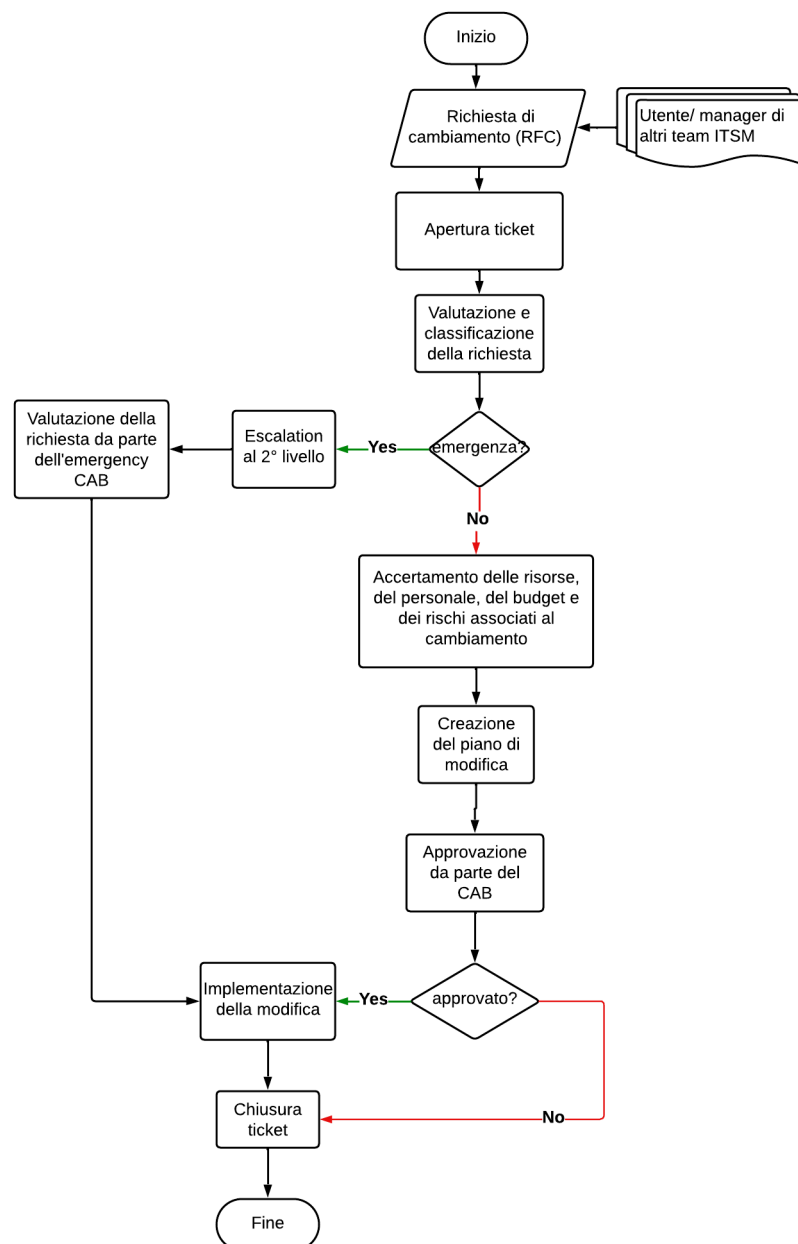


Figura 7: Flowchart della pratica di Change Enablement Management.

Dopo aver identificato i cambiamenti necessari e valutato la portata di ciascun cambiamento, è necessario coinvolgere tutte le parti interessate e comunicare in modo chiaro la necessità di adottare le nuove misure proposte.

A questo proposito, il *Change enablement manager*, in collaborazione con il *release manager*, ha il compito di:

- pianificare il cambiamento definendo risorse, persone, strumenti e budget;
- fornire formazione adeguata per assicurarsi che il personale sia preparato ad adottare i nuovi processi;
- mettere in atto l'implementazione dei cambiamenti;
- condurre test per valutare l'efficacia del cambiamento e raccogliere feedback per apportare eventuali miglioramenti;
- valutare l'impatto dei cambiamenti dopo l'implementazione.

Si legge dal testo che non è presente un processo formale di valutazione dei cambiamenti per fornire supporto.

Definiamo quindi i seguenti indicatori chiave di performance (KPIs) che verranno considerati su base semestrale:

- **Numero di cambiamenti non autorizzati:** un numero basso indica che il processo di approvazione è solido e in grado di gestire tutti i cambiamenti.

Livello	Valore
Eccellente	0-1 cambiamenti
Buono	2-5 cambiamenti
Accettabile	6-10 cambiamenti
Sfavorevole	11-15 cambiamenti
Critico	> 15 cambiamenti

Tabella 14: Valori di riferimento per il numero di cambiamenti non autorizzati.

- **Numero di richieste di servizi ad alto impatto soddisfatte senza un cambiamento:** un numero elevato è segno di un'infrastruttura vulnerabile a problematiche.

Livello	Valore
Eccellente	0-1 richieste
Buono	2-5 richieste
Accettabile	6-10 richieste
Sfavorevole	11-15 richieste
Critico	> 15 richieste

Tabella 15: Valori di riferimento per il numero di richieste soddisfatte senza un cambiamento.

- **Percentuale delle modifiche seguite da rollback:** un numero elevato è un indicatore di cambiamenti mal pianificati.

Livello	Valore
Eccellente	0-2%
Buono	3-5%
Accettabile	6-8%
Sfavorevole	9-12%
Critico	> 12%

Tabella 16: Valori di riferimento per la percentuale delle modifiche seguite da rollback.

- **Percentuale di accettazione dei cambiamenti:** un numero elevato è segno che le tue modifiche e la pianificazione sono solide.

Livello	Valore
Eccellente	90-100%
Buono	80-89%
Accettabile	70-79%

Sfavorevole	60-69%
Critico	< 60%

Tabella 17: Valori di riferimento per la percentuale di accettazione dei cambiamenti.

- **Deviazione dal programma:** indica se le modifiche sono implementate secondo la tabella di marcia e se aderiscono al piano dei cambiamenti.

Livello	Valore
Eccellente	0-2 giorni
Buono	3-5 giorni
Accettabile	6-8 giorni
Sfavorevole	9-12 giorni
Critico	> 12 giorni

Tabella 18: Valori di riferimento per i giorni di deviazione dal programma.

- **Numero di incidenti causati da un cambiamento:** un numero elevato è segno della necessità di una migliore comunicazione dei cambiamenti.

Livello	Valore
Eccellente	0-1 incidenti
Buono	2-5 incidenti
Accettabile	6-10 incidenti
Sfavorevole	11-15 incidenti
Critico	> 15 incidenti

Tabella 19: Valori di riferimento per il numero di incidenti causati da un cambiamento.

- **Percentuale di cambiamenti completati in tempo:** più alta è la percentuale, migliore è il processo di gestione dei cambiamenti.

Livello	Valore
Eccellente	90-100%
Buono	80-89%
Accettabile	70-79%
Sfavorevole	60-69%
Critico	< 60%

Tabella 20: Valori di riferimento per la percentuale di cambiamenti completati in tempo.

5.3.1 Piano di rollout

Settimana uno

Obiettivo: comunicare le modifiche alle pratiche che verranno implementate

Partecipanti: Change manager, CIO, IT Asset manager, Supplier manager, availability manager, incident manager, Service Desk, problem manager.

Attività previste:

- annuncio delle modifiche alle pratiche di IT Asset Management, Supplier Management, Availability Management e Incident Management;
- annuncio dei nuovi software per IT Asset Management e Supplier Management.

Checkpoint: ogni manager informa il resto del team delle modifiche che verranno effettuate.

Settimana due

Obiettivo: formazione del personale

Partecipanti: IT Asset Management team, Supplier Management team, Availability Management team, Incident Management team, Release Management team.

Attività previste:

- formazione IT Asset Management team su utilizzo del software IBM Control Desk;
- formazione Supplier Management team su utilizzo del software ProcureWare;
- installazione nuovi software;

- configurazione strumenti aggiornati di IT Asset Management, Supplier Management, Availability Management e Incident Management.

Checkpoint: incontro con manager dei team coinvolti per ricevere feedback sulle nuove applicazioni software e sul processo di formazione.

Settimana tre

Obiettivo: implementazione dei cambiamenti

Partecipanti: IT Asset Management team, Supplier Management team, Availability Management team, Incident Management team, Release management team.

Attività previste:

- inizio utilizzo dei nuovi software implementati;
- implementazione nuovi flussi di lavoro.

Checkpoint: chiedere a coloro coinvolti di completare un sondaggio per condividere il loro feedback sulle nuove applicazioni software e sulla formazione ricevuta.

Settimana quattro

Obiettivo: valutazione dei cambiamenti

Partecipanti: Change manager, IT Asset manager, Supplier manager, availability manager, incident manager, problem manager.

Attività previste:

- incontro con i manager per esaminare i feedback precedentemente raccolti.

Checkpoint: i diversi manager comunicano ai rispettivi team l'avvenuta implementazione del cambiamento.

Le attività previste dal piano di *rollout* per l'implementazione del cambiamento sono riportate nel seguente diagramma di Gantt.

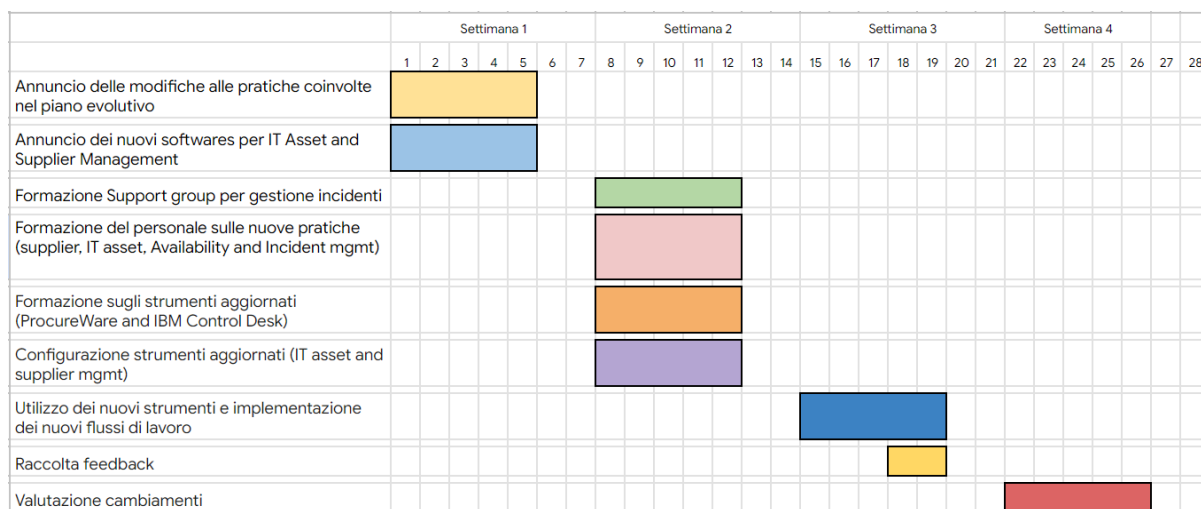


Figura 7: GANTT del piano evolutivo.

Al termine di questo periodo, se le valutazioni dei manager risultano positive, il cambiamento viene chiuso e considerato come consolidato.

Per il principio di *Continual Improvement* è necessario che vi sia un processo di valutazione ricorrente e successivo alla chiusura del cambiamento, basato sulle metriche introdotte precedentemente.

Come anticipato, le valutazioni hanno periodicità semestrale e verranno inserite nello strumento per la gestione ITSM in dotazione della banca.