

# I PROCESSI DI SERVICE OPERATION

---

REQUEST FULFILMENT



Il processo di **Request Fulfilment** è nuovo con ITIL v3.

Gli obiettivi di questo processo sono i seguenti:

- Fornire agli utenti un canale per richiedere (e ricevere) servizi standard per i quali esiste uno schema predefinito di approvazione (i.e. richiesta di un computer)
- Fornire agli utenti informazioni sui servizi disponibili e sulle procedure per ottenerli
- Fornire i servizi standard di cui sopra agli utenti finali
- Assistere gli utenti su richieste generiche, consigli e lamentele



Nell'ambito del processo di Request Fulfilment si definisce la **Service Request** come:

una richiesta da un utente per un informazione, consiglio, un cambiamento standard (standard change) o per un accesso ad un servizio IT



Le attività del processo di **Request Fulfilment** in ITIL v2 erano incluse nel processo di **Incident Management**, ove si suggeriva di utilizzare per le **Service Request** lo stesso **workflow** degli incidenti.

Uno dei motivi per cui si è deciso di separare le due cose è che gli **incidenti** sono non-schedulabili o non-pianificabili, mentre le **Service Request** possono e devono essere pianificate.

Per ogni tipologia di **Service Request** dovrebbe esserci un chiaro flusso di attività che determini la fornitura (o non approvazione) del particolare servizio all'utente.



Stante la particolare natura delle **Service Request**, queste posso essere aperte solo in presenza di:

- Una **voce di catalogo** che le prevede esplicitamente
- Un **WF** definito per quella voce
- **Ruoli** definiti per l'esigenza
- **Costo preventivato** (sia economico che di effort uomo)
- Uno **SLA** garantito con tempi certi
- Un **rischio** molto basso, praticamente nullo
- La **delega ad approvare** la Service Request da parte di personale diverso dal CAB



## Request Model:

Alcune Service Request occorrono frequentemente e, quindi, necessitano di essere gestite in modo consistente al fine di garantire il raggiungimento degli SLA concordati.

Per venire incontro a queste esigenze, molte organizzazioni creano dei flussi di attività che prendono il nome di Request Model.

## Menu Selection:

Le Service Request sono particolarmente adatte ad una gestione Self-Service dove l'utente può selezionare in autonomia la voce di catalogo interessata e compilare il form che ne permette l'apertura.



## Request Status Tracking:

Le SR devono essere monitorate durante tutto il loro ciclo di vita. Gli **Status Code** servono appunto a questo (es. draft, in review, suspended, waiting authorization, rejected, cancelled, in progress, completed, closed)

## Prioritizing Requests:

Alla stregua degli incidenti, anche le SR devono essere prioritizzate con logiche e matrici simili a quelle utilizzate nell'Incident Management.



## Escalating Request:

In alcune condizioni, può essere necessario (es. misrouting alla funzione sbagliata, SLA vicino alla rottura, problemi di soddisfazione del cliente, SR aperta in vece di una richiesta più complessa o di una RFC)

## Financial Approval:

Anche se tutto è previsto, le SR che richiedono un investimento aziendale devono essere approvate dalla funzione prevista (delega del CAB)



## Escalating Request:

In alcune condizioni, può essere necessario (es. misrouting alla funzione sbagliata, SLA vicino alla rottura, problemi di soddisfazione del cliente, SR aperta in vece di una richiesta più complessa o di una RFC)

## Financial Approval:

Anche se tutto è previsto, le SR che richiedono un investimento aziendale devono essere approvate dalla funzione prevista (delega del CAB)



Il processo, in generale include i seguenti passi:

- Richiesta da parte dell'utente - può essere fatta sia attraverso il Service Desk che attraverso meccanismi automatici (per esempio via intranet/internet)
- Approvazione finanziaria (se rilevante) - chi di dovere dovrebbe approvare i costi relativi alla richiesta. In molti casi questi possono essere pre-approvati (per esempio, per tutto lo staff si approva la fornitura di un nuovo computer ogni due anni, dietro richiesta)

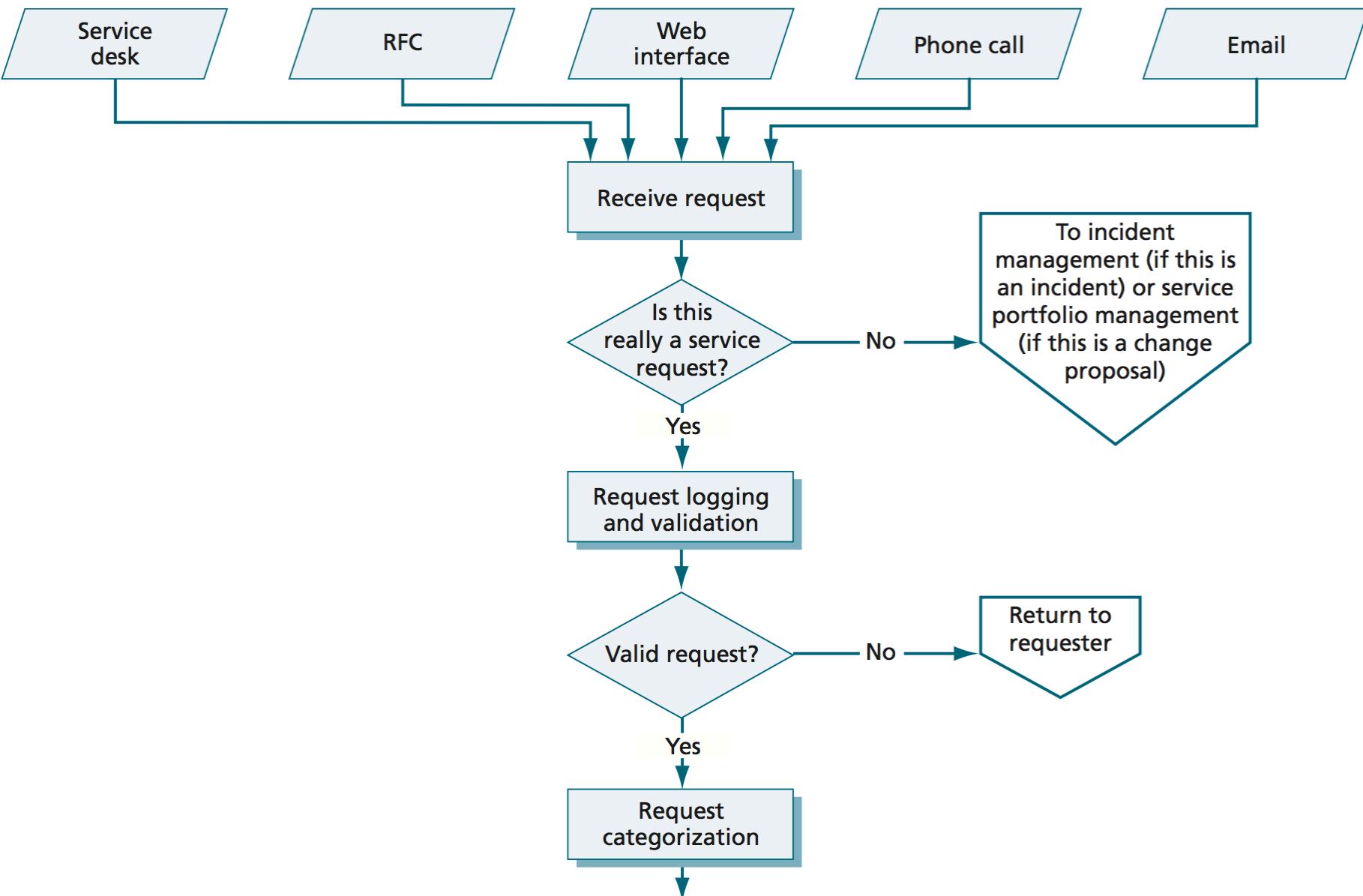


- Altre approvazioni - in molti casi approvazioni aggiuntive possono essere necessarie (per esempio, per avere un computer high-end ci vuole una ulteriore approvazione)
- Compimento della richiesta - spesso effettuata dallo stesso Service Desk, oppure responsabilità di gruppi specifici (per esempio i magazzinieri possono essere responsabili della consegna del computer all'utente)
- Chiusura - questa fase del processo è simile alla chiusura degli incidenti: la si può fare solo controllando se l'utente è soddisfatto.

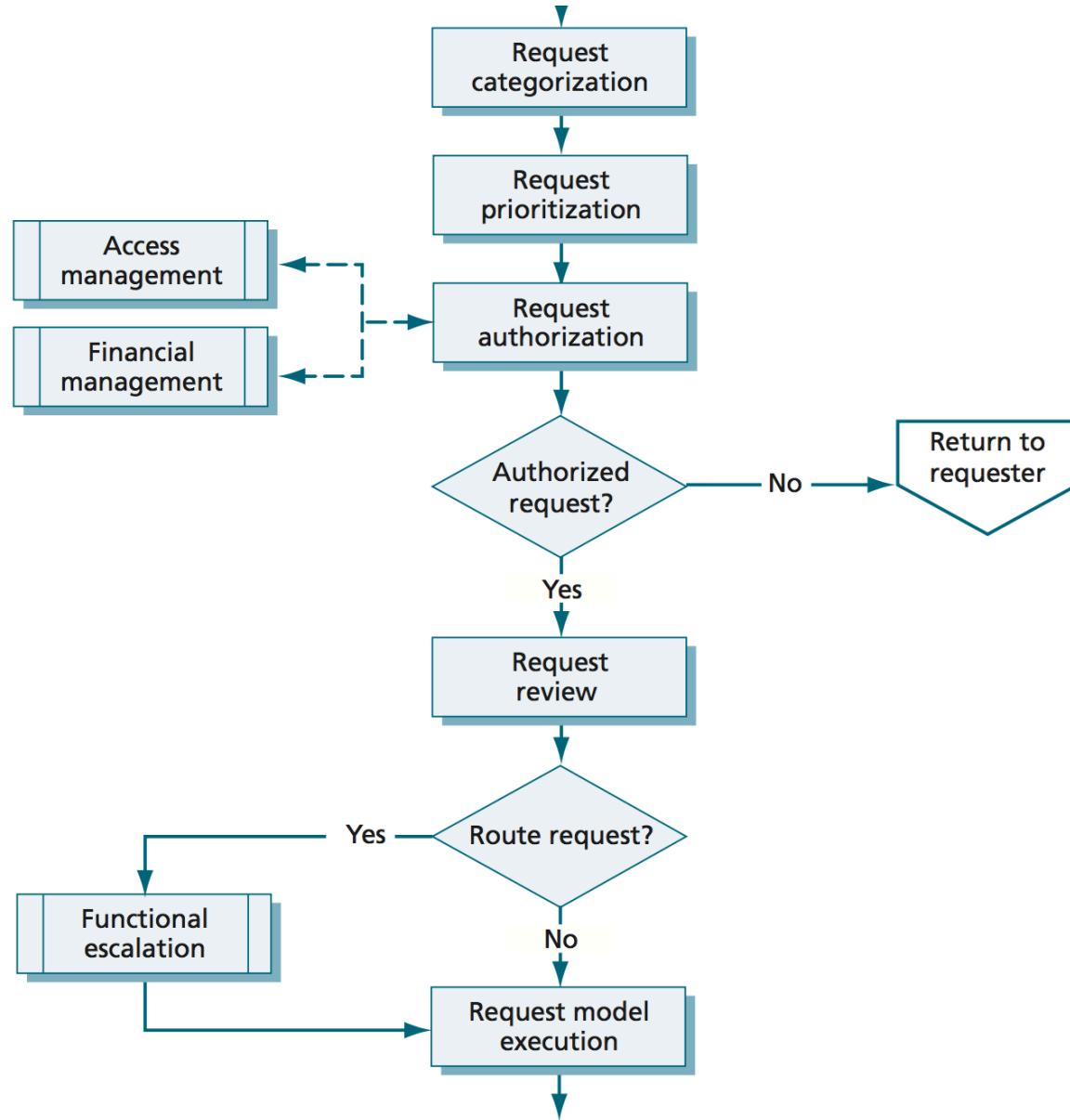


Una parte cruciale per l'implementazione del processo è la definizione delle richieste per una accurata pianificazione dei processi di fornitura per ogni tipo di richiesta (**Catalogo delle Service Request**)

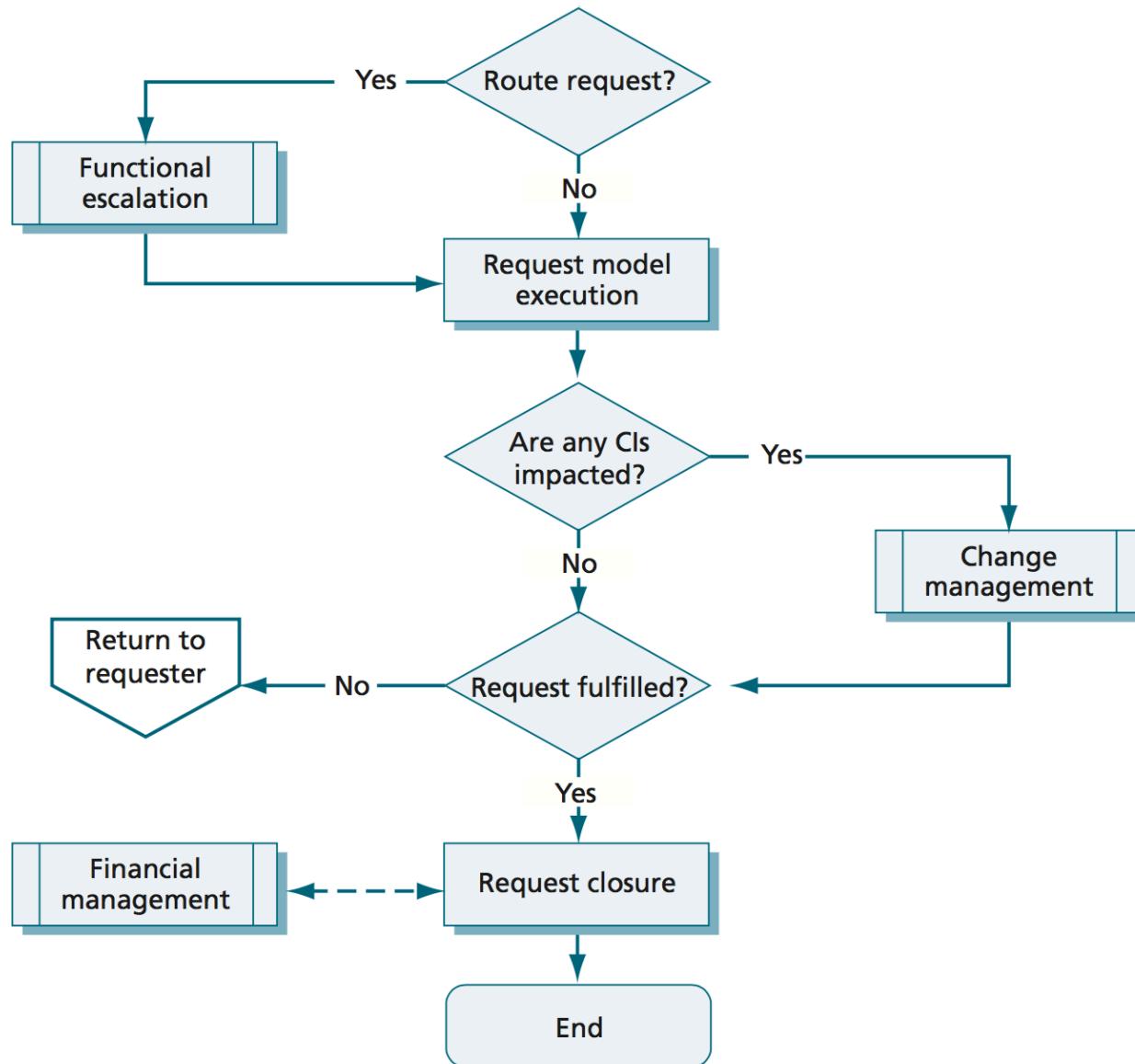
# REQUEST FULFILMENT: IL FLUSSO



# REQUEST FULFILMENT: IL FLUSSO



# REQUEST FULFILMENT: IL FLUSSO





# ESEMPIO DI INFORMAZIONI NECESSARIE PER LA GESTIONE DELLE SERVICE REQUEST

- Unique reference number
- Request categorization (often broken down into sub-categories including which service the request is being asked for)
- Request urgency
- Request impact
- Request prioritization
- Date/time recorded
- Name/ID of the person and/or group making the request
- Method of notification (telephone, web interface, RFC, email, in person etc.)
- Name/department/phone/location of user
- Budget centre in case a charge is associated
- User 'hours of working' (e.g. 9–5 weekdays)
- Call-back method (telephone, mail etc.)
- Description of request
- Request status (in progress, waiting authorization, closed etc.)
- Related CIs
- Support group/person to which the service request will be allocated
- Fulfilment date and time
- Closure date and time.



**CSF Requests** must be fulfilled in an efficient and timely manner that is aligned to agreed service level targets for each type of request

**KPI** The mean elapsed time for handling each type of service request

**KPI** The number and percentage of service requests completed within agreed target times

**KPI** Breakdown of service requests at each stage (e.g. logged, work in progress, closed etc.)

**KPI** Percentage of service requests closed by the service desk without reference to other levels of support (often referred to as ‘first point of contact’)

**KPI** Number and percentage of service requests resolved remotely or through automation, without the need for a visit

**KPI** Total numbers of requests (as a control measure)

**KPI** The average cost per type of service request



**CSF** Only authorized requests should be fulfilled

**KPI** Percentage of service requests fulfilled that were appropriately authorized

**KPI** Number of incidents related to security threats from request fulfilment activities



## CSF User satisfaction must be maintained

**KPI** Level of user satisfaction with the handling of service requests (as measured in some form of satisfaction survey)

**KPI** Total number of incidents related to request fulfilment activities

**KPI** The size of current backlog of outstanding service requests.

# I PROCESSI DI SERVICE OPERATION

---

PROBLEM MANAGEMENT



Lo scopo di questa disciplina è quello di gestire tutti i problemi dei servizi IT.

Il suo obiettivo principale è quello di identificare le cause di origine di tali problemi e raccomandare modifiche ai Cls tramite il Change Management.

Il processo di PM usa le informazioni raccolte da varie aree, tra cui Incident e Change Management.



Si focalizza su queste aree:

- **Problem Control:** trovare la causa di origine degli incidenti
- **Error Control:** correggere i problemi, gestire le informazioni relative ai problemi ed ai known errors



- Il primo obiettivo del processo di PM consiste nel minimizzare l'impatto sul business degli incidenti e dei problemi che sono causati da errori all'interno dell'infrastruttura IT
- Il secondo è quello di prevenire il ripetersi di incidenti dovuti a tali errori
- Per raggiungere tale scopo, il PM cerca di trovare le cause di origine degli incidenti e poi di dare inizio ad azioni volte a migliorare o correggere la situazione
- Tra le responsabilità del PM c'è quella di garantire che le suddette informazioni siano documentate



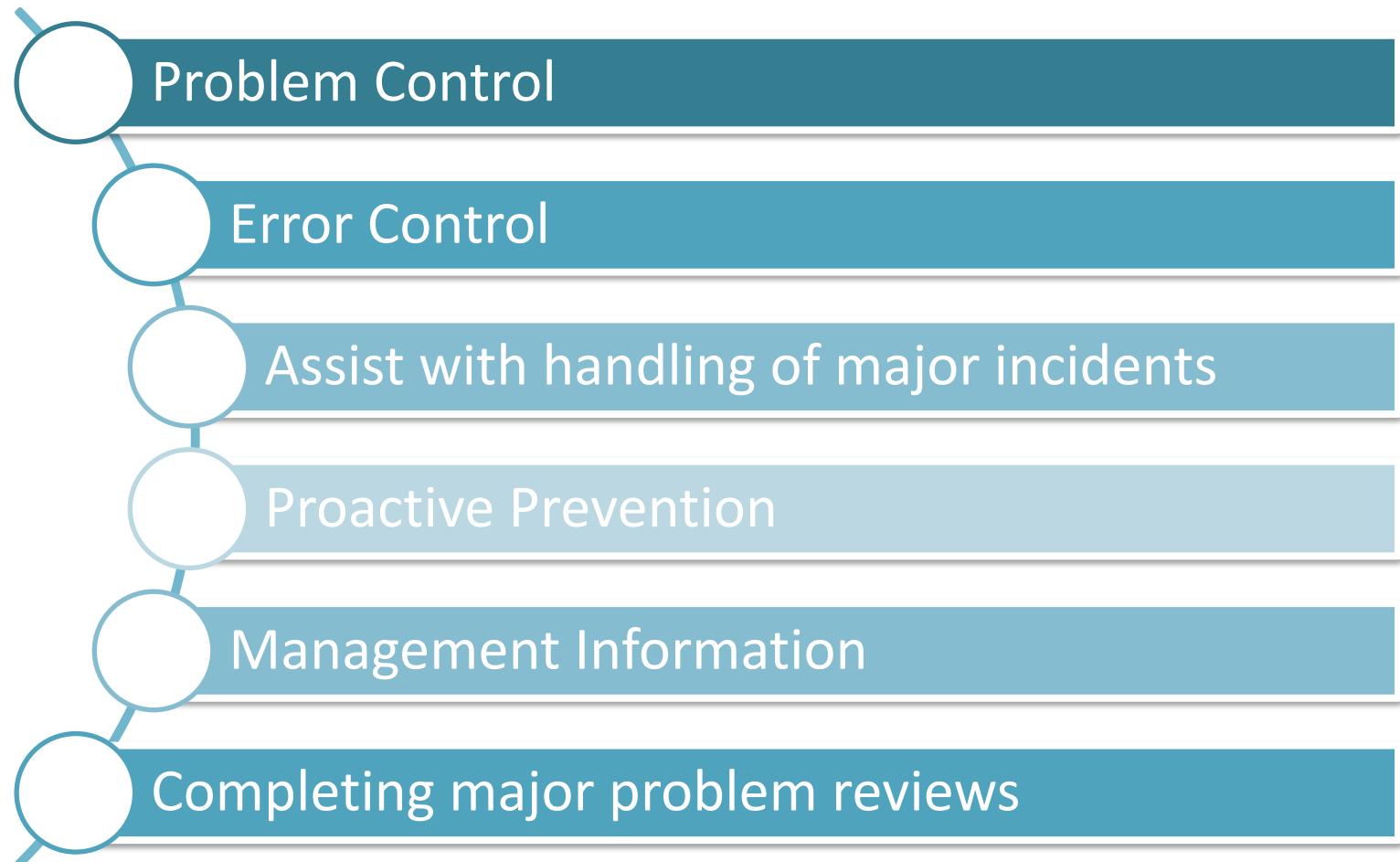
Questo processo ha un aspetto **reattivo** ed uno **proattivo**:

- L'aspetto **reattivo** riguarda la risoluzione di problemi in risposta ad uno o più incidenti segnalati
- Quello **proattivo** è, invece, relativo all'identificazione e risoluzione di problemi e known errors prima che gli incidenti si verifichino

# PROBLEM MANAGEMENT - RESPONSABILITÀ



Possono essere riassunte nei seguenti punti  
(sottoprocessi):





## Problem Control

- Questa parte del processo avviene quando i problemi sono identificati e registrati
- Successivamente ogni problema viene classificato e viene assegnato al giusto team di supporto, che effettuerà l'analisi della causa di origine per trovare una soluzione permanente
- E' la parte del processo che si preoccupa della gestione del work flow dell'errore
- E' qui che si trovano le soluzioni ai problemi



## Error Control

- Questa parte del processo riguarda il controllo dei known error e la generazione di RFC indirizzate al Change Management, per eliminare i known error dall'infrastruttura
- Questo sottoprocesso mantiene i database delle informazioni e dei known error
- Rende inoltre noti i known errors in modo che il processo di Incident Management possa risolvere gli incidenti più in fretta e studiare se i problemi e/o i known error sono presenti anche in altre parti dell'infrastruttura gestita



Assist with handling of major incidents  
(fornire assistenza nel gestire gli incidenti più gravi)

- Gli incidenti gravi sono quelli che hanno un forte impatto sulla comunità di utenti
- Il SD informa il Problem Manager il quale, in queste circostanze, dovrebbe organizzare un incontro formale con i responsabili dello staff di supporto



## Proactive Prevention

- Prevenire l'insorgere di nuovi incidenti, problemi, etc.
- i.e. Manutenzione preventiva, comunicazione verso gli altri dipartimenti come il SW development
- Attività di Trend Analysis
- Questo sottoprocesso si occupa di monitorare attivamente gli incidenti e, tramite metodi statistici, tenta di identificare trends in modo che i problemi possano essere individuati
- Solitamente i trends da per se non sono sufficienti per identificare un problema: una certa esperienza è necessaria per determinare se effettivamente il trend porterà ad un problema



## Management Information (gestione delle informazioni)

- Questo sottoprocesso ha lo scopo di:
  - Creare reports riguardo all'efficacia e le performance dell'intero processo di Problem Management
  - Fornire tali informazioni ai manager degli altri processi



## Completing Major Problem Review (condurre le review dei principali problemi)

- Il Problem Management genera RFC
- Solo dopo l'avvenuta implementazione di una change può essere stabilito se le modifiche hanno portato a ciò che effettivamente il Problem Management voleva, cioè la riduzione o l'eliminazione degli incidenti
- La Post Implementation Review (PIR) controlla se effettivamente tali risultati sono stati ottenuti



## *Chronological analysis*

- Es. i log applicativi o di apparati

## *Pain value analysis*

- Invece di analizzare solo il numero di incidenti e problemi di un particolare tipo ed in un particolare periodo, possono essere condotte analisi più approfondite prendendo in considerazione:
  - Il numero delle persone affette
  - La durata del downtime causato
  - Il costo al business (se facilmente calcolabile o stimabile)



## Kepner and Tregoe

- Tecnica di analisi approfondita delle ***root cause***

## Brainstorming

- Le sessioni di Brainstorming, coinvolgendo un gran numero di persone, possono essere molto efficaci a patto che si documentino bene le azioni concordate

## 5-Whys

- Ricerca delle ***root cause*** iterativa chiedendosi sempre “perché questo accade?”



## Fault isolation

- Rieseguire le transazioni o gli eventi che hanno portato al *fault* usando la modalità step-by-step, fino a che non viene identificato il CI responsabile del *fault*.

## Affinity mapping

- Si raggruppano grandi moli di dati al fine di ricercare una caratteristica comune.

## Hypothesis testing

- Si elencano una serie di ipotesi alla base delle *root cause* e si verificano una ad una.



## Technical observation post

- Allertare un ampio numero di specialisti affinché si preparino per “catturare” gli eventi che conducono al problema.

## Ishikawa diagrams

- Metodo per la correlazione causa-effetto utilizzato nei sistemi di gestione della qualità.

## Pareto analysis

- Tecnica per separare le più importanti cause potenziali da altri problemi secondari.

# TECNICHE DI ANALISI DEI PROBLEMI



Problem situation	Suggested analysis techniques
Complex problems where a sequence of events needs to be assembled to determine exactly what happened	Chronological analysis Technical observation post
Uncertainty over which problems should be addressed first	Pain value analysis Brainstorming
Uncertain whether a presented root cause is truly the root cause	5-Whys Hypothesis testing
Intermittent problems that appear to come and go and cannot be recreated or repeated in a test environment	Technical observation post Kepner–Tregoe Hypothesis testing Brainstorming
Uncertainty over where to start for problems that appear to have multiple causes	Pareto analysis Kepner–Tregoe Ishikawa diagrams Brainstorming
Struggling to identify the exact point of failure for a problem	Fault isolation Ishikawa diagrams Kepner–Tregoe Affinity mapping Brainstorming
Uncertain where to start when trying to find root cause	5-Whys Kepner–Tregoe Brainstorming Affinity mapping



## Problema:

- La causa sconosciuta di uno o più incidenti
- Può anche essere descritto come una situazione identificata come il risultato di vari incidenti che mostrano gli stessi sintomi
- I problemi possono anche essere identificati attraverso il verificarsi di un singolo incidente significativo
- Solitamente, ma non necessariamente, i problemi vengono risolti nel momento in cui l'incidente viene chiuso



## Errore:

- Un incidente o un problema per il quale la causa di origine è nota
- Può essere la causa nota di più di un incidente
- Al termine dell'investigazione sulle “root cause” di un problema si giunge sempre all'individuazione di un errore: si potrebbe dire che un problema si chiude con la generazione di un errore



## Known Error:

- Un errore per il quale una fix (o workaround) temporanea o una soluzione permanente sia stata individuata
- Esso rimane un known error a meno che non sia permanentemente risolto tramite un change

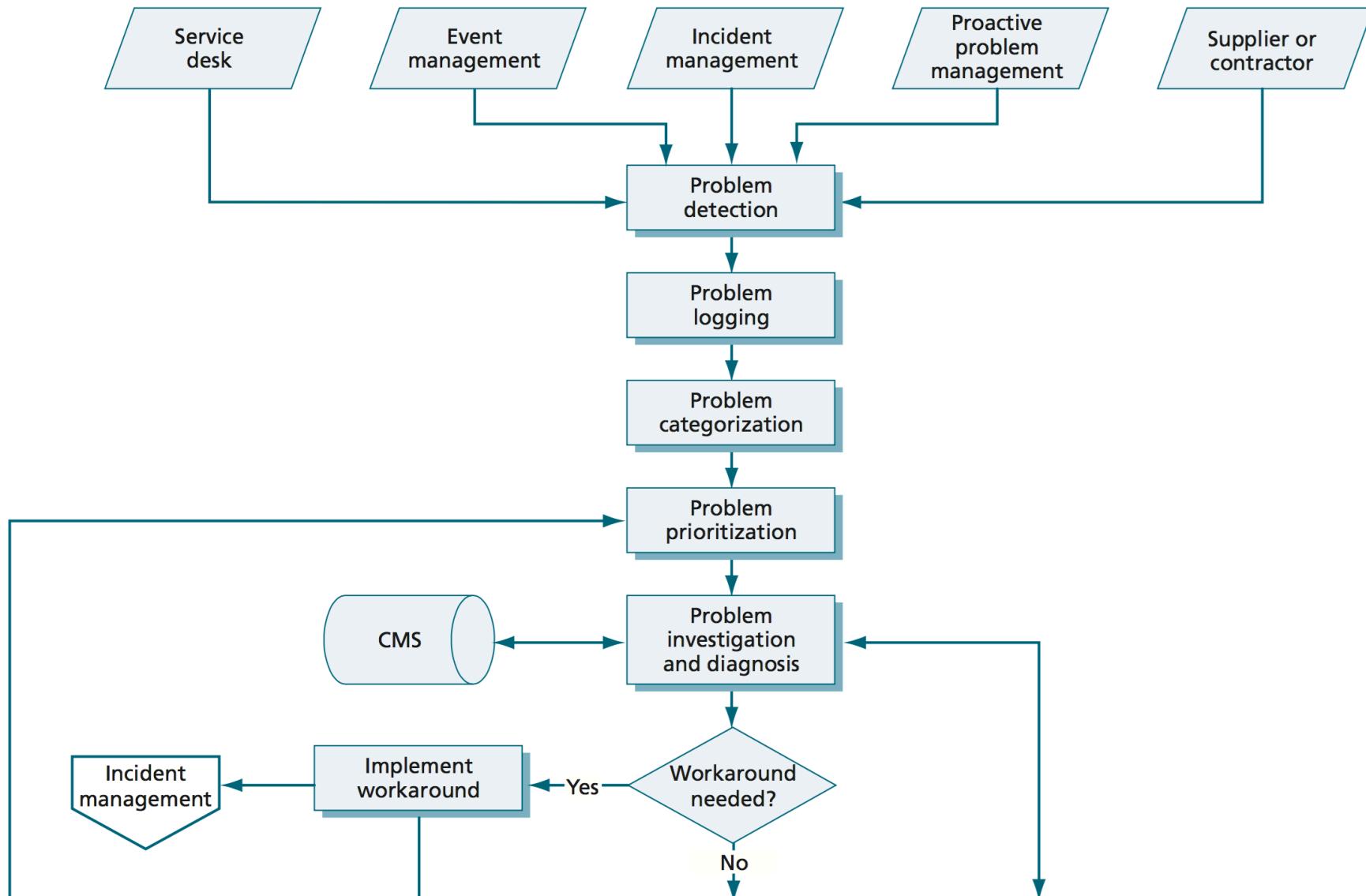
Nella pratica i termini errore e known error sono spesso usati come sinonimi

# ESEMPIO DI INFORMAZIONI NECESSARIE PER LA GESTIONE DEI PROBLEMI

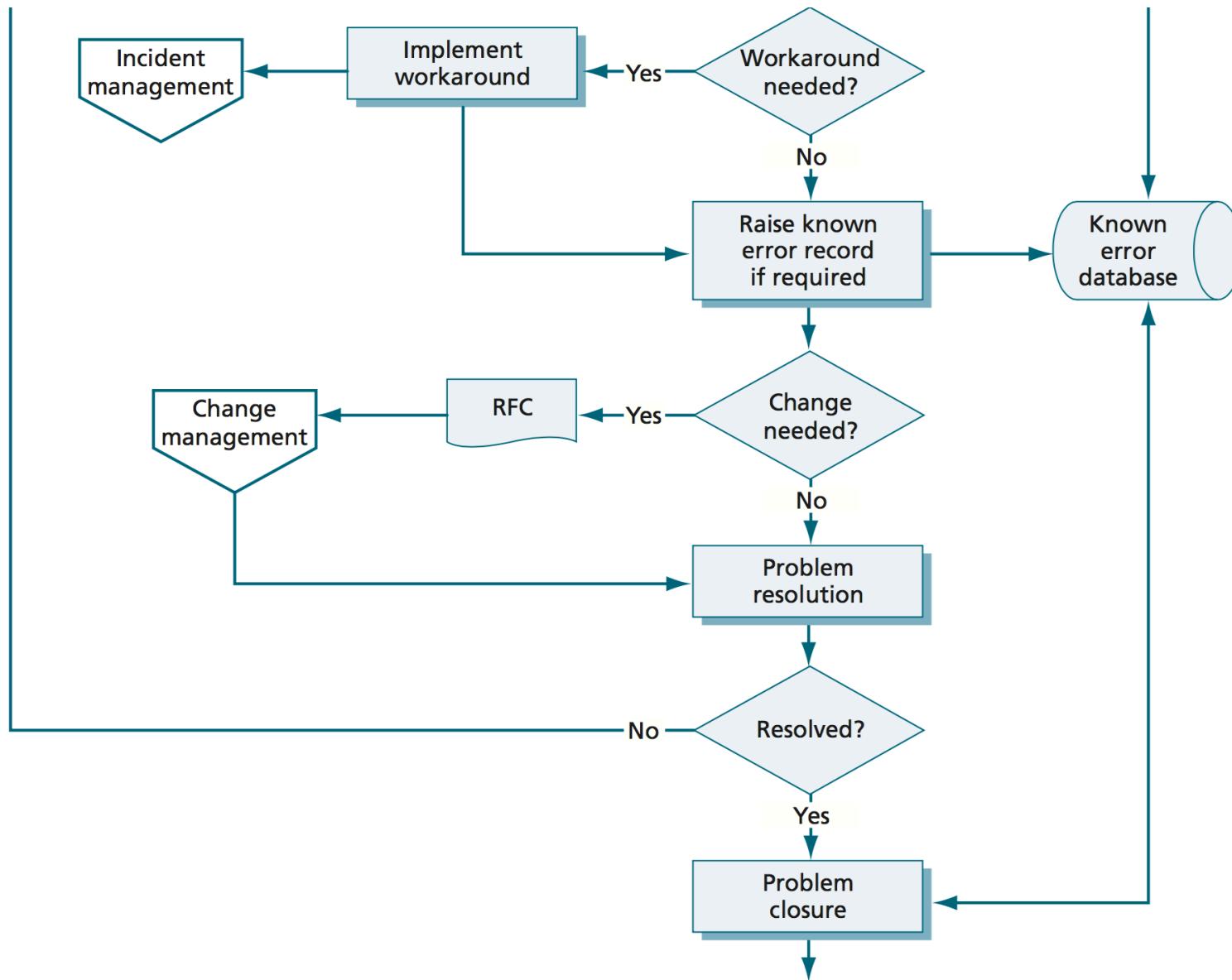


- User details
- Service details
- Equipment details
- Date/time initially logged
- Priority and categorization details
- Incident description
- Incident record numbers or other cross-reference
- Details of all diagnostic or attempted recovery actions taken.

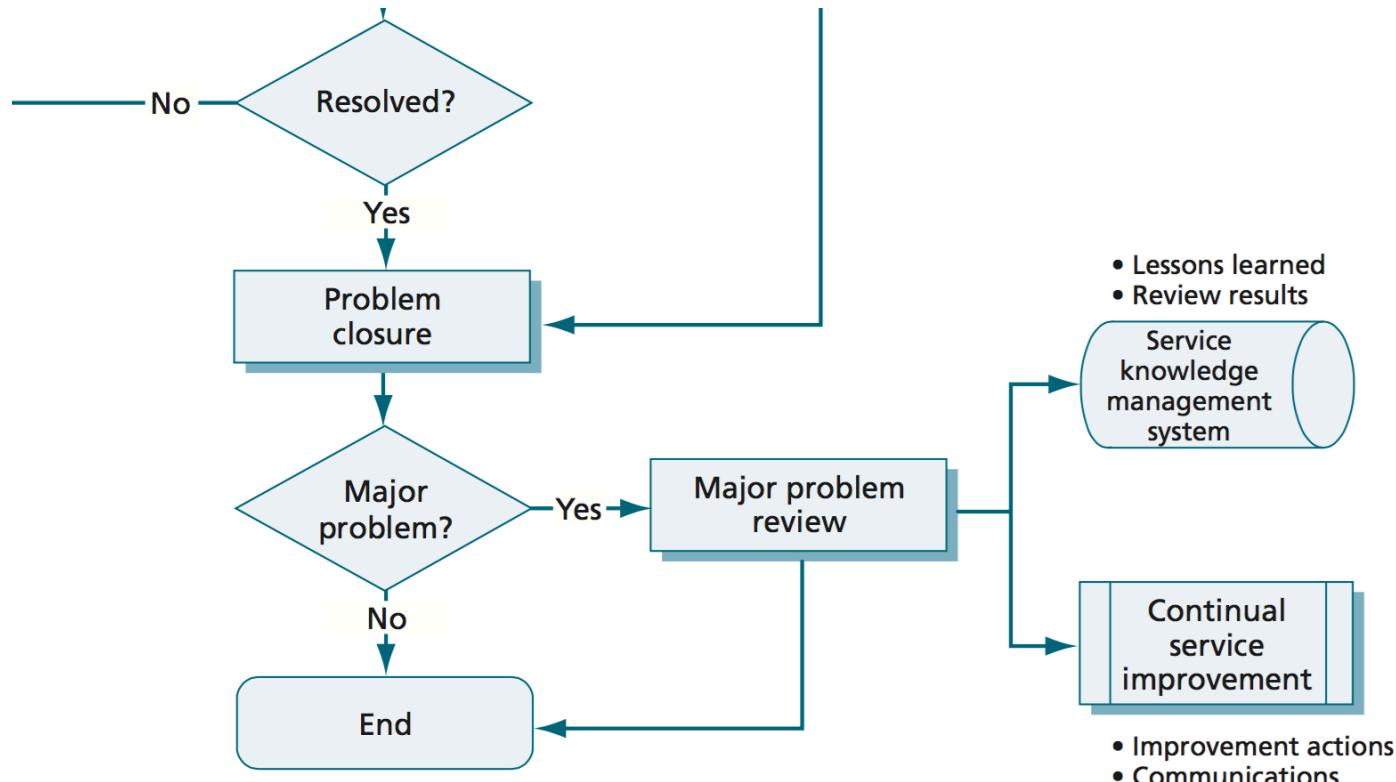
# PROBLEM MANAGEMENT: IL FLUSSO



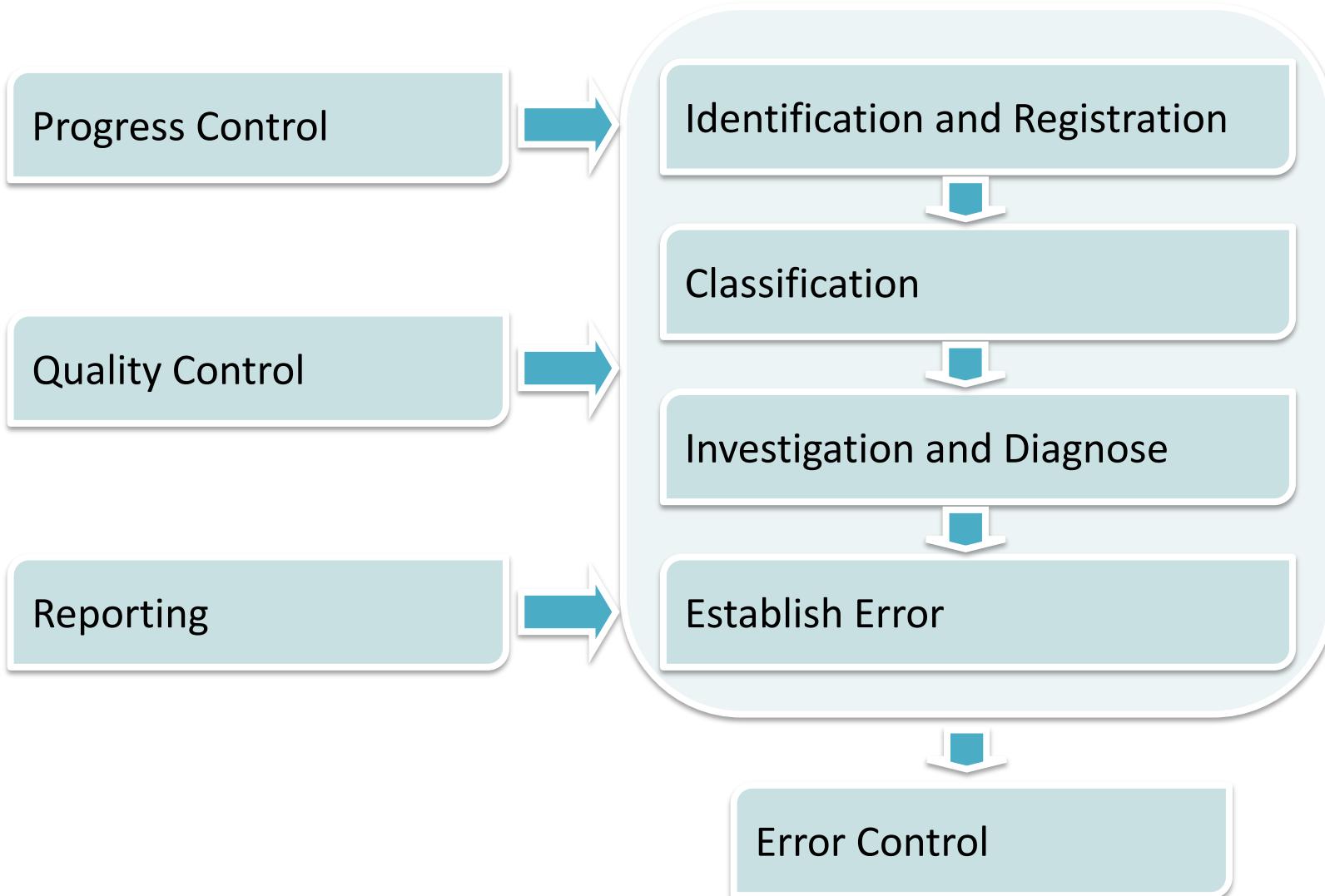
# PROBLEM MANAGEMENT: IL FLUSSO



# PROBLEM MANAGEMENT: IL FLUSSO



# SOTTOPROCESSO "PROBLEM CONTROL"





## Identification and Registration

I modi per identificare un problema sono:

- Se c’è stato un incidente con impatto considerevole che è stato risolto, il Problem Manager dovrebbe subito registrare un problema in modo che possa iniziare una investigazione per determinarne la causa
- Durante la Trend Analysis potrebbero essere individuati una serie di incidenti con sintomi simili
- Qualcuno scopre una fonte di potenziali problemi
- Se un incidente viene chiuso con codice “workaround”
- Se un problema viene segnalato da un altro settore



## Classification

- Questa fase include la raccolta di dati in modo che il problema possa essere categorizzato e gli possa essere assegnata una priorità
- Quali sono i CIs coinvolti? Quali sono gli incidenti ad esso collegati? Quali sono i sintomi? Quali sono le cause? Quali sono le soluzioni/workaround? Quali sono le modifiche relative a questo CI? A quali livelli di servizio si riferisce? Quale è il rischio? Quali clienti sono coinvolti? Quanto tempo necessita per trovare una risposta? Con che urgenza deve essere risolto il problema? Quale è il beneficio derivante dalla risoluzione del problema (impatto)?



## Allocazione delle risorse

- La classificazione (categorizzazione ed assegnazione della priorità) di un problema consente di allocare le giuste risorse
- Questo garantisce che i problemi siano gestiti efficientemente ed efficacemente
- Ciò evidenzia inoltre quelli che hanno il maggiore impatto sul business



## Investigation and Diagnose

- Lo scopo è quello di individuare la causa di origine di uno o più incidenti
- L'attività di investigazione include l'individuazione dei workarounds disponibili per gli incidenti relativi al problema e la loro registrazione nel DB degli incidenti
- Anche l'elenco dei change recenti deve essere consultato, poiché esso potrebbe fornire indizi che conducono alla causa
- Infine le informazioni riguardo la storia dei CIs potrebbero essere anch'esse utili



## Establish Error

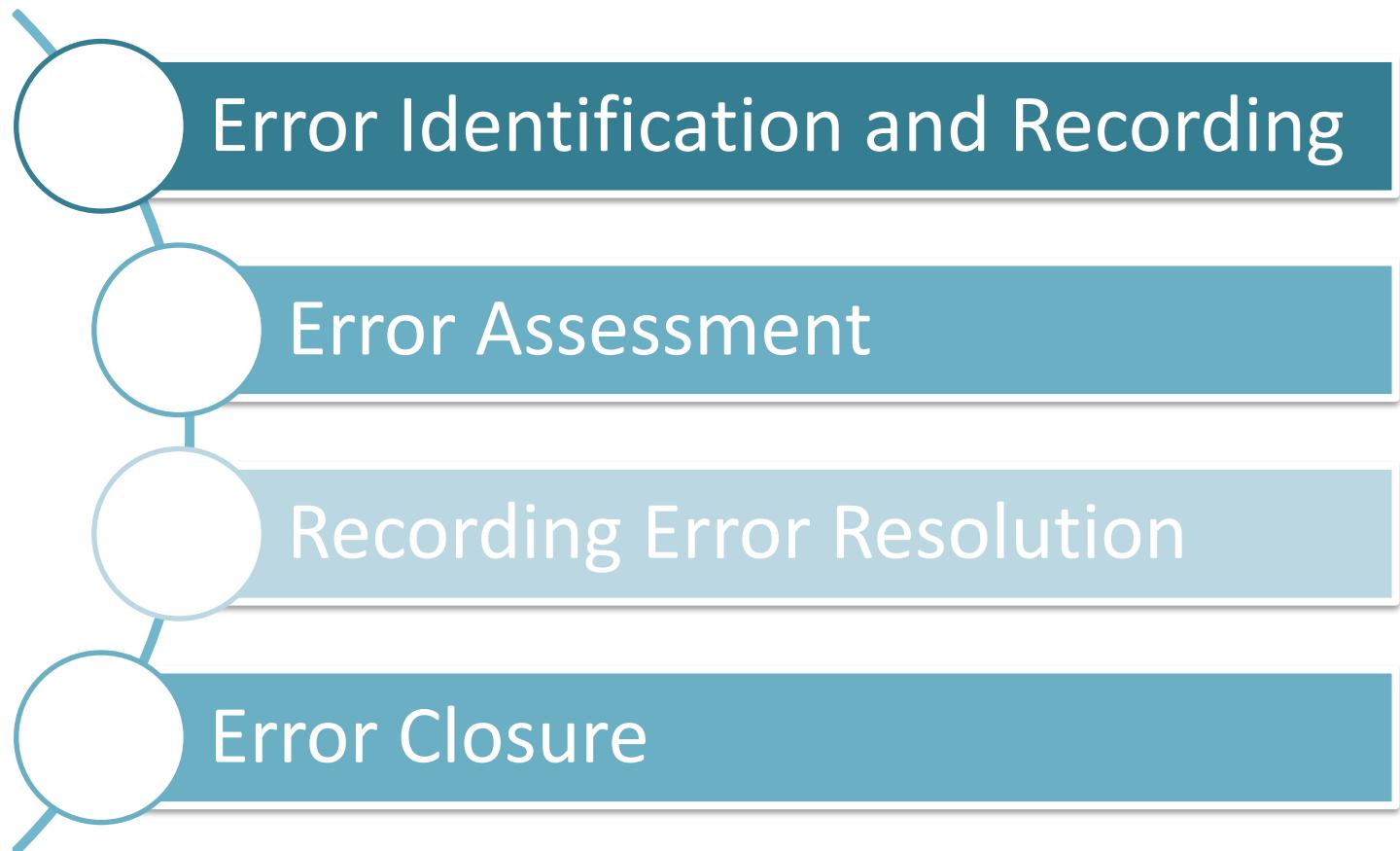
- Dopo la fase precedente, l'errore viene determinato
- In questa fase si traccia tale errore e lo si inoltra al sottoprocesso di “Error Control”
- Durante tutto il processo il Problem Manager ha la responsabilità di tracciare e monitorare lo stato di avanzamento e il livello di qualità per fornire i reports necessari



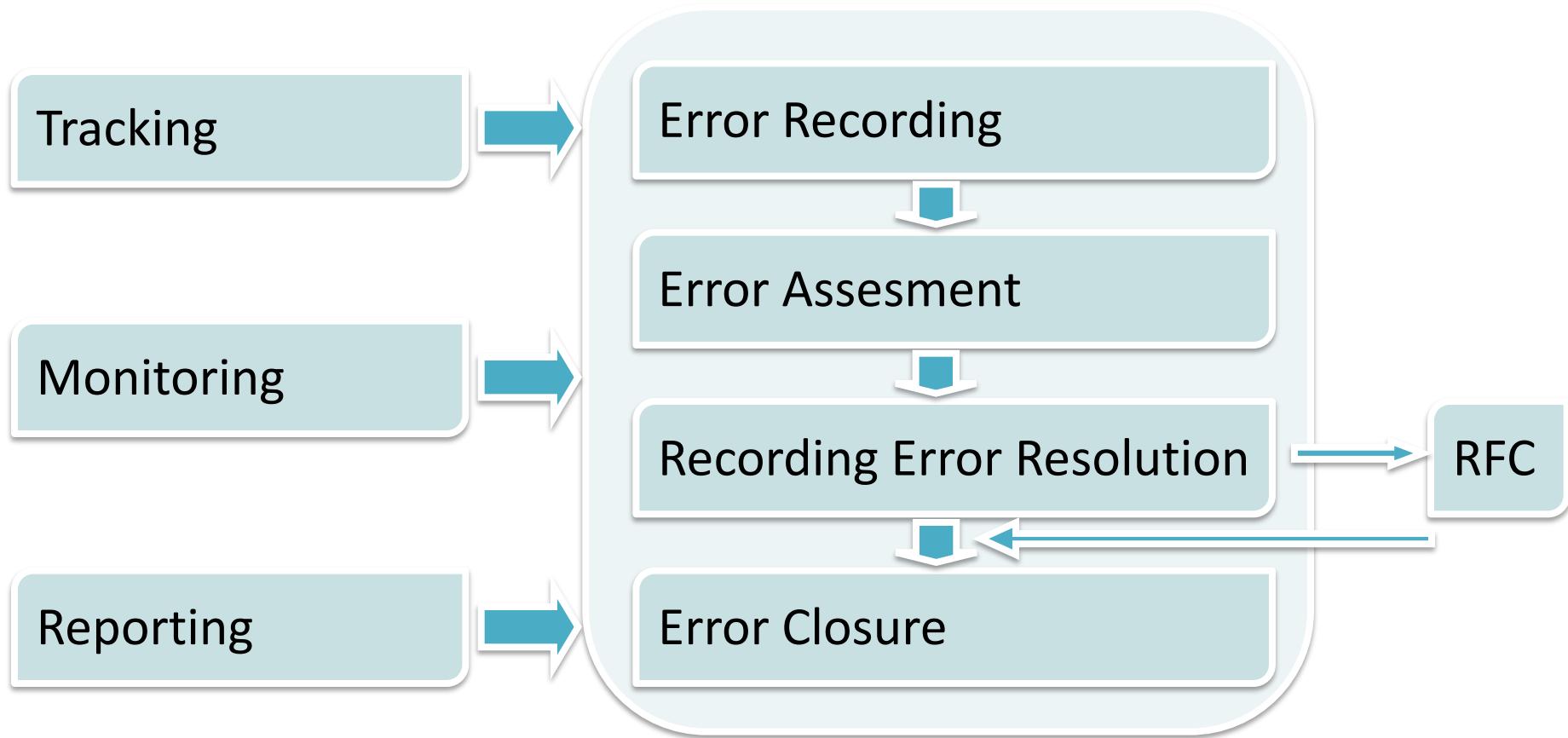
**Il sottoprocesso di “Error Control” è responsabile della registrazione, del monitoraggio e della gestione di tutti gli errori, dall’inizio (identificazione) fino all’implementazione con successo del *change* che rimuove le cause di origine**



Le fasi sono:



# SOTTOPROCESSO “ERROR CONTROL”





## Error Identification and Recording (identificazione e registrazione dell'errore)

- Un errore è identificato quando un CI difettoso è stato individuato
- Lo status di Known Error viene assegnato quando la causa di origine di un problema è stata trovata
- Ci sono due fonti di Known Errors:
  - Il Problem Control nell'ambiente live
  - Il Problem Control nell'ambiente di sviluppo



## Error Assessment (valutazione dell’errore)

- In questa fase si svolge una stima iniziale dei mezzi necessari per la risoluzione dell’errore, in collaborazione con uno staff di specialisti
- Il processo di risoluzione per ciascun known Error deve essere registrato nel sistema utilizzato dal PM (workflow)
- E’ fondamentale che le informazioni inerenti i Cls, i sintomi e la risoluzione di tutti i KE siano registrate nel KEDB
- In questo modo tali informazioni saranno poi disponibili per svolgere attività di Incident Matching, per fornire delle linee guida per le future investigazioni e per fornire informazioni al management



## **Recording Error Resolution (registrazione della risoluzione)**

- In questa fase si registra il processo di risoluzione per ciascun KE e si prepara una RFC secondo le procedure del Change Management
- La priorità di una RFC viene determinata in base all’urgenza e all’impatto dell’errore sul business
- RFC e KE devono avere una relazione (collegamento)
- Le fasi finali della risoluzione (analisi di impatto, valutazione delle azioni da intraprendere per la risoluzione, modifica dell’item difettoso e test del change) ricadono sotto il controllo del CM



## Error Closure (chiusura dell’errore)

- Successivamente all’implementazione con successo dei changes (determinata da una Post Implementation Review) che risolvono gli errori, il corrispondente record di KE viene chiuso insieme ad ogni record di incidente o problema ad esso relativo



Il sottoprocesso di “Proactive Control Management” svolge quelle attività finalizzate all’identificazione ed alla risoluzione dei Problemi prima che questi possano provocare incidenti.

Queste attività sono:

Trend Analysis

Targeting Support Action

Informing the organization



## Trend Analysis

- La reportistica sugli incidenti e sui problemi può fornire delle informazioni per misure preventive per il miglioramento della qualità del servizio
- Le analisi sugli incidenti e sui problemi possono identificare trends come:
  - Il verificarsi di un certo tipo di problemi a seguito di un change
  - L'inizio di un certo tipo di anomalie o malfunzionamenti
  - Il ripetersi di particolari incidenti e problemi con alcuni CIs in particolare
  - La necessità di fare del training allo staff o al cliente



## Targeting Support Action

- Le Trend Analysis possono condurre all'individuazione di parti difettose nell'infrastruttura IT, che possono quindi essere analizzate e corrette
- Può anche condurre all'identificazione di aree di problemi che necessitino di maggiore attenzione da parte del supporto



## Informing the organization

- Il Problem Management può fornire informazioni circa problemi, KE ed RFC emesse
- Questo aiuta a determinare lo stato di salute del business e i dettagli possono essere utilizzati per informare i processi di “decision making” all’interno dell’organizzazione e altri processi come il SLM e funzioni come il SD



**Reindirizzando gli sforzi di un'organizzazione da reattivi verso un gran numero di incidenti a preventivo, un'organizzazione fornisce un miglior servizio ai suoi clienti e rende più efficace ed efficiente l'utilizzo delle risorse disponibili all'interno dell'organizzazione di supporto IT**



Tutti processi prevedono l'interazione con altri processi, ma alcuni sono così legati da richiedere di essere, normalmente, implementati assieme.

Capire la logica di interazione fra questi è fondamentale per capire come funziona ITIL.

Di seguito alcune considerazioni ed esempi.

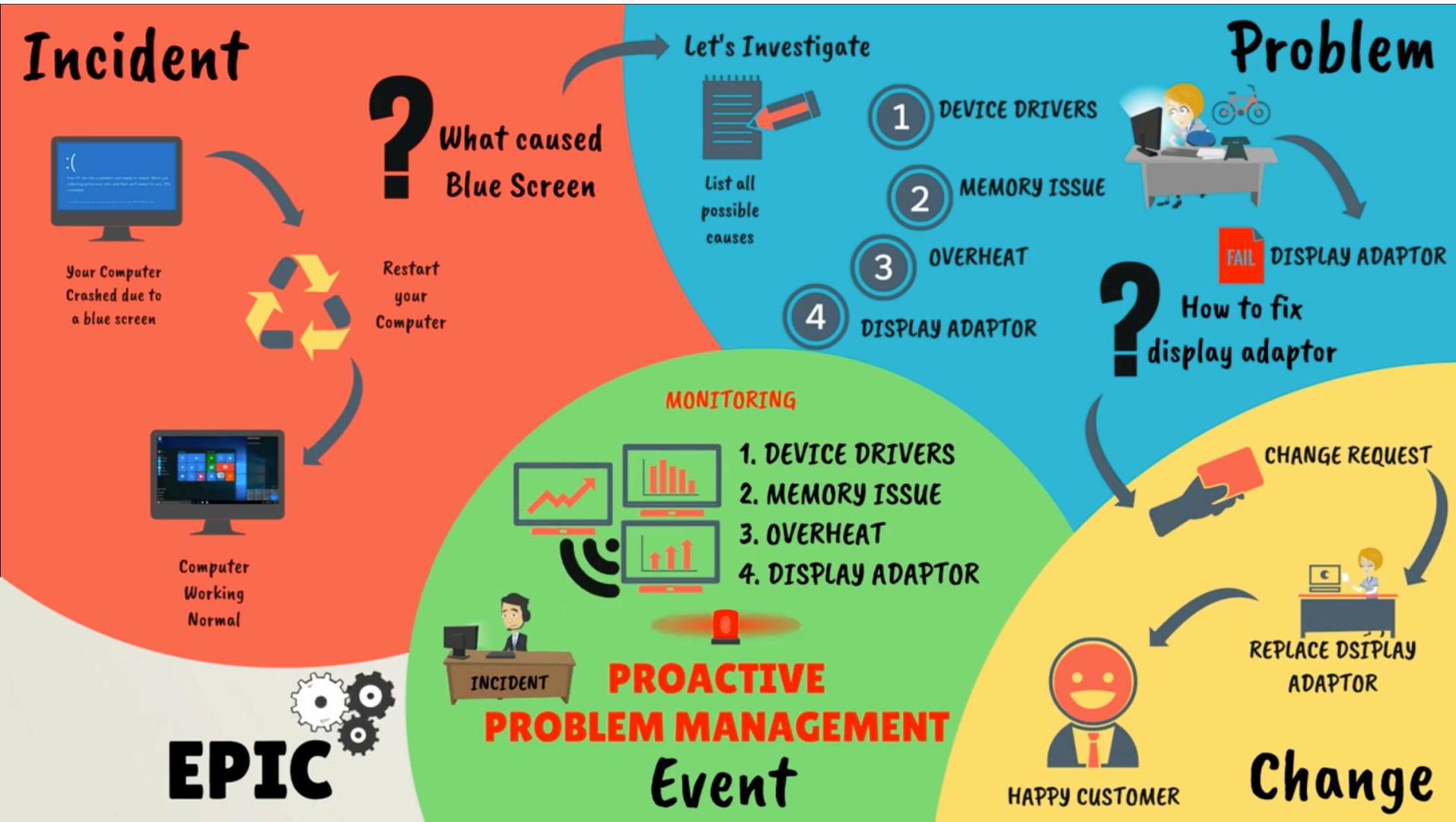


- *Incidenti, problemi* e *change* sono entità distinte
- Un incidente non diventa mai un problema
- ITIL mostra un modello nel quale gli *incidenti*, i *problem*i ed anche i *change* possono esistere simultaneamente

# EPIC OPERATIONAL RELATIONS



Look at «EPIC | Event Problem Incident Change (Operational Relation) - Learn and Gain» on YouTube for more information



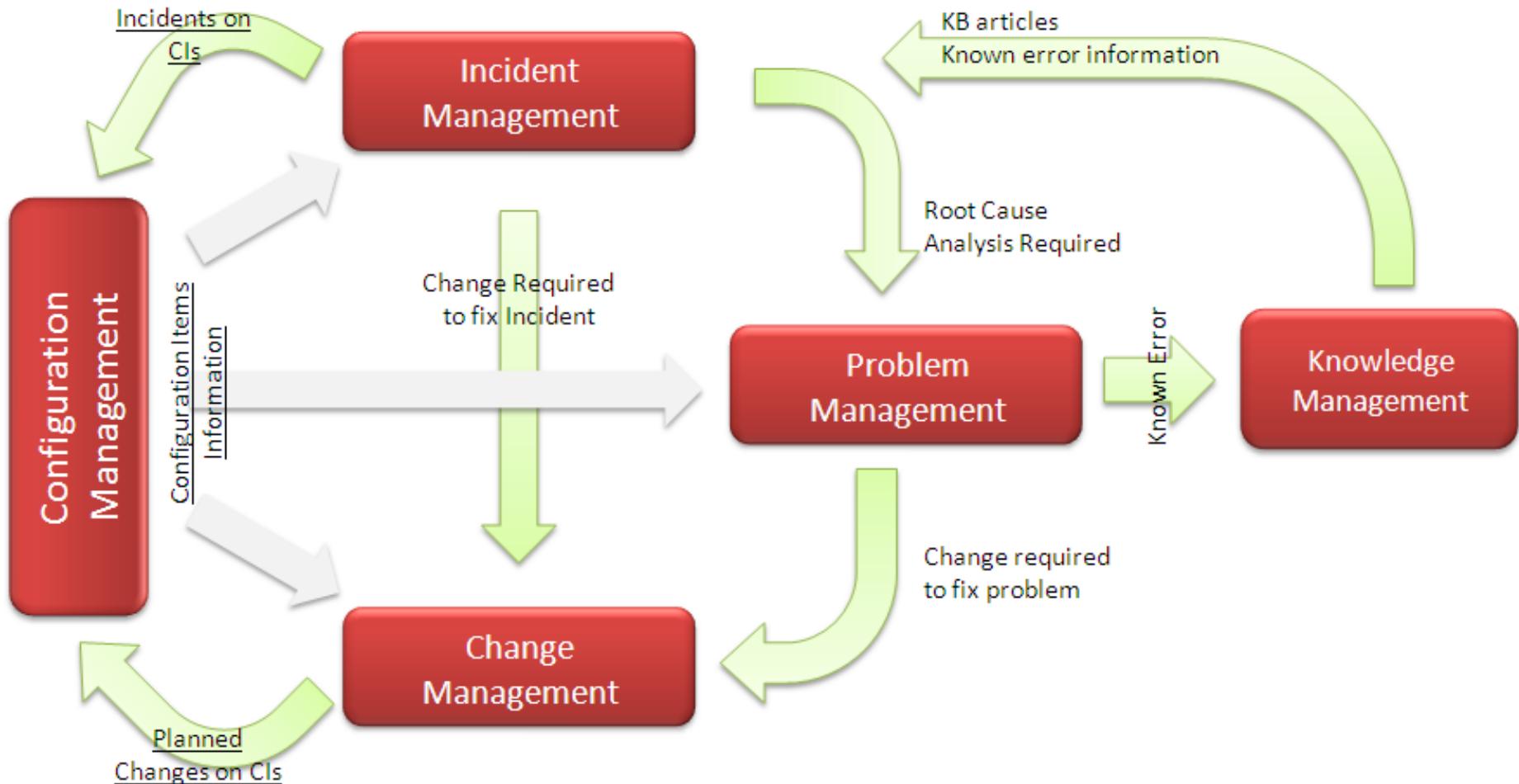
**EPIC**

**NETCOM**

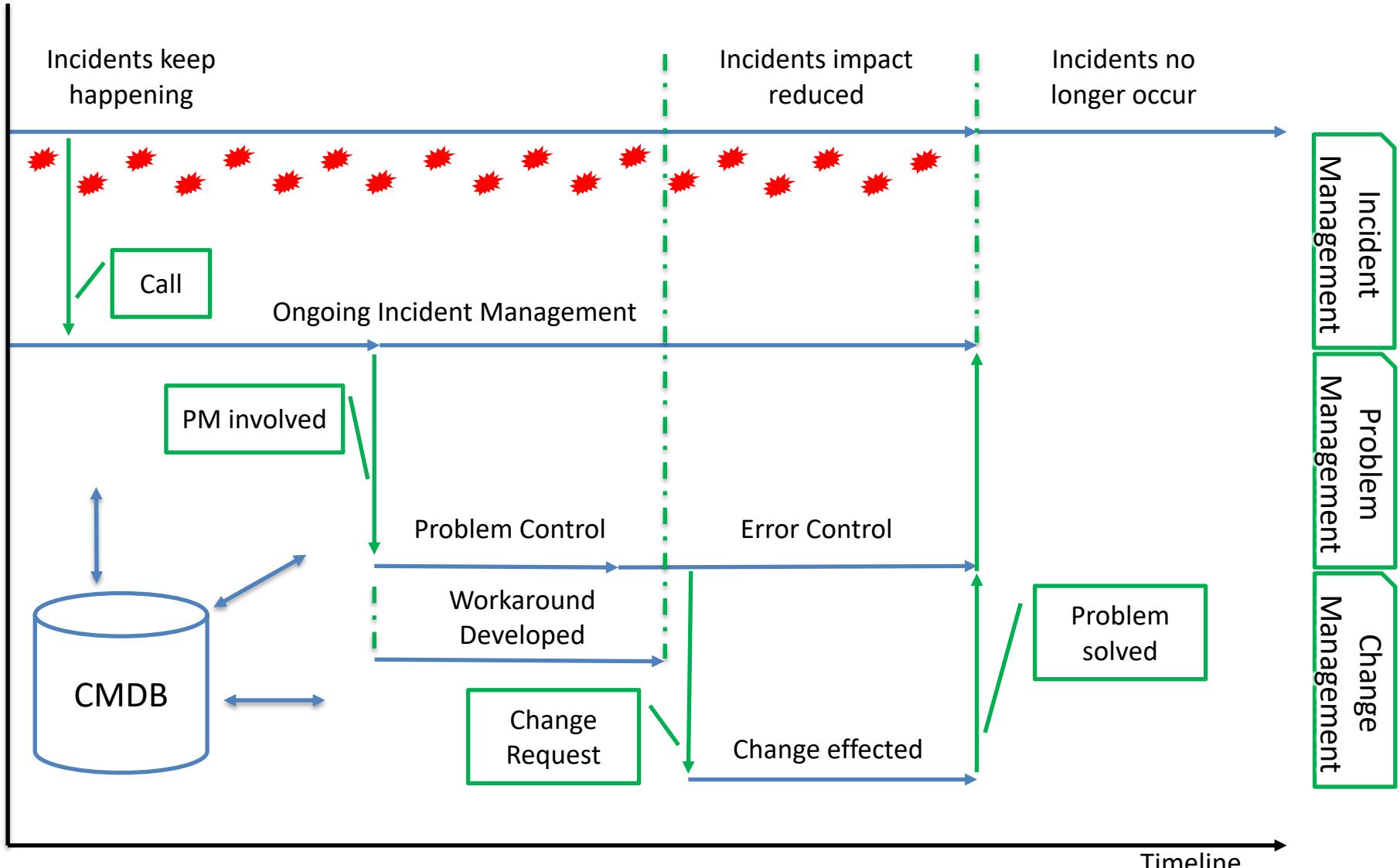
IT Life Cycle Management

162

# INTERAZIONE FRA PROCESSI



# INCIDENT, PROBLEM, CHANGE





## Inizio di un incidente:

- Quando avviene un incidente, il processo di IM tenta di risolverlo il più rapidamente possibile
- L'incidente può essere chiuso solo quando viene data conferma dal cliente
- Se durante la fase di investigazione dell'incidente non viene trovata alcuna soluzione, allora il processo di IM chiede supporto al PM, in modo che la causa di origine dell'incidente possa essere determinata



## Investigazione ed Escalation

- L'incidente ed il Problema esistono simultaneamente
- Il PM definisce un problema con urgenza alta ed assegna immediatamente le risorse
- Tali risorse fanno una diagnosi del problema e trovano la causa di origine dell'incidente



## Diagnosi

- L'incidente, il Problema e il Known Error esistono simultaneamente
- Un Known Error viene definito e, dopo aver stabilito come risolverlo, viene mandata una RFC al CM per risolvere la situazione



## Change avviato

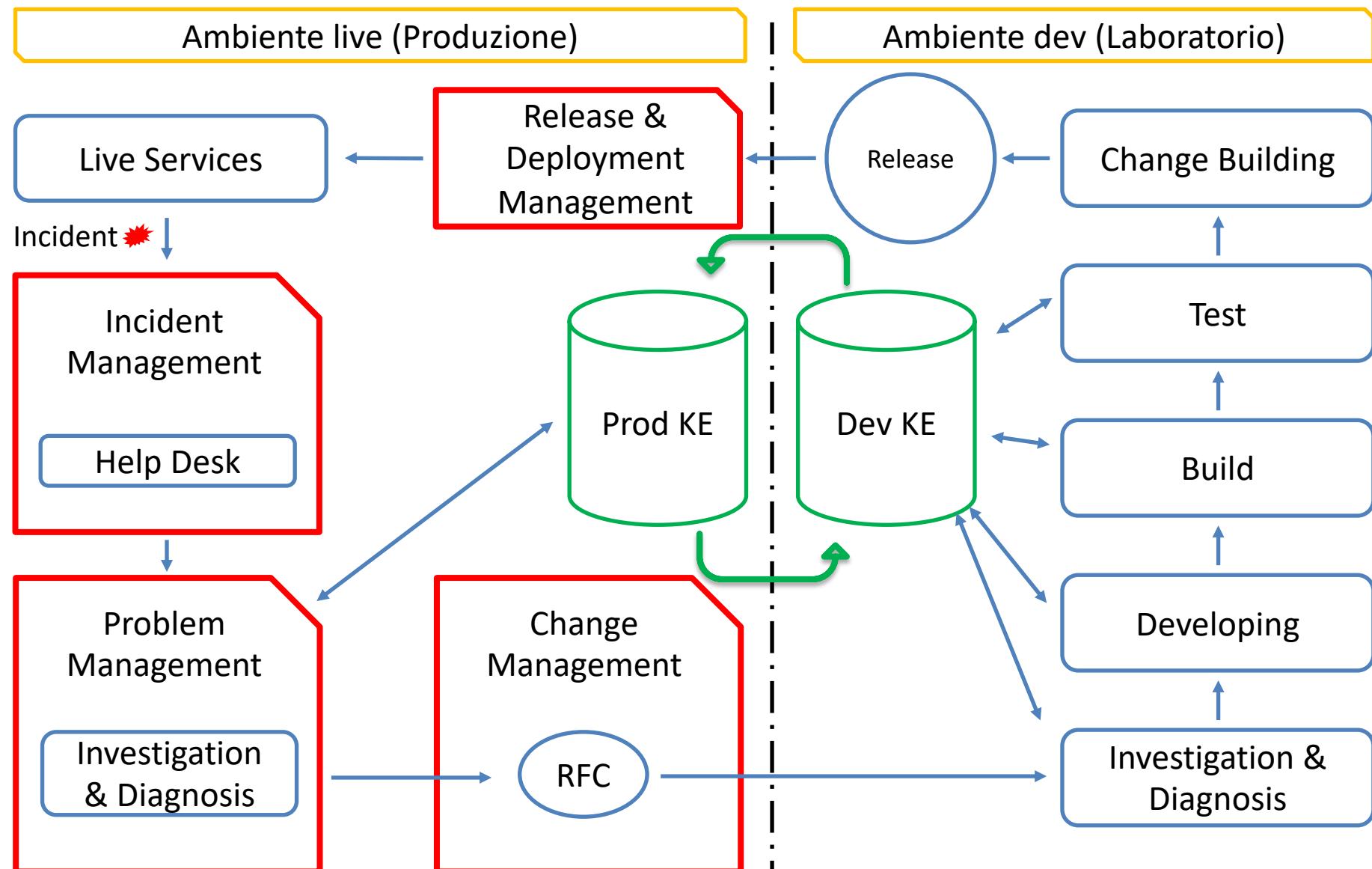
- L'incidente, il Problema e il Known Error ed il Change esistono simultaneamente
- Il Change viene implementato con successo
- La PIR mostra che il change ha di fatto eliminato il KE con successo
- L'investigazione mostra anche che l'incidente è stato risolto e lo stesso per il problema aperto
- Per questa ragione il suo stato può diventare “closed”



## Fine

- L'incidente è risolto
- Il Problema e il Known Error sono chiusi
- Se da qualche parte durante la fase di diagnosi il team dedicato ai problemi trova un workaround, l'incidente può essere chiuso (sempre con l'OK dell'utente)
- Questo non significa che il problema non esiste più
- L'unico aggiornamento al record del problema sarà che l'urgenza scenderà da urgente a non urgente
- Sta al processo di PM decidere se ci sono abbastanza risorse disponibili al momento per fare la diagnosi del problema o se tali risorse possono essere usate meglio per altre attività

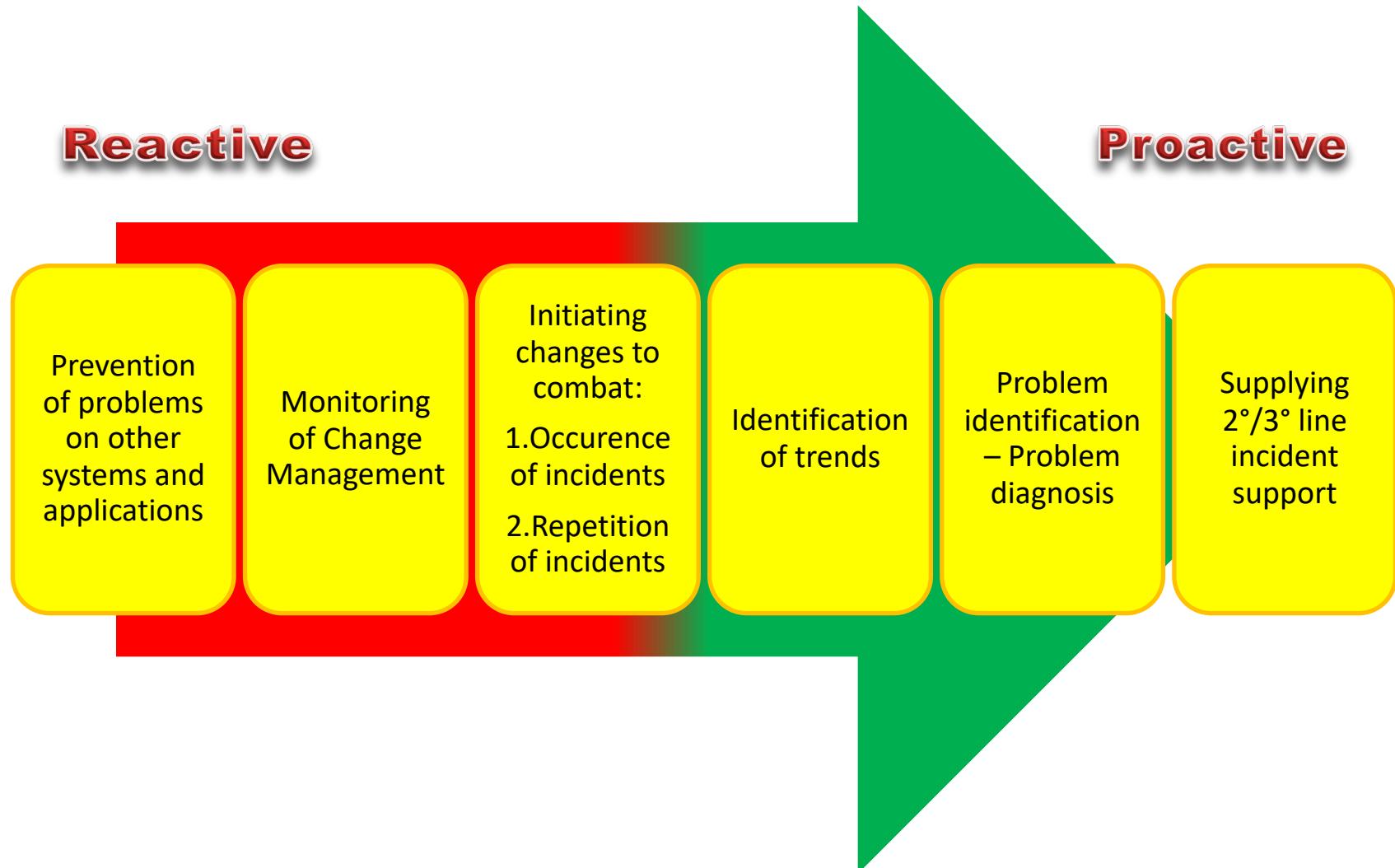
# GESTIONE DEI KE IN AMBIENTE DI SVILUPPO





- La seconda fonte di KE proviene dalle attività del team di sviluppo
- I.e. l'implementazione di una nuova applicazione o di un release package possono facilmente introdurre errori noti ma ancora irrisolti, generati durante la fase di sviluppo
- Quando una applicazione o un release package vengono implementati, le informazioni relative ai KE generati dal team di sviluppo devono essere resi noti al PM, il quale a sua volta deve notificarlo al SD

# REATTIVO – PROATTIVO (PREVENTIVO)



# REATTIVO – PROATTIVO (PREVENTIVO)



- Le attività descritte finora in problem ed error control sono principalmente di tipo **reattivo**
- Le attività di “Proactive Problem Management” riguardano l’identificazione e la risoluzione di problemi e KE prima che gli incidenti accadano. In altre parole, **minimizzare l’impatto sul servizio e sui costi sostenuti dal business**
- La prevenzione dei problemi spazia dalla prevenzione dei singoli problemi fino alle decisioni strategiche
- Quest’ultime possono richiedere grosse spese per essere realizzate, i.e. investire in una infrastruttura di rete migliore

# REATTIVO – PROATTIVO (PREVENTIVO)



- Le **principal attivit**à dei processi di PM proattivo sono le **Trend Analysis** e le **azioni di prevenzione mirate**
- Le **Trend Analysis** possono condurre all'identificazione di parti difettose nell'infrastruttura IT che possono poi essere analizzate e corrette come descritto nelle sezioni riguardanti il problem e l'error control
- Le **Trend Analysis** possono anche portare all'identificazione di aree di problema generali che necessitano di più attenzione
- Deve essere anche possibile fare **valutazioni in termini di costi** per l'organizzazione
- I report degli incidenti e delle Problem Analysis forniscono informazioni per **misure preventive** mirate al **miglioramento della qualit**à del servizio

# REATTIVO – PROATTIVO (PREVENTIVO)



- L'**obiettivo** è quello di **identificare componenti “fragili”** dell'infrastruttura IT ed investigare sulle ragioni alla base di tali fragilità. In questo contesto la “fragilità” è proporzionata all’impatto che potrebbe avere sul business la “rottura” di un CI
- La **categorizzazione** degli incidenti e dei problemi e delle analisi “creative” possono rivelare trends e portare all’identificazione di **specifiche (potenziali) aree** di problemi che necessitano di ulteriori investigazioni
- I.e. le analisi potrebbero indicare che gli incidenti relativi all’utilizzo di sistemi client-server recentemente installati sono l’area di problemi che ha avuto la maggior crescita in termini di **impatto negativo sul business**

# REATTIVO – PROATTIVO (PREVENTIVO)



- Le analisi dei dati del PM possono rivelare che i problemi che si sono verificati su una piattaforma possono verificarsi anche su un'altra piattaforma
  - I.e. un problema relativo ad una applicazione di rete su un sistema midrange potrebbe avere conseguenze su un sistema mainframe
- L'esistenza di problemi ricorrenti
  - 3 router vengono sostituiti consecutivamente a causa dello stesso difetto: potrebbe indicare che il tipo di router non è appropriato e dovrebbe essere sostituito con uno di altro tipo



**Per poter iniziare una attività di Trend Analysis seria ci vuole almeno un anno di accumulo dati**



I benefici derivanti da un approccio formale al Problem Management includono:

- **Miglioramento della qualità del servizio IT.** Il PM aiuta a creare un ciclo di incremento rapido della qualità del servizio IT, ed è un bene per la produttività e lo stato d'animo di chi fornisce il servizio IT
- **Riduzione del volume di incidenti.** Il PM contribuisce alla riduzione del numero di incidenti che interrompono la conduzione del business
- **Soluzioni permanenti.** C'è una graduale riduzione del numero e dell'impatto dei Problemi e dei KE una volta che quelli risolti rimangono risolti



- **Miglioramento del livello di apprendimento a livello organizzativo.** Il processo di PM si basa sul concetto di apprendere dalle esperienze passate. Il processo fornisce dati storici per consentire l'identificazione di trends, un mezzo di prevenzione dei malfunzionamenti failures e di riduzione dell'impatto di questi, con conseguente miglioramento della produttività degli utenti
- **Maggior numero di fix funzionanti sin dalla prima volta a disposizione del SD.** Il PM fornisce al SD un maggior numero di fix di incidenti che funzionano al primo tentativo grazie al processo basato sulle informazioni del CMDB



**CSF** Minimize the impact to the business of incidents that cannot be prevented

**KPI** The number of known errors added to the KEDB

**KPI** The percentage accuracy of the KEDB (from audits of the database)

**KPI** Percentage of incidents closed by the service desk without reference to other levels of support (often referred to as 'first point of contact')

**KPI** Average incident resolution time for those incidents linked to problem records



**CSF** Maintain quality of IT services through elimination of recurring incidents

**KPI** Total numbers of problems (as a control measure)

**KPI** Size of current problem backlog for each IT service

**KPI** Number of repeat incidents for each IT service



**CSF** Provide overall quality and professionalism of problem handling activities to maintain business confidence in IT capabilities

**KPI** The number of major problems (opened and closed and backlog)

**KPI** The percentage of major problem reviews successfully performed

**KPI** The percentage of major problem reviews completed successfully and on time

**KPI** Number and percentage of problems incorrectly assigned

**KPI** Number and percentage of problems incorrectly categorized



**KPI** The backlog of outstanding problems and the trend (static, reducing or increasing?)

**KPI** Number and percentage of problems that exceeded their target resolution times

**KPI** Percentage of problems resolved within SLA targets (and the percentage that are not!)

**KPI** Average cost per problem.

## IT SERVICE OPERATION

---

### ATTIVITÀ DI SERVICE OPERATION

# CAPITOLI DELLA SEZIONE NEL CORE Book



- Monitoring and control
- IT operations
- Server and mainframe management and support
- Network management
- Storage and archive
- Database administration
- Directory services management
- Desktop and mobile device support
- Middleware management
- Internet/web management
- Facilities and data centre management
- Operational activities of processes covered in other lifecycle stages
- Improvement of operational activities

# STEP DI MATURAZIONE DI UNA AZIENDA



			<b>Level 5</b>	<ul style="list-style-type: none"> <li>– IT is measured in terms of its contribution to the business</li> <li>– All services are measured by their ability to add value</li> <li>– Technology is subordinate to the business function it enables</li> <li>– Service portfolio drives investment and performance targets</li> <li>– Technology expertise is entrenched in everyday operations</li> <li>– IT is viewed as a utility by the business</li> </ul>	
			<b>Level 4</b>	<ul style="list-style-type: none"> <li>– Services are quantified and initiatives aimed at delivering agreed service levels</li> <li>– Service requirements and technology constraints drive procurement</li> <li>– Service design specifies performance requirements and operational norms</li> <li>– Consolidated systems support multiple services</li> <li>– All technology is mapped to services and managed to service requirements</li> <li>– Change management covers both development and operations</li> </ul>	
			<b>Level 3</b>	<ul style="list-style-type: none"> <li>– Critical services have been identified together with their technology dependencies</li> <li>– Systems are integrated to provide required performance, availability and recovery for those services</li> <li>– More focus on measuring performance across multiple devices and platforms</li> <li>– Virtual mapping of configuration and asset data with single change management for operations</li> <li>– Consolidated availability and capacity planning on some services</li> <li>– Integrated disaster recovery planning</li> <li>– Systems are consolidated to save cost</li> </ul>	
			<b>Level 2</b>	<ul style="list-style-type: none"> <li>– Initiatives are aimed at achieving control and increasing the stability of the infrastructure</li> <li>– IT has identified most technology components and understands what each is used for</li> <li>– Technical management focuses on achieving high performance of each component regardless of its function</li> <li>– Availability of components is measured and reported</li> <li>– Reactive problem management and inventory control are performed</li> <li>– Change control is performed on ‘mission-critical’ components</li> <li>– Point solutions are used to automate those processes that are in place, usually on a platform-by-platform basis</li> </ul>	
			<b>Level 1</b>	<ul style="list-style-type: none"> <li>– IT is driven by technology and most initiatives are aimed at trying to understand infrastructure and deal with exceptions</li> <li>– Technology management is performed by technical experts, and only they understand how to manage each device or platform</li> <li>– Most teams are driven by incidents, and most improvements are aimed at making management easier – not to improve services</li> <li>– Organizations entrench technology specializations and do not encourage interaction with other groups</li> <li>– Management tools are aimed at managing single technologies, resulting in duplication</li> <li>– Incident management processes start being created</li> </ul>	



## *Active versus passive monitoring*

	Active	Passive
Reactive	<p>Used to diagnose which device is causing the failure and under what conditions (e.g. 'ping' a device, or run and track a sample transaction through a series of devices)</p> <p>Requires knowledge of the infrastructure topography and the mapping of services to Cls</p> <p>Requires capability to simulate service workloads and demand volumes</p>	<p>Detects and correlates event records to determine the meaning of the events and the appropriate action (e.g. a user logs in three times with the incorrect password, which represents a security exception and is escalated through information security management procedures)</p> <p>Requires detailed knowledge of the normal operation of the infrastructure and services</p>
Proactive	<p>Used to determine the real-time status of a device, system or service – usually for critical components or following the recovery of a failed device to ensure that it is fully recovered (i.e. is not going to cause further incidents)</p>	<p>Event records are correlated over time to build trends for proactive problem management</p> <p>Patterns of events are defined and programmed into correlation tools for future recognition</p>



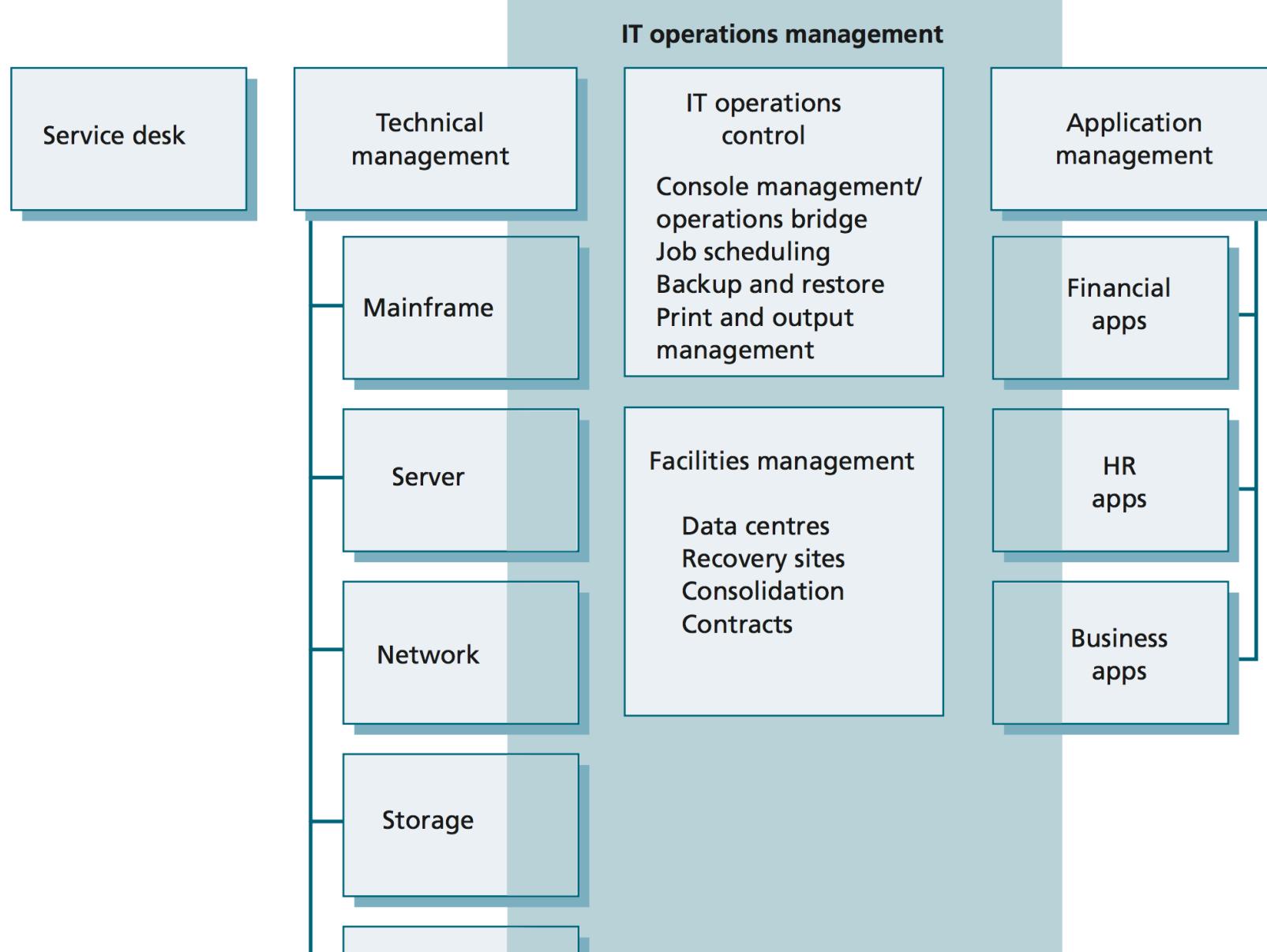
- Reactive versus proactive monitoring
- Continuous measurement versus exception-based measurement
- Performance versus output
- Monitoring items being tested
- Measurement, Metrics and Key performance Indicators

# IT SERVICE OPERATION

---

## LE FUNZIONI

# LE FUNZIONI DEL SERVICE OPERATION

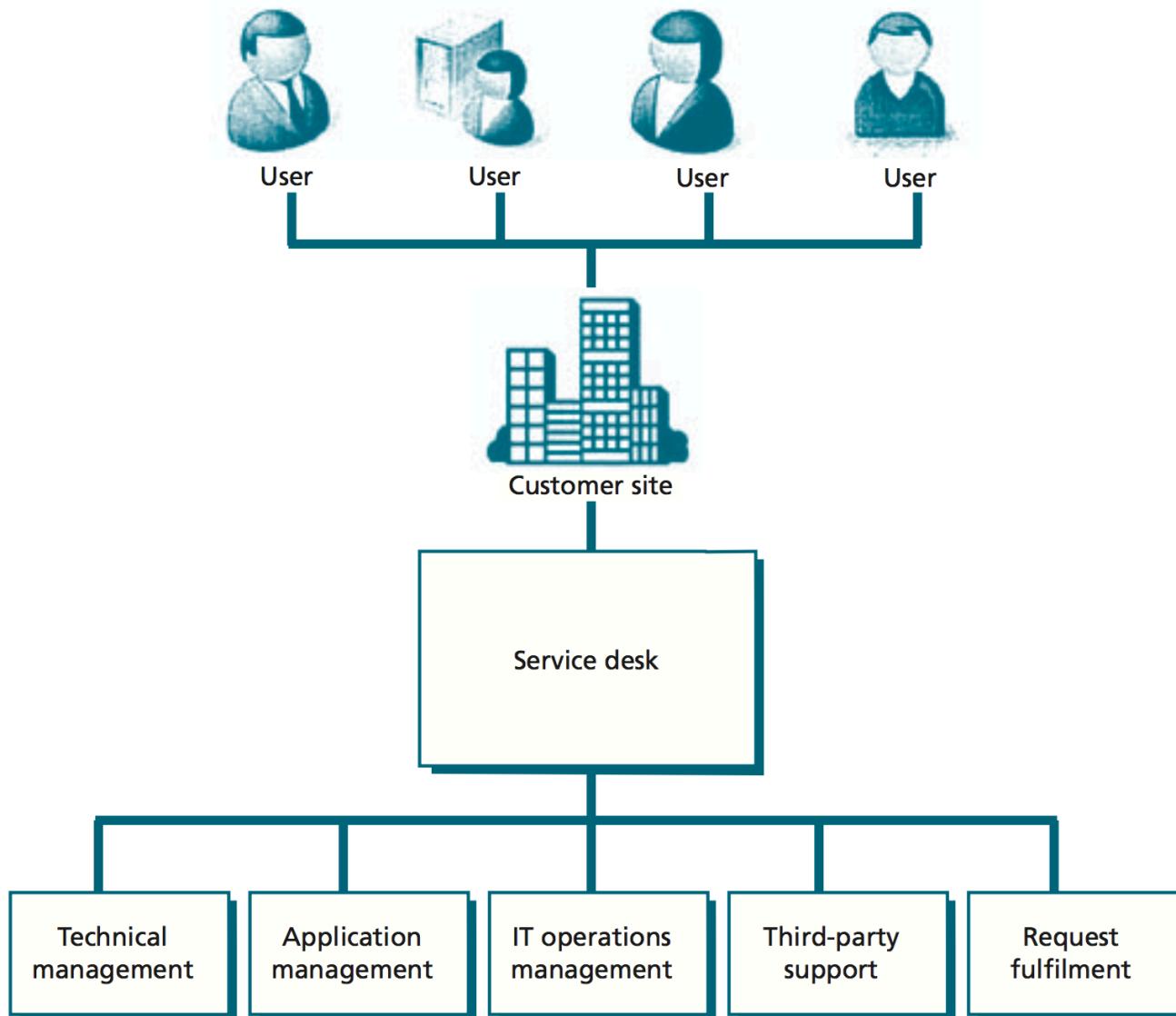




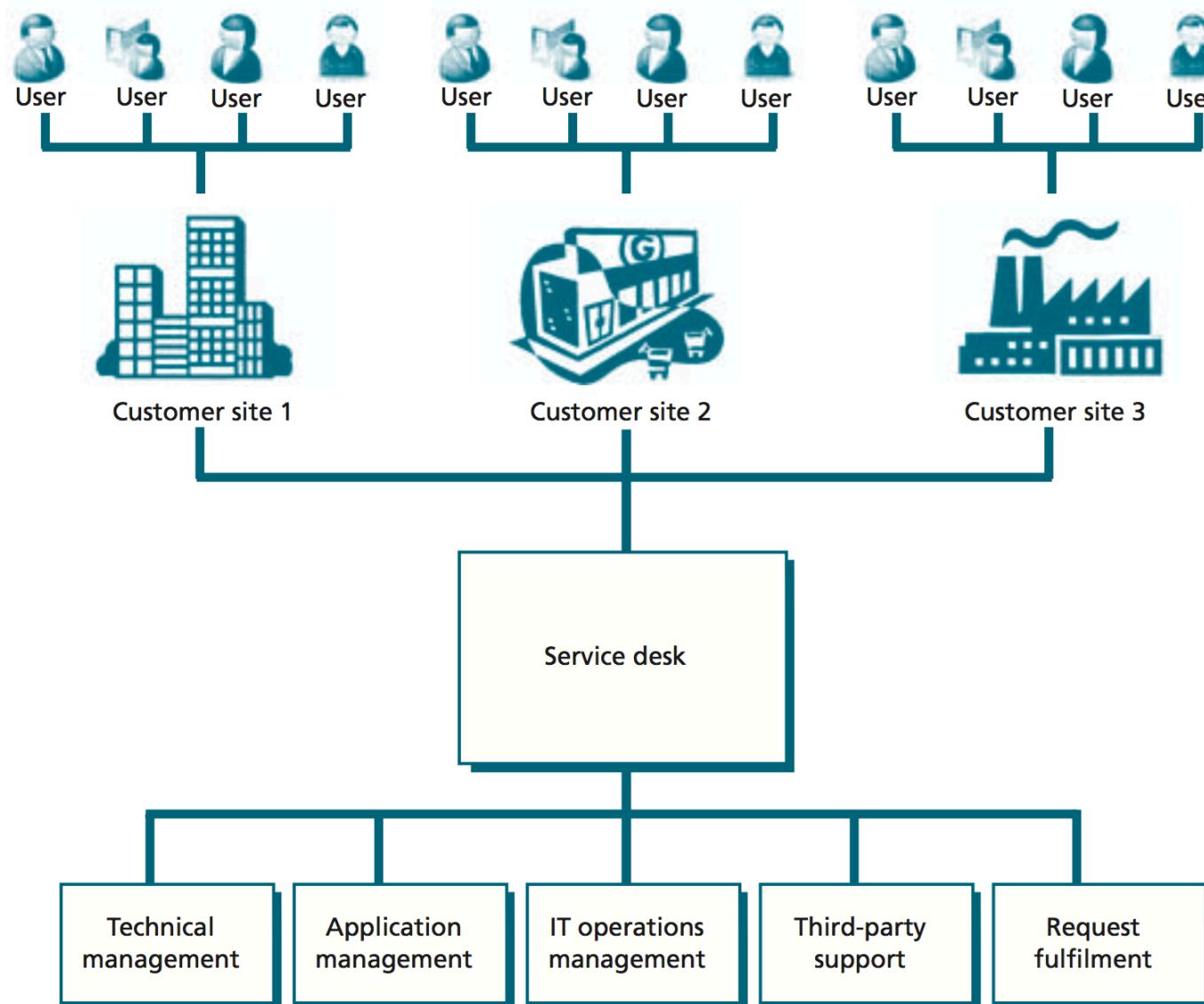
Il **Service Desk** è il “single point of contact” per gli utenti ogniqualvolta si verifica l’interruzione di un servizio o per le richieste di nuovi servizi.

Il Service Desk è il punto di congiunzione fra gli utenti e gli altri gruppi e processi IT. Perchè questo possa avvenire, normalmente viene tenuto separato dalle altre funzioni.

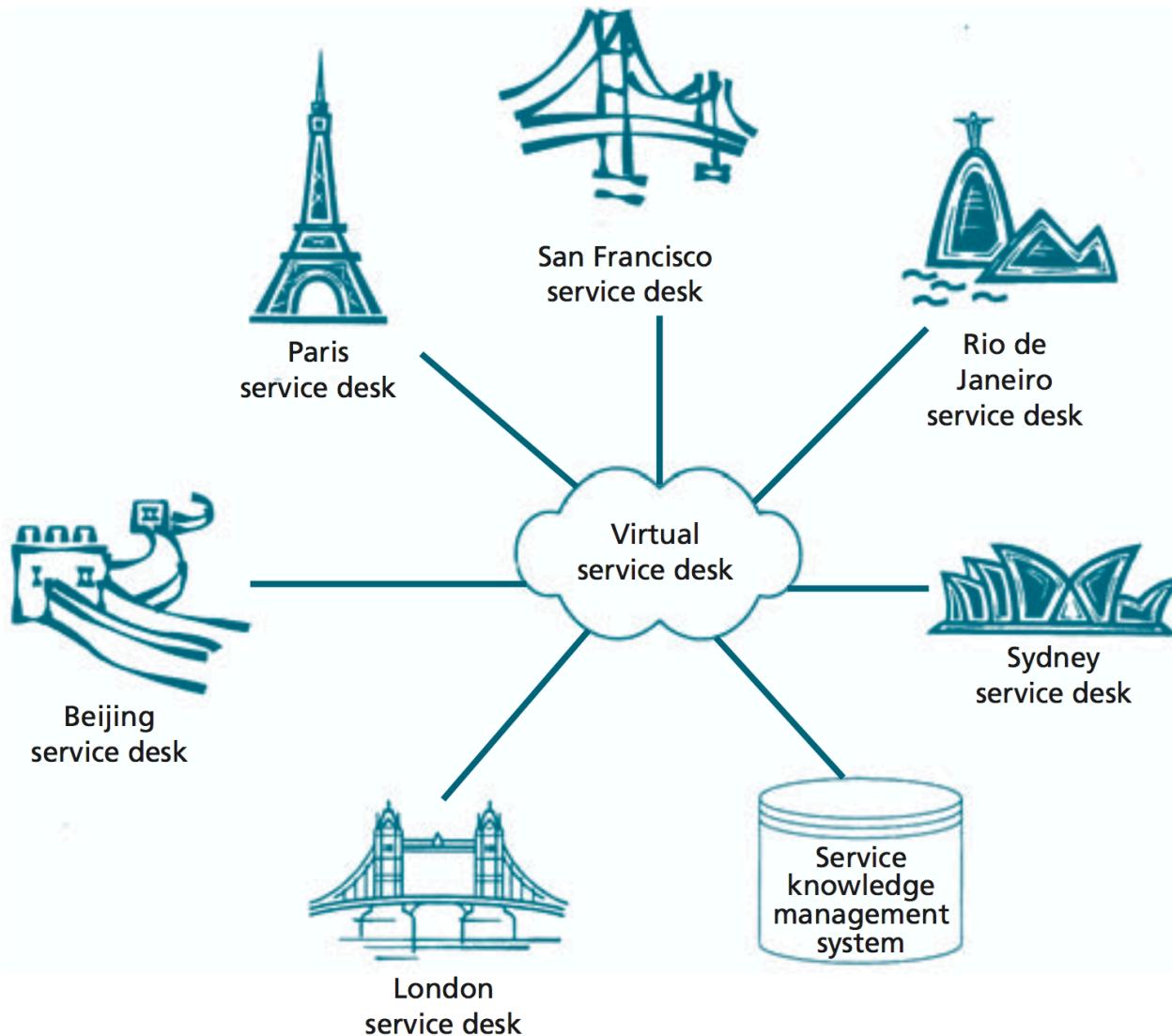
# LE FUNZIONI DEL SERVICE OPERATION



# LE FUNZIONI DEL SERVICE OPERATION



# LE FUNZIONI DEL SERVICE OPERATION





La funzione di **Technical Management** fornisce le capacità tecniche e le risorse necessarie per supportare le attività day-by-day e la gestione dell'infrastruttura IT.

Il **Technical Management** gioca anche una ruolo determinante nella progettazione, nel test, nel rilascio in esercizio e nell'ottimizzazione dei servizi IT.



**IT Operations Management** è la funzione responsabile delle attività quotidiane necessarie a gestire i servizi e supportare l'infrastruttura IT.

La funzione opera all'interno degli standard definiti in fase di progettazione dei servizi IT (Service Design). In alcune organizzazioni la funzione è centralizzata in un unico dipartimento mentre in altre può essere distribuita.



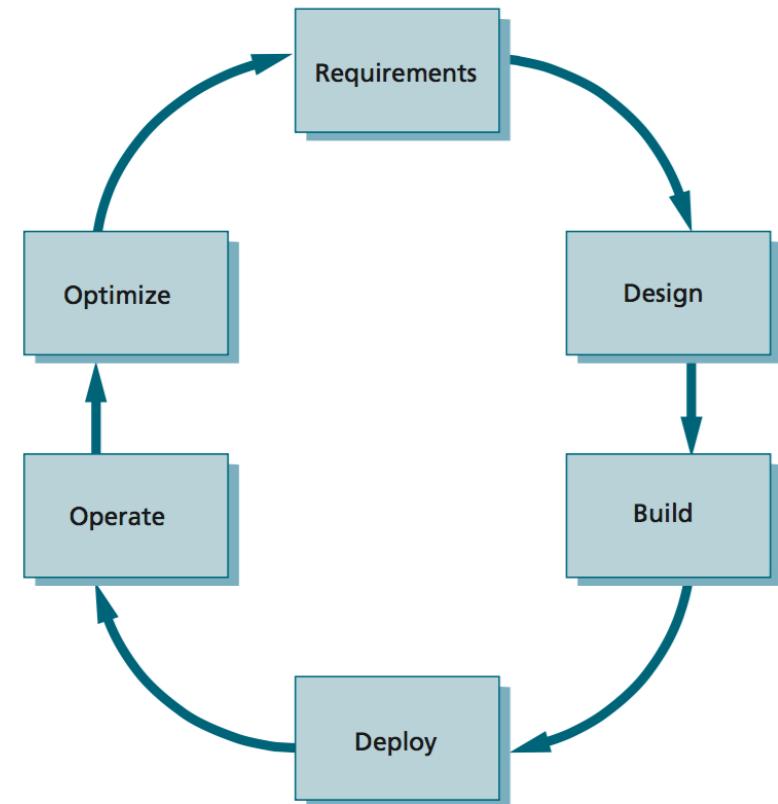
La funzione è divisa in due sottofunzioni:

- **IT Operations Control** che si preoccupa di assicurare lo svolgimento delle attività di routine (backup, monitoraggio, etc.)
- **Facilities Management** che si occupa della gestione delle location fisiche (data center, server room, etc.), a partire dalla componente contrattuale, compresi tutti i contratti di outsourcing.

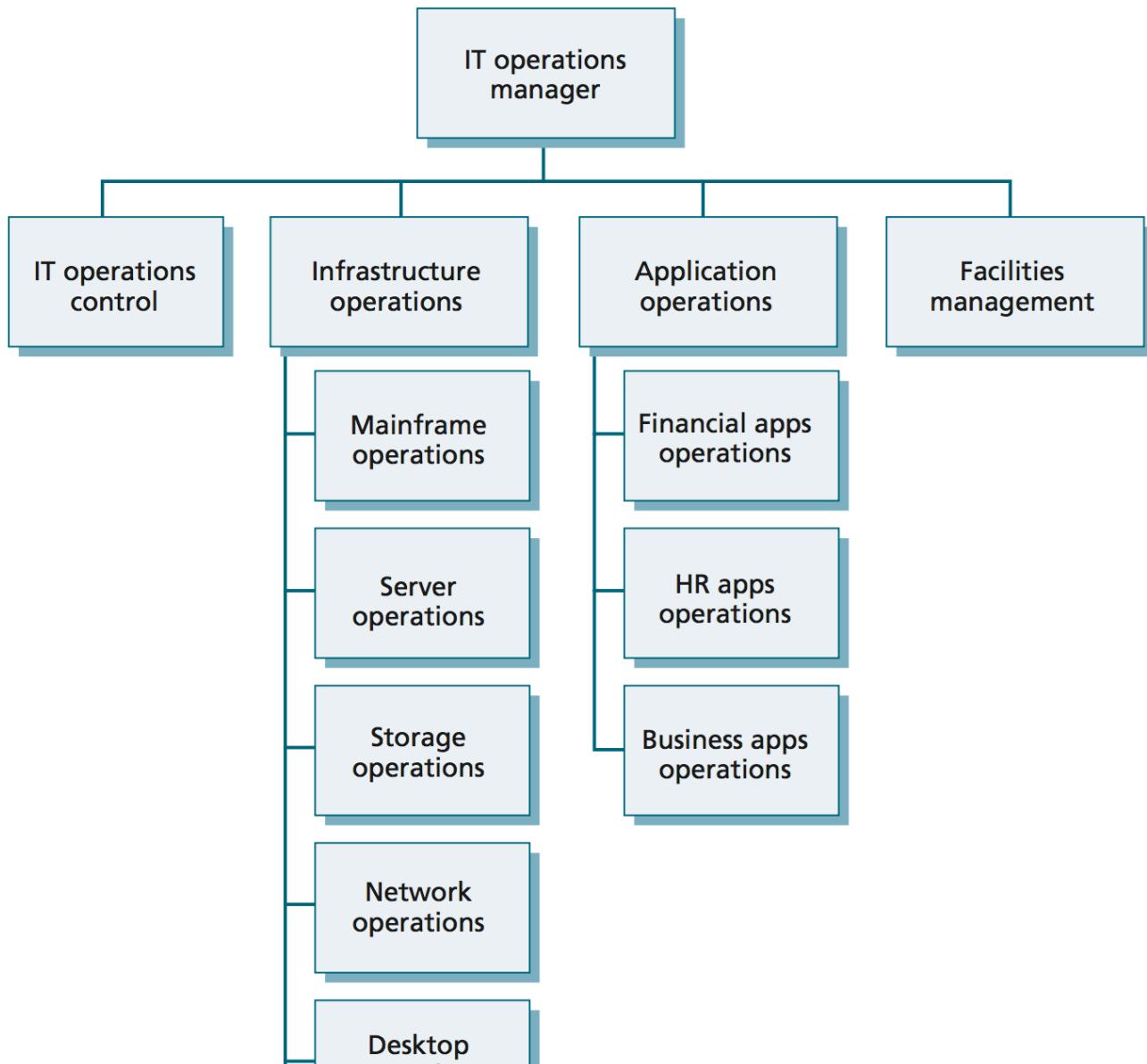


La funzione di **Application Management** è responsabile della gestione delle applicazioni durante tutto il loro ciclo di vita.

L'**Application Management** è usualmente suddiviso in reparti a seconda dell'applicazione o della area applicativa in questione.

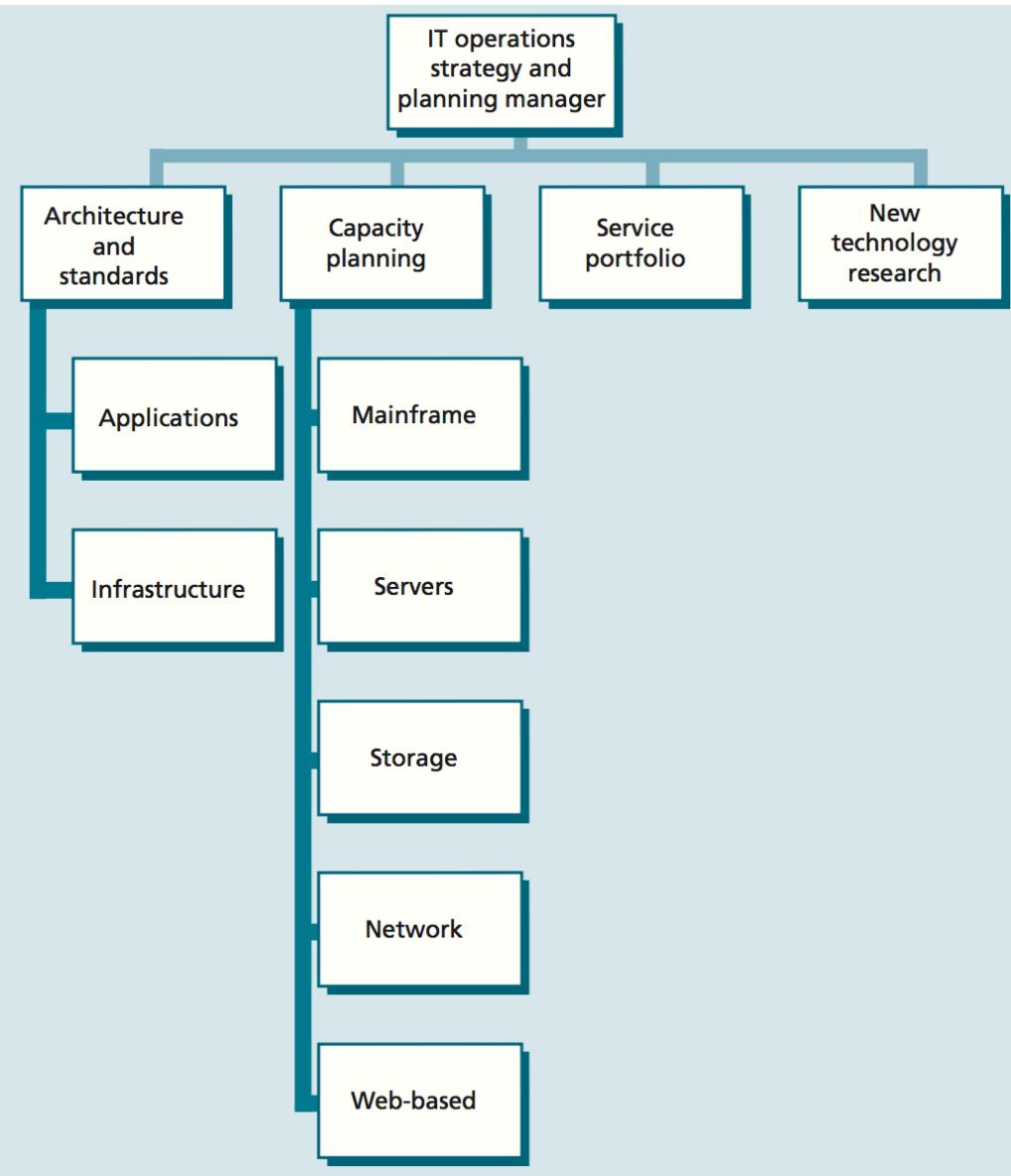


# LE FUNZIONI DEL SERVICE OPERATION



ORGANIZZAZIONE PER  
SPECIALIZZAZIONE TECNICA

# LE FUNZIONI DEL SERVICE OPERATION



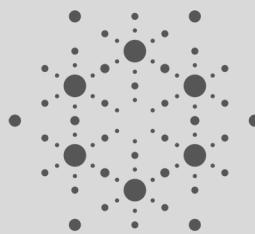
ORGANIZZAZIONE PER  
AREA FUNZIONALE

DOMANDE?

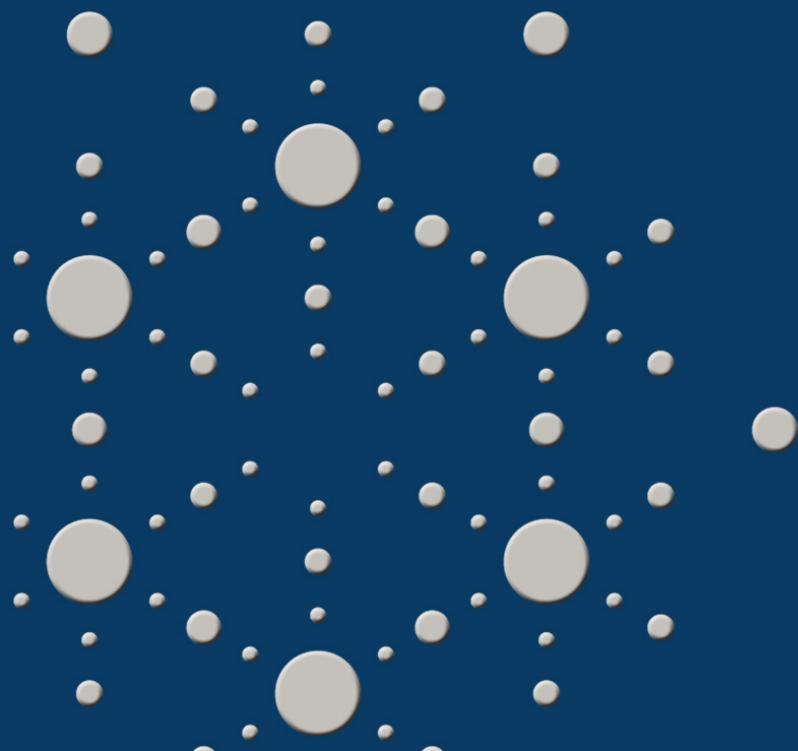
---

# GRAZIE PER L'ATTENZIONE.

---



**NETCOM**  
IT Life Cycle Management



**N E T C O M**  
IT Life Cycle Management