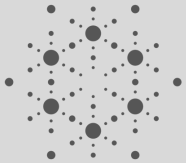
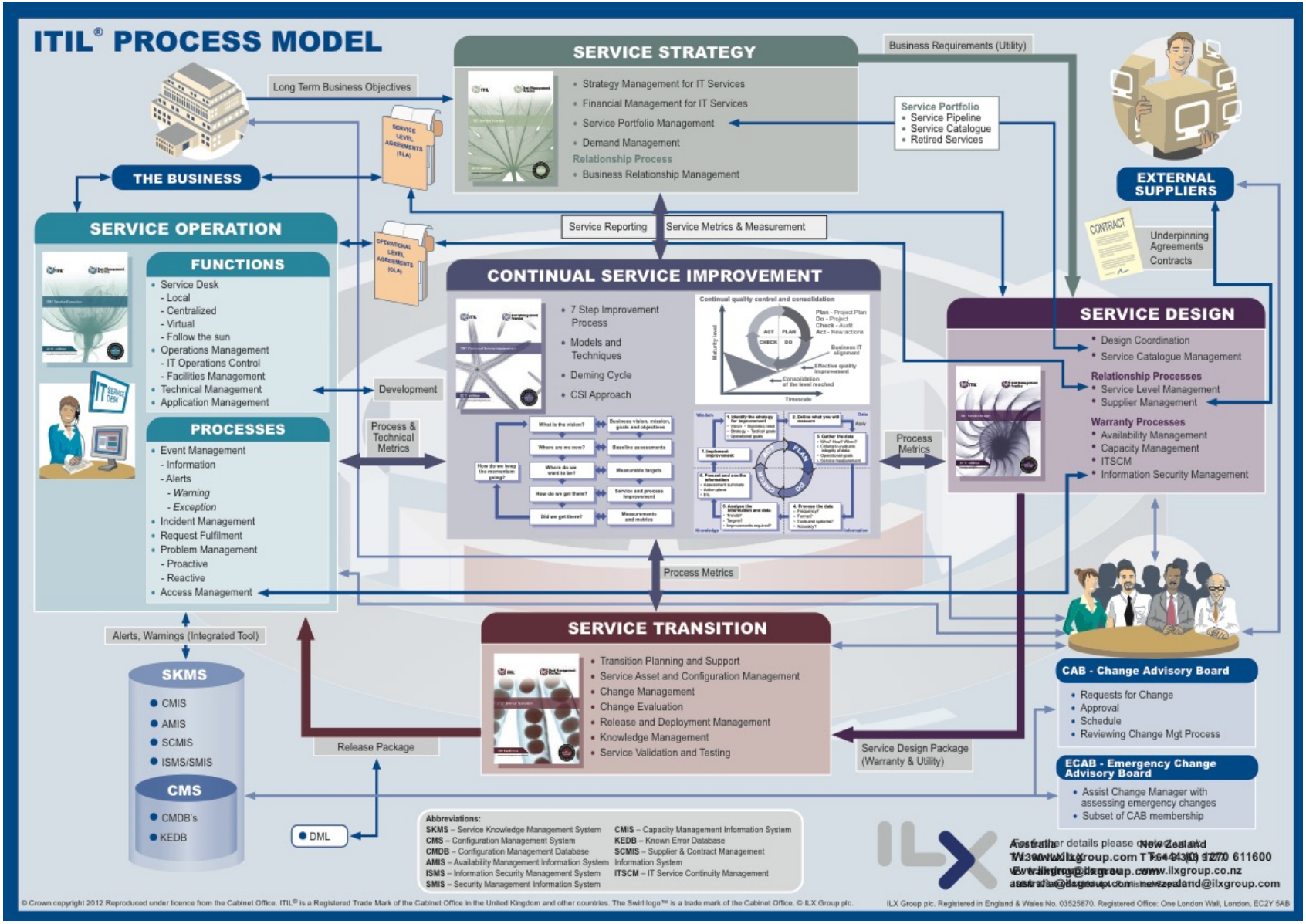


NETCOM
IT Life Cycle Management

ITIL 2011 – ITIL Service Operation

FRANCESCO CLABOT

ITIL: IL FRAMEWORK



ITIL Core Books

Core ITIL lifecycle publication	Processes described in the publication
ITIL Service Strategy	Strategy management for IT services
	Service portfolio management
	Financial management for IT services
	Demand management
	Business relationship management
ITIL Service Design	Design coordination
	Service catalogue management
	Service level management
	Availability management
	Capacity management
	IT service continuity management
	Information security management
	Supplier management

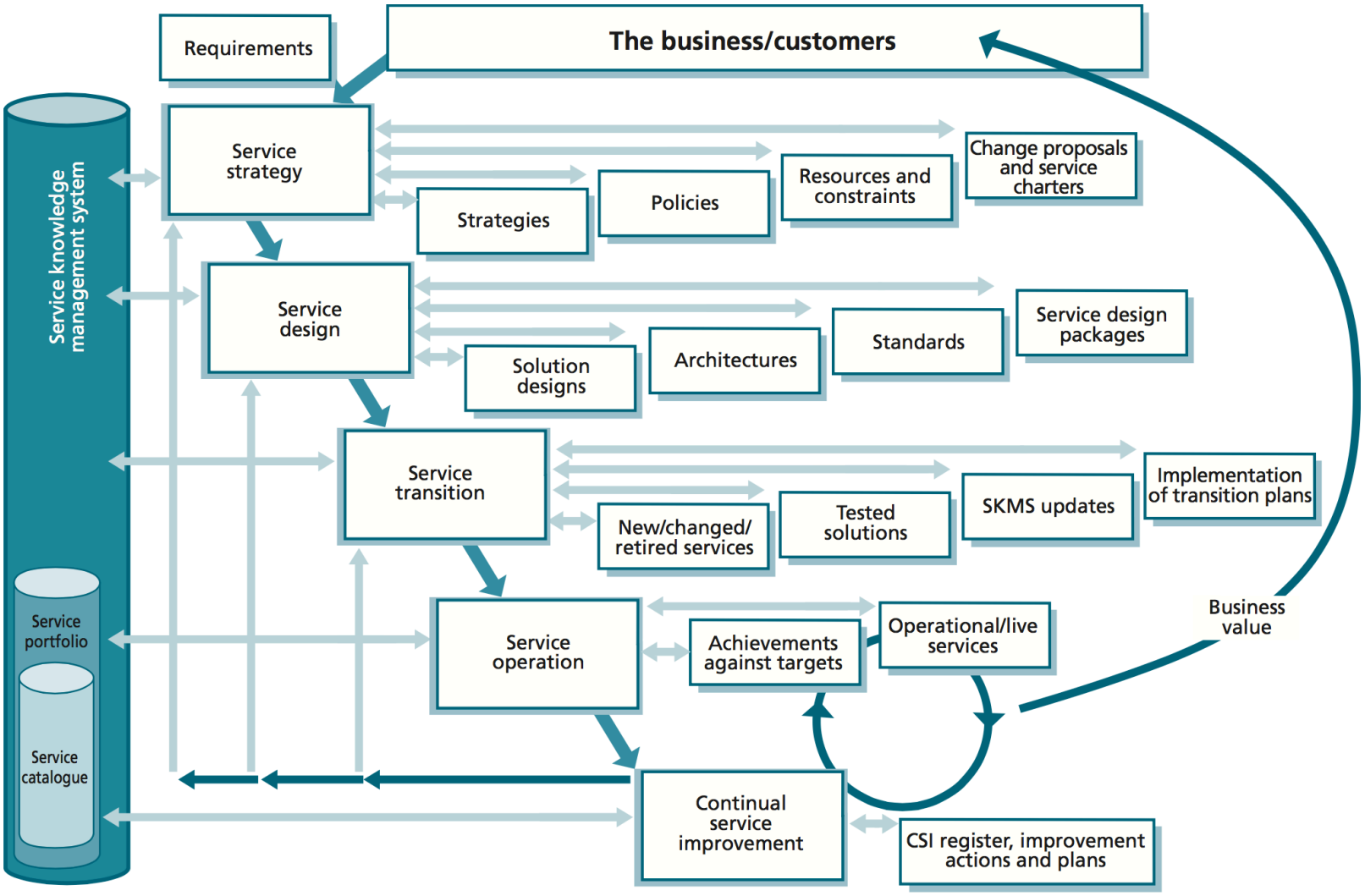
ITIL Core Books

ITIL Service Transition	Transition planning and support
	Change management
	Service asset and configuration management
	Release and deployment management
	Service validation and testing
	Change evaluation
	Knowledge management
ITIL Service Operation	Event management
	Incident management
	Request fulfilment
	Problem management
	Access management
ITIL Continual Service Improvement	Seven-step improvement process

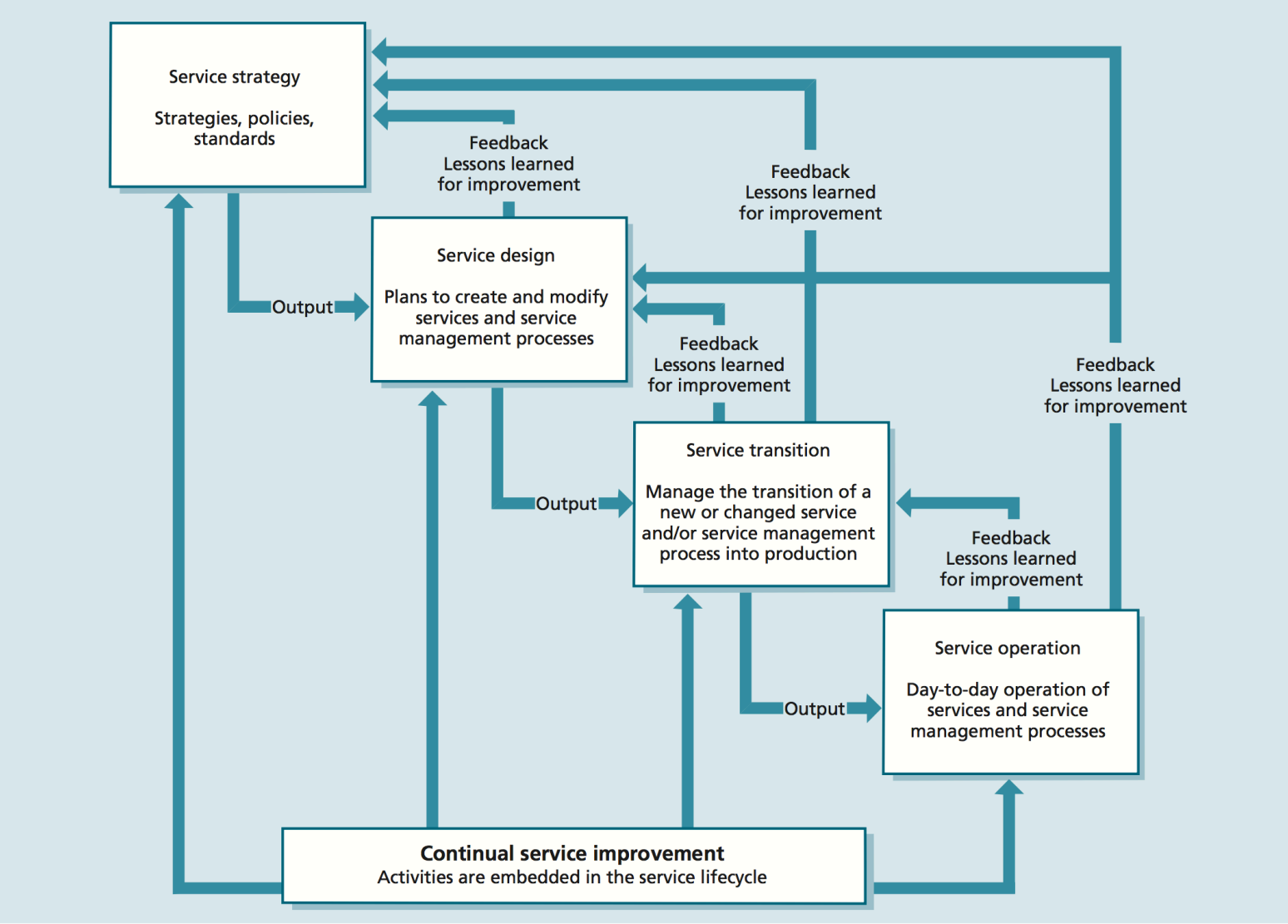
IT Service Operation

Principi base

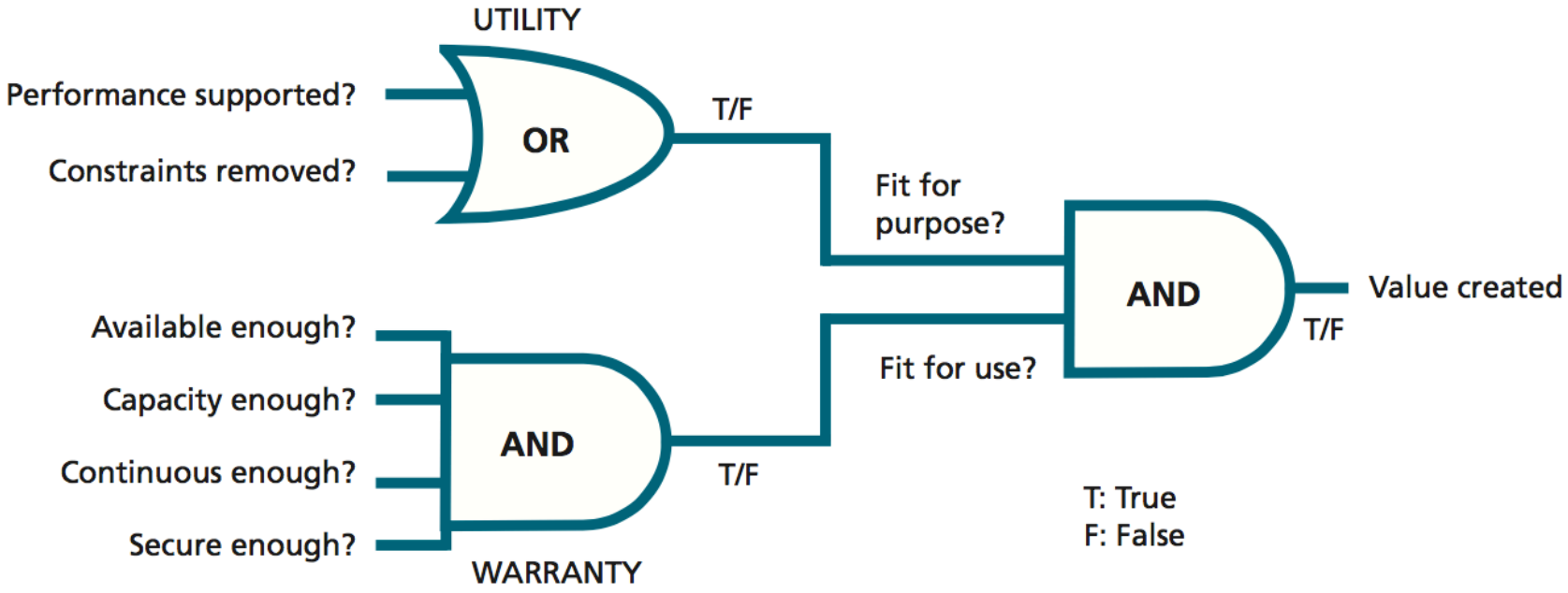
PRINCIPI BASE



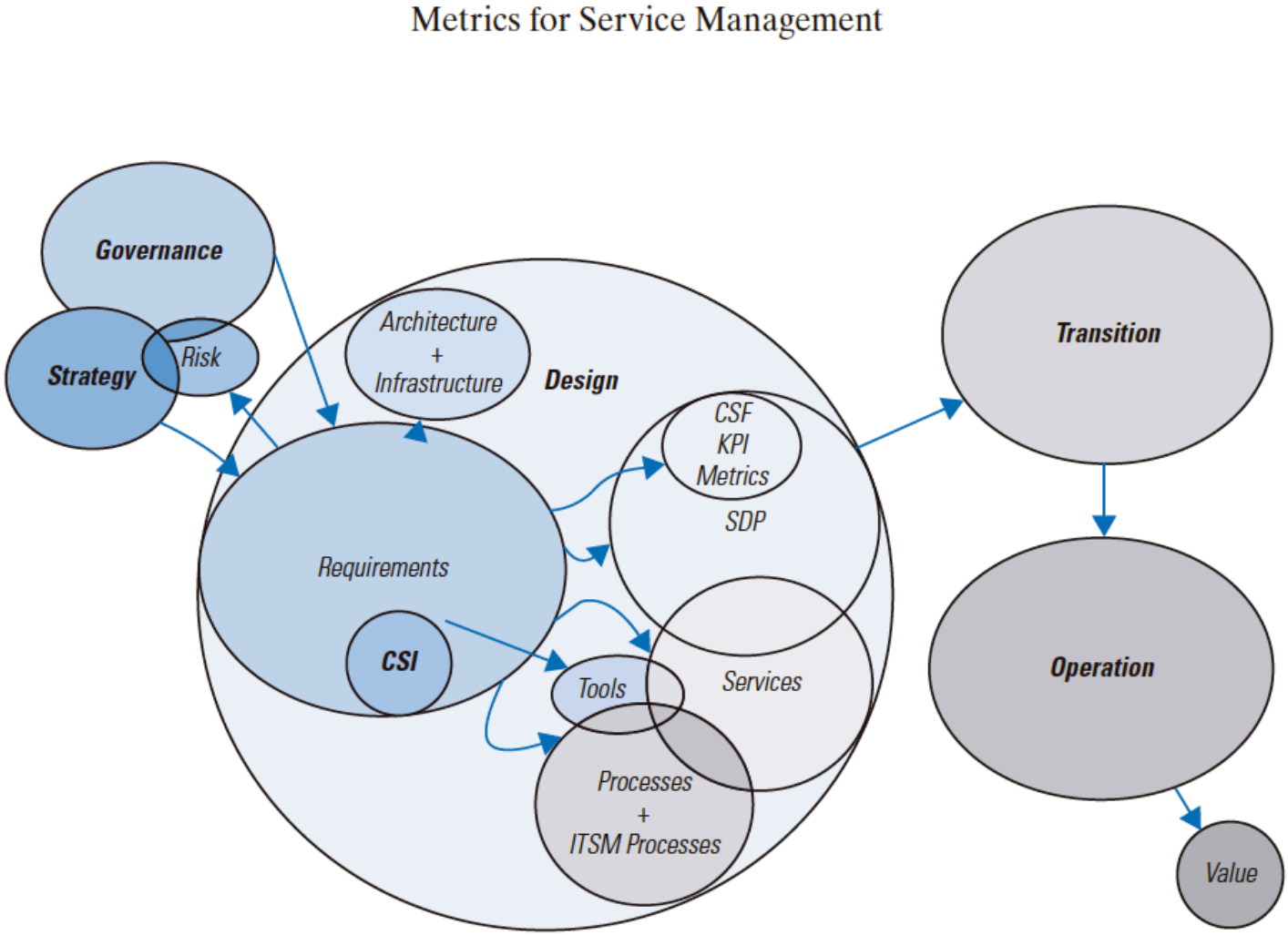
PRINCIPI BASE



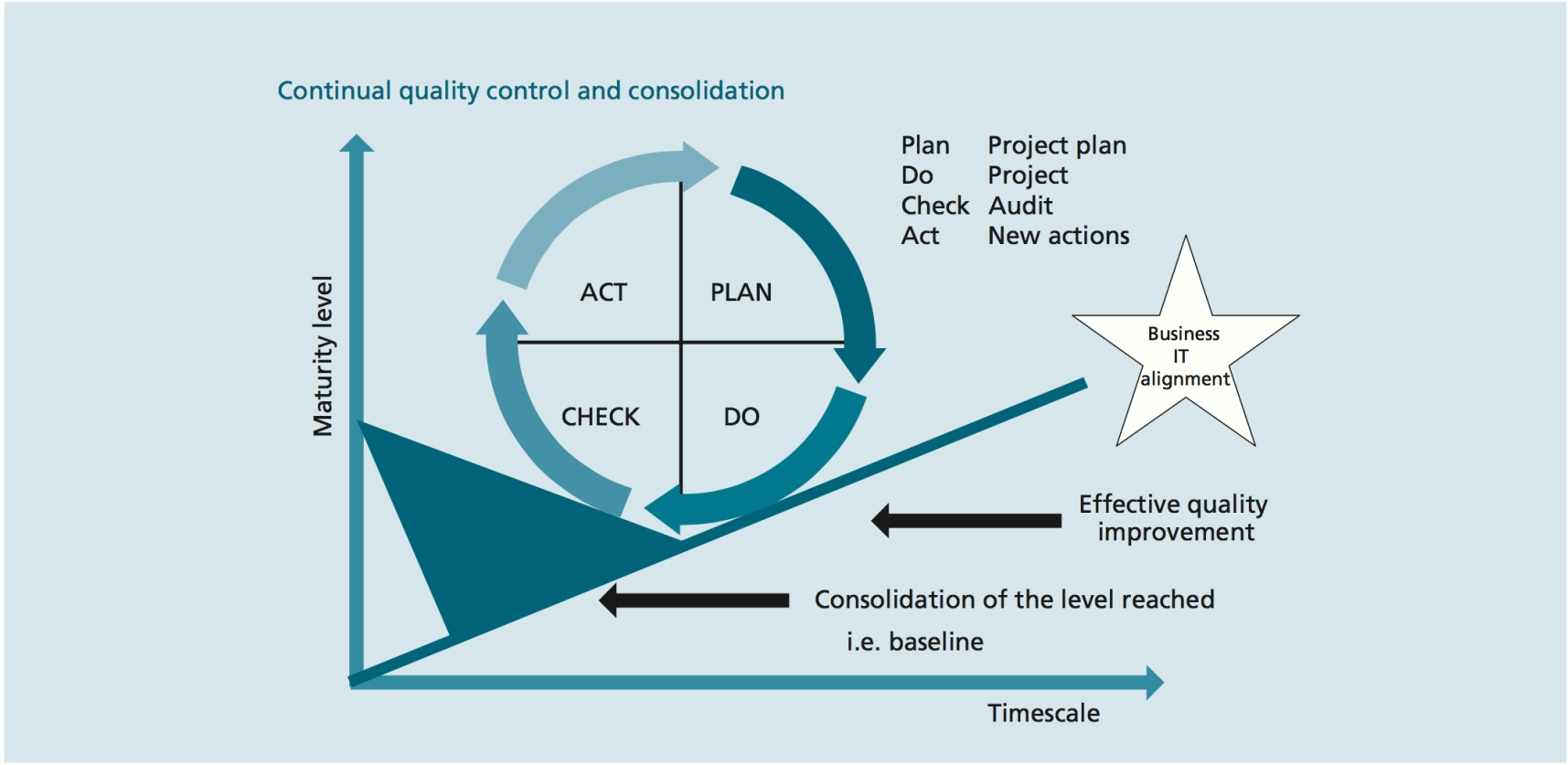
Value = Utility + Warranty



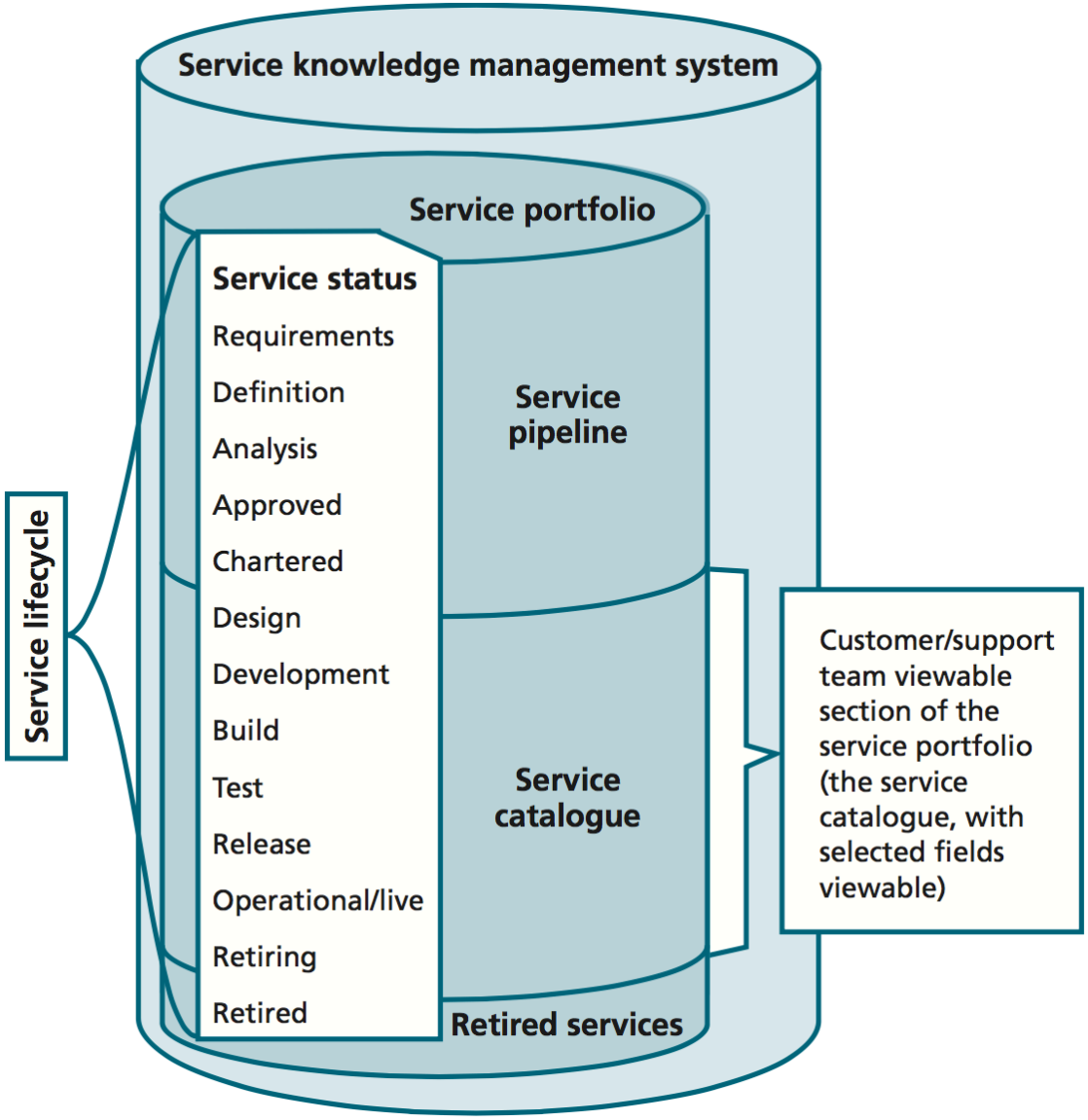
PRINCIPI BASE



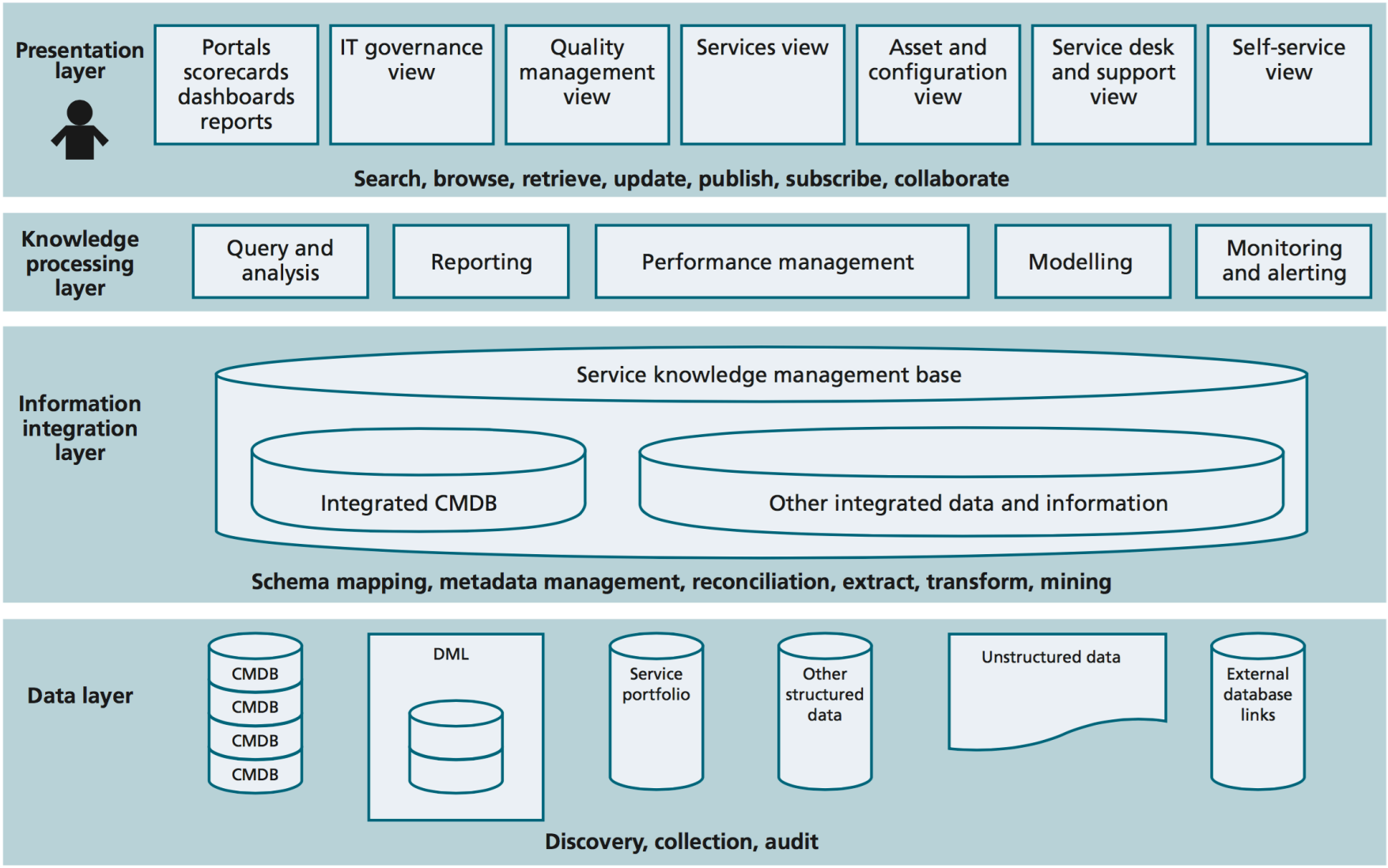
Ciclo di Deming



PRINCIPI BASE



PRINCIPI BASE



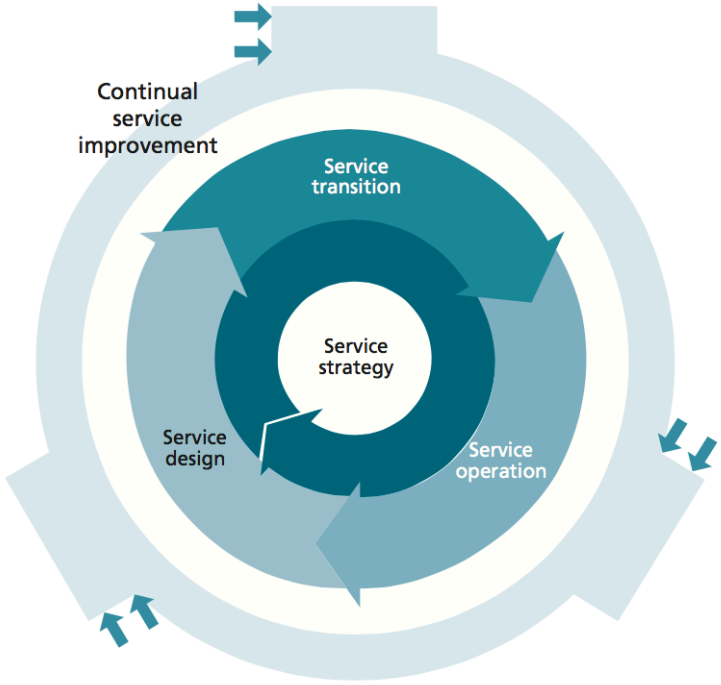
IT Service Operation

Obiettivi

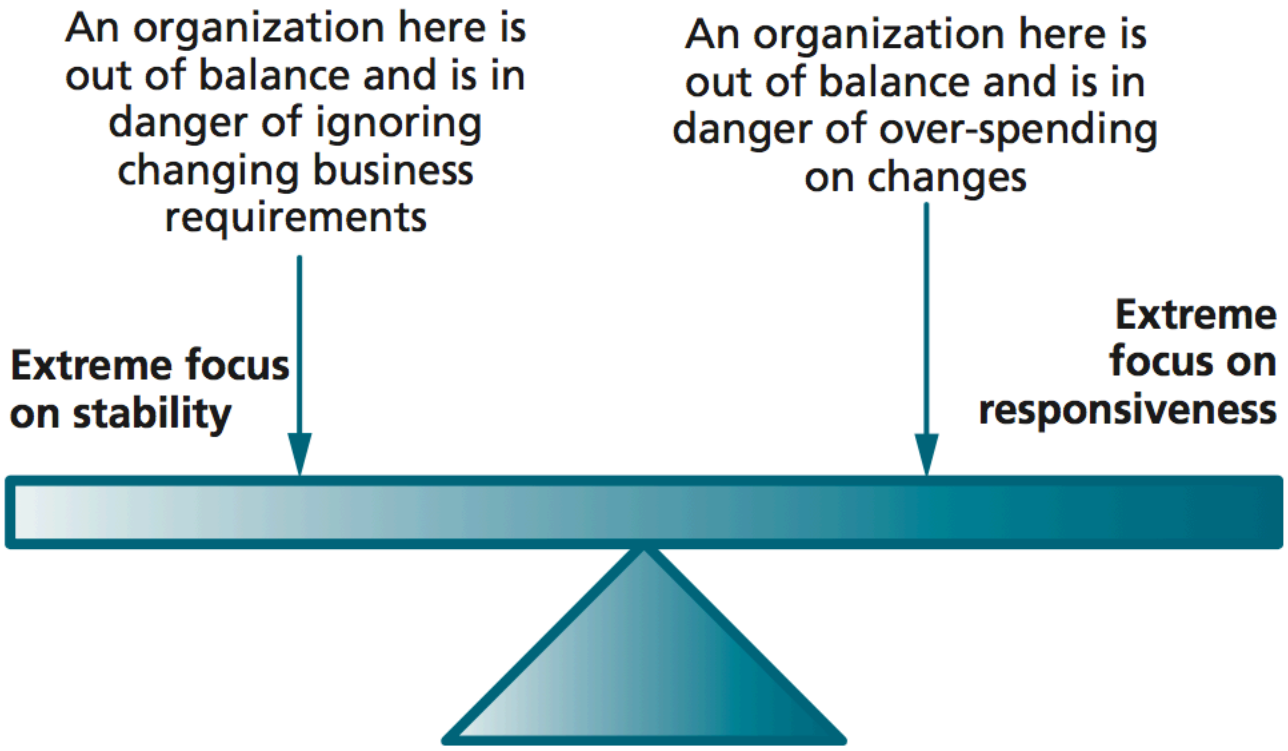
Obiettivi del Service Operation

ITIL Service Operation si occupa di garantire l'efficace ed efficiente erogazione dei Servizi ICT con l'obiettivo del raggiungimento dei livelli di funzionamento, dei costi e degli altri vincoli stabiliti.

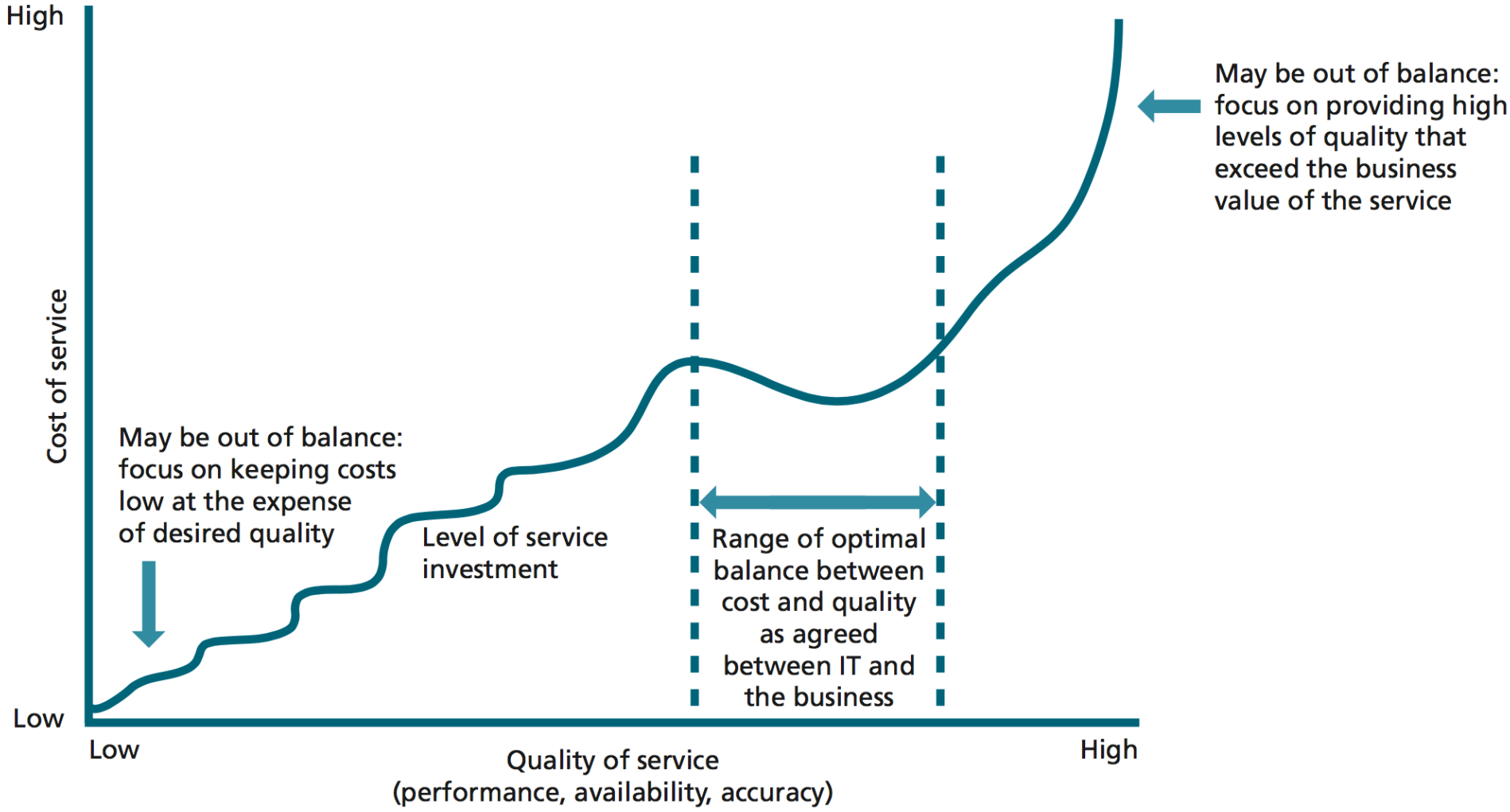
Inoltre aiuta le organizzazioni a sviluppare le capacità necessarie per erogare i Servizi ICT in modo affidabile e ripristinarne rapidamente il funzionamento in caso di problemi.



BILANCIAMENTO FRA STABILITÀ E TEMPI DI RISPOSTA



Bilanciamento fra Qualità e Costi



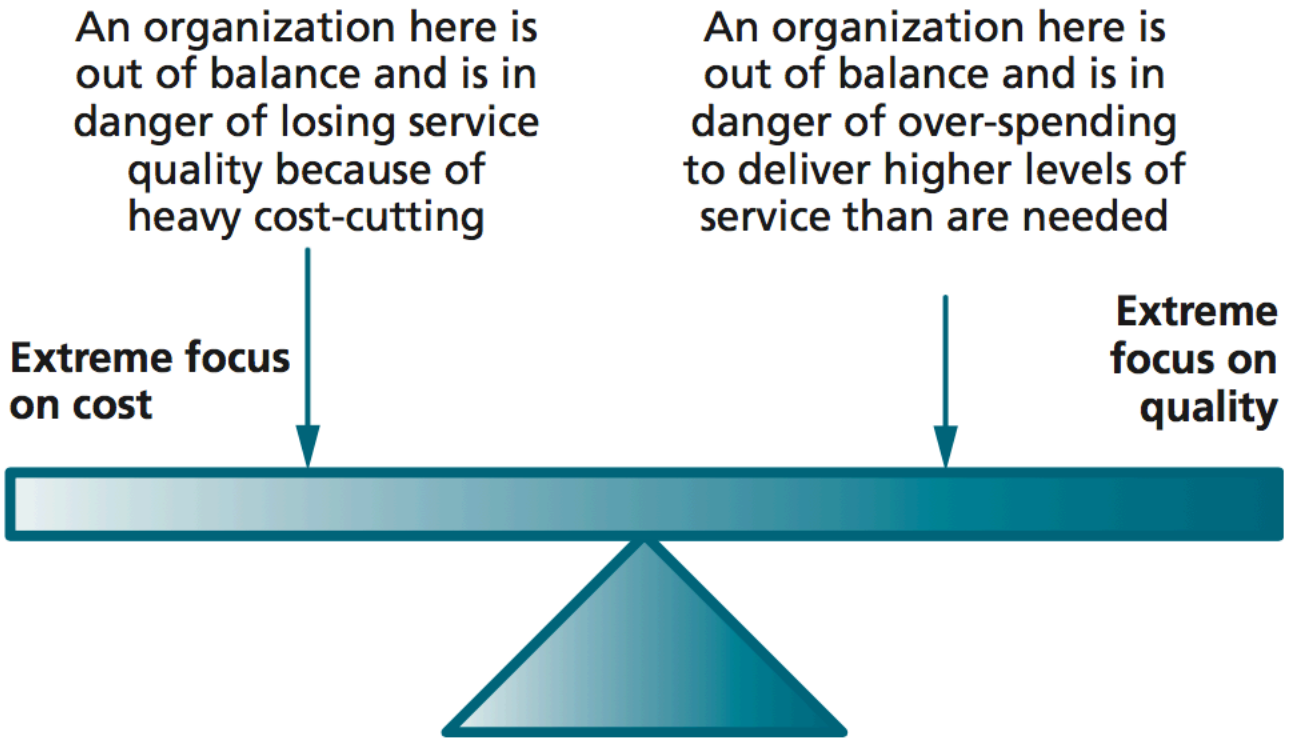
Bilanciamento fra Riduzione dei Costi e Qualità

Special note: just how far is too much?

Over the past several years, IT organizations have been under pressure to cut costs. In many cases this resulted in optimized costs and quality. But in other cases, costs were cut to the point where quality started to suffer. At first, the signs were subtle – small increases in incident resolution times and a slight increase in the number of incidents. Over time, though, the situation became more serious as staff worked long hours to handle multiple workloads and services ran on ageing or outdated infrastructure.

There is no simple calculation to determine when costs have been cut too far, but good SLM is crucial to making customers aware of the impact of cutting too far, so recognizing these warning signs and symptoms can greatly enhance an organization's ability to correct this situation.

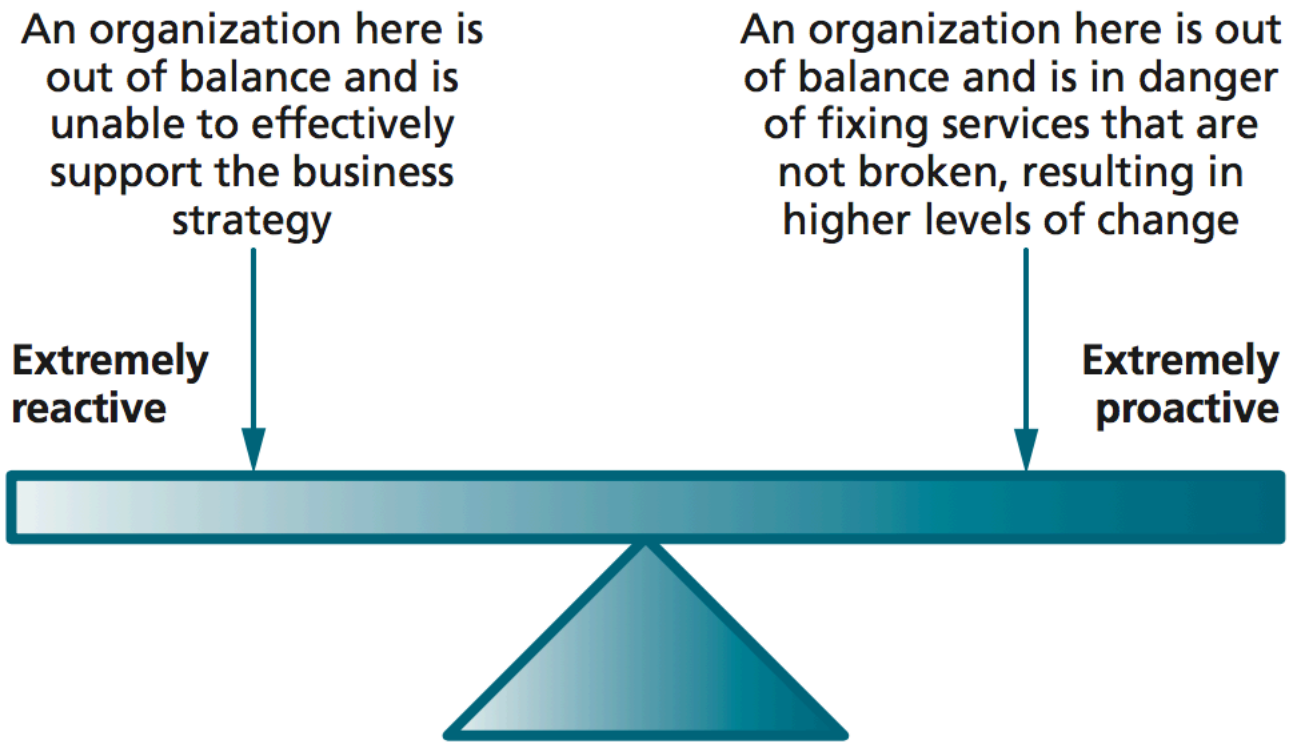
Bilanciamento fra Riduzione dei Costi e Qualità



Bilanciamento fra Riduzione dei Costi e Qualità

	Extreme focus on quality	Extreme focus on cost
Primary focus	Delivering the level of quality demanded by the business regardless of what it takes	Meeting budget and reducing costs
Typical problems experienced	Escalating budgets IT services generally deliver more than is necessary for business success Escalating demands for higher-quality services Use of more support resources and other service assets than necessary to fulfil service demands.	IT limits the quality of service based on their budget availability Escalations from the business to get more service from IT
Financial management	IT usually does not have a method of communicating the cost of IT services. Accounting methods are based on an aggregated method (e.g. cost of IT per user)	Financial reporting is done purely on budgeted amounts. There is no way of linking activities in IT to the delivery of IT services

Bilanciamento Reattivo vs Proattivo



Bilanciamento Reattivo vs Proattivo

E’ corretto gestire i servizi in una logica proattiva, ma per giungere a questa capacità sarà necessario superare alcune difficili sfide riguardanti:

- La **Maturità** dell’organizzazione
- La **Cultura** dell’organizzazione
- Il **Ruolo** dell’IT ed il suo **Mandato**
- Il Livello di **integrazione** fra gestione dei processi e strumenti
- La Maturità e l’ampiezza della **Knowledge** nell’organizzazione

Bilanciamento Reattivo vs Proattivo

	Extremely reactive	Extremely proactive
Primary focus	Responds to business needs and incidents only after they are reported	Anticipates business requirements before they are reported and problems before they occur
Typical problems experienced	Preparing to deliver new services takes a long time because each project is dealt with as if it is the first Similar incidents occur again and again, as there is no way of trending them Staff turnover is high and morale is generally low, as IT staff keep moving from project to project without achieving a lasting, stable set of IT services	Money is spent before the requirements are stated. In some cases IT purchases items that will never be used because they anticipated the wrong requirements or because the project is stopped IT staff tend to have been in the organization for a long time and tend to assume that they know the business requirements better than the business does
Capacity planning	Wait until there are capacity problems and then purchase surplus capacity to last until the next capacity-related incident	Anticipate capacity problems and spend money on preventing these – even when the scenario is unlikely to happen

Bilanciamento Reattivo vs Proattivo

IT service continuity planning	No plans exist until after a major event or disaster IT plans focus on recovering key systems, but without ensuring that the business can recover its processes	Over-planning (and over-spending) of IT recovery options. Usually immediate recovery is provided for most IT services, regardless of their impact or priority
Change management	Changes are often not logged, or logged at the last minute as emergency changes Not enough time for proper impact and cost assessments Changes are poorly tested and controlled, resulting in a high number of incidents	Changes are requested and implemented even when there is no real need, i.e. a significant amount of work done to fix items that are not broken

Interfacce con gli altri gruppi di Processi

Lifecycle stage	Service operation inputs (from the lifecycle stages in the first column)	Service operation outputs (to the lifecycle stages in the first column)
Service strategy	Vision and mission Service portfolio Policies Strategies and strategic plans Priorities Financial information and budgets Demand forecasts and strategies Strategic risks	Operating risks Operating cost information for total cost of ownership (TCO) calculations Actual performance data
Service design	Service catalogue Service design packages, including: ■ Details of utility and warranty ■ Operations plans and procedures ■ Recovery procedures Knowledge and information in the SKMS Vital business functions Hardware and software maintenance requirements Designs for service operation processes and procedures SLAs, OLAs and underpinning contracts Security policies	Operational requirements Actual performance data RFCs to resolve operational issues Historical incident and problem records

INTERFACCE CON GLI ALTRI GRUPPI DI PROCESSI

Service transition	New or changed services Known errors Standard changes for use in request fulfilment Knowledge and information in the SKMS (including the configuration management system) Change schedule	RFCs to resolve operational issues Feedback on quality of transition activities Input to operational testing Actual performance information Input to change evaluation and change advisory board meetings
Continual service improvement	Results of customer and user satisfaction surveys Service reports and dashboards Data required for metrics, key performance indicators (KPIs) and critical success factors (CSFs) RFCs for implementing improvements	Operational performance data and service records Proposed problem resolutions and proactive measures Knowledge and information in the SKMS Achievements against metrics, KPIs and CSFs Improvement opportunities logged in the continual service improvement register

The Service Operation Processes

- Event Management
- Incident Management
- Request Fulfulment
- Problem Management
- Access Management

IT Service Operation

I Processi

I Processi di Service Operation

Event Management

EVENT MANAGEMENT IN ITIL

Nasce con ITIL v3 e si inserisce nella fase Service Operation del modello di lifecycle dei servizi IT

In ITIL v2, l'Event Management era trattato solo parzialmente

In ITIL v3, l'Event Management diventa un processo indipendente

Le motivazioni di questa "evoluzione" sono da ricercarsi nella diffusione dei tool di monitoraggio, che permettono di gestire gli eventi in modo appropriato

COSA È UN EVENTO?

<<Un cambio di stato che ha rilevanza ai fini della gestione di un Configuration Item o di un servizio IT>>

Normalmente si tratta di segnalazioni utili (es. Microinterrruzioni su una linea dati che non pregiudicano il servizio ma che indicano comunque la necessità di analisi più approfondite)

Un evento potrebbe indicare un malfunzionamento di una parte dell'infrastruttura ed essere un trigger per la generazione di un incidente.

Gli eventi possono anche indicare un andamento normale delle attività oppure la finalizzazione di un intervento di routine (es. il cambiamento di un tape).

INPUT DEL PROCESSO: IL MONITORAGGIO

Si basa su sistemi di monitoraggio.

Differisce dal normale monitoraggio in quanto genera ed identifica eventi (cambi di stato), mentre i sistemi di monitoraggio controllano i componenti dell'infrastruttura anche in assenza di eventi.

Tipi di monitoraggio:

- **Sistemi di monitoraggio attivi**
  - (polling del sistema di moniotraggio)
- **Sistemi di monitoraggio passivi**
  - (il CI comunica al sistema di monitoraggio il suo stato)

EVENT MANAGEMENT: SCOPO

Il core business del processo di

Event Management

e' quello di identificare gli eventi, capirne il senso e determinare l'azione piu' appropriata.

L'**Event Management** può anche essere utile per automatizzare delle attività di routine, quali azionare in automatico l'avvio di script se determinate condizioni si verificano, etc...

IL MONITORAGGIO

Il Monitoraggio

The difference between monitoring and event management

Monitoring and event management are closely related, but slightly different in nature. Event management is focused on generating and detecting meaningful notifications about the status of the IT infrastructure and services.

While it is true that monitoring is required to detect and track these notifications, monitoring is broader than event management. For example, monitoring tools will check the status of a device to ensure that it is operating within acceptable limits, even if that device is not generating events.

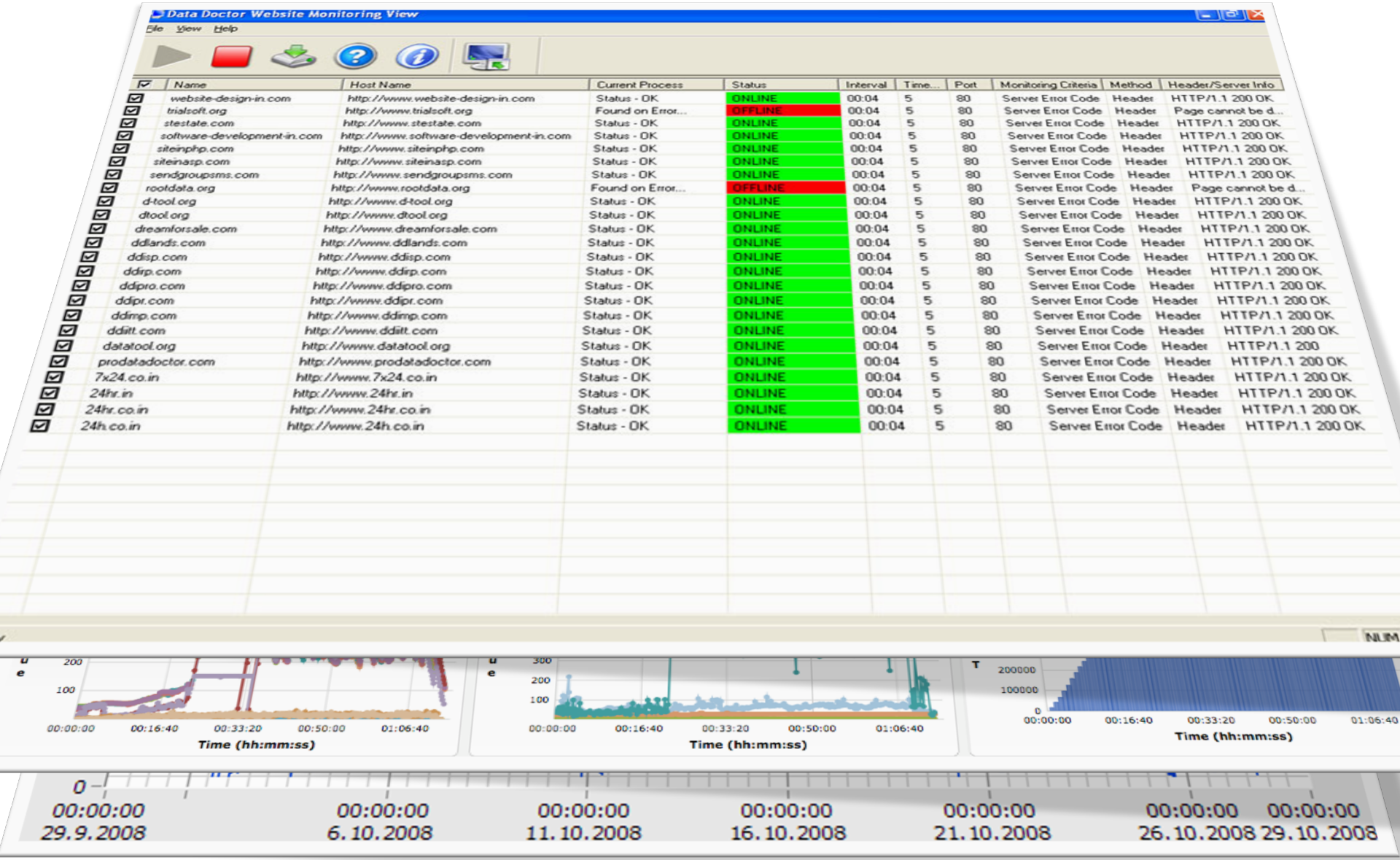
Put more simply, event management works with occurrences that are specifically generated to be monitored. Monitoring tracks these occurrences, but it will also actively seek out conditions that do not generate events.

Tipi di Evento:

- Informational
- Warning
- Exception

Non esiste una regola definitiva per categorizzare gli eventi

IL MONITORAGGIO

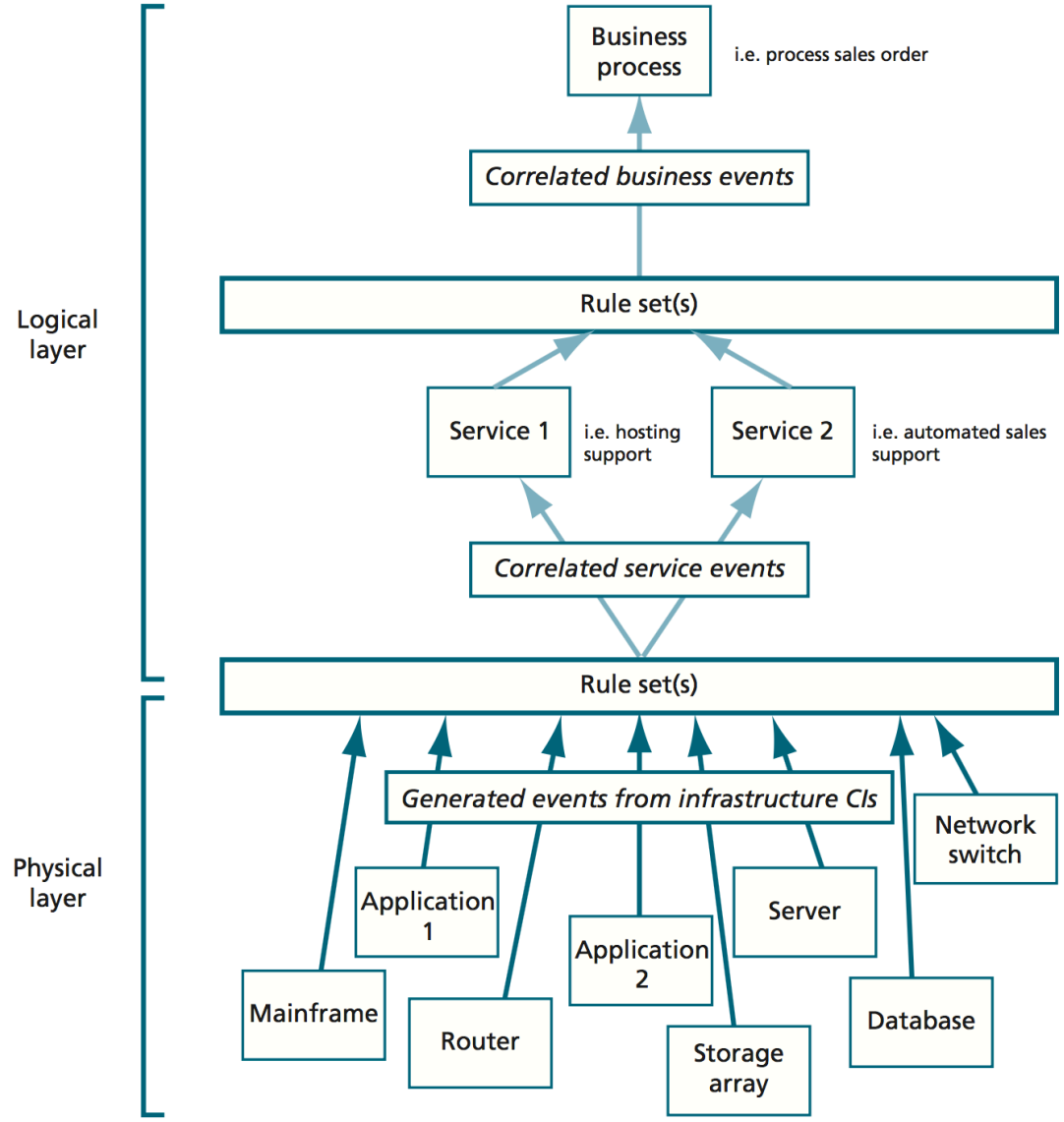


IL MONITORAGGIO

Non esiste uno standard. Dipende molto dai tool in uso. Di solito è utile tracciare:

- Device
- Component
- Type of failure
- Date/time
- Parameters in exception
- Unique identifier to allow for tracking of the event across the event management infrastructure and correlation into the other ITSM processes like incident, problem and change
- Value

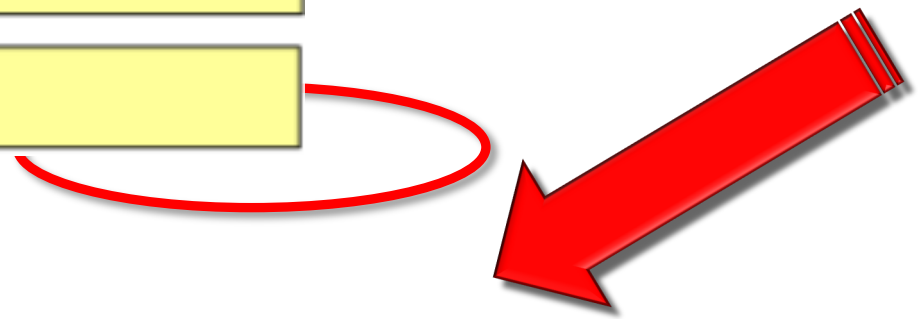
EVENTI, SERVIZI E PROCESSI DI BUSINESS



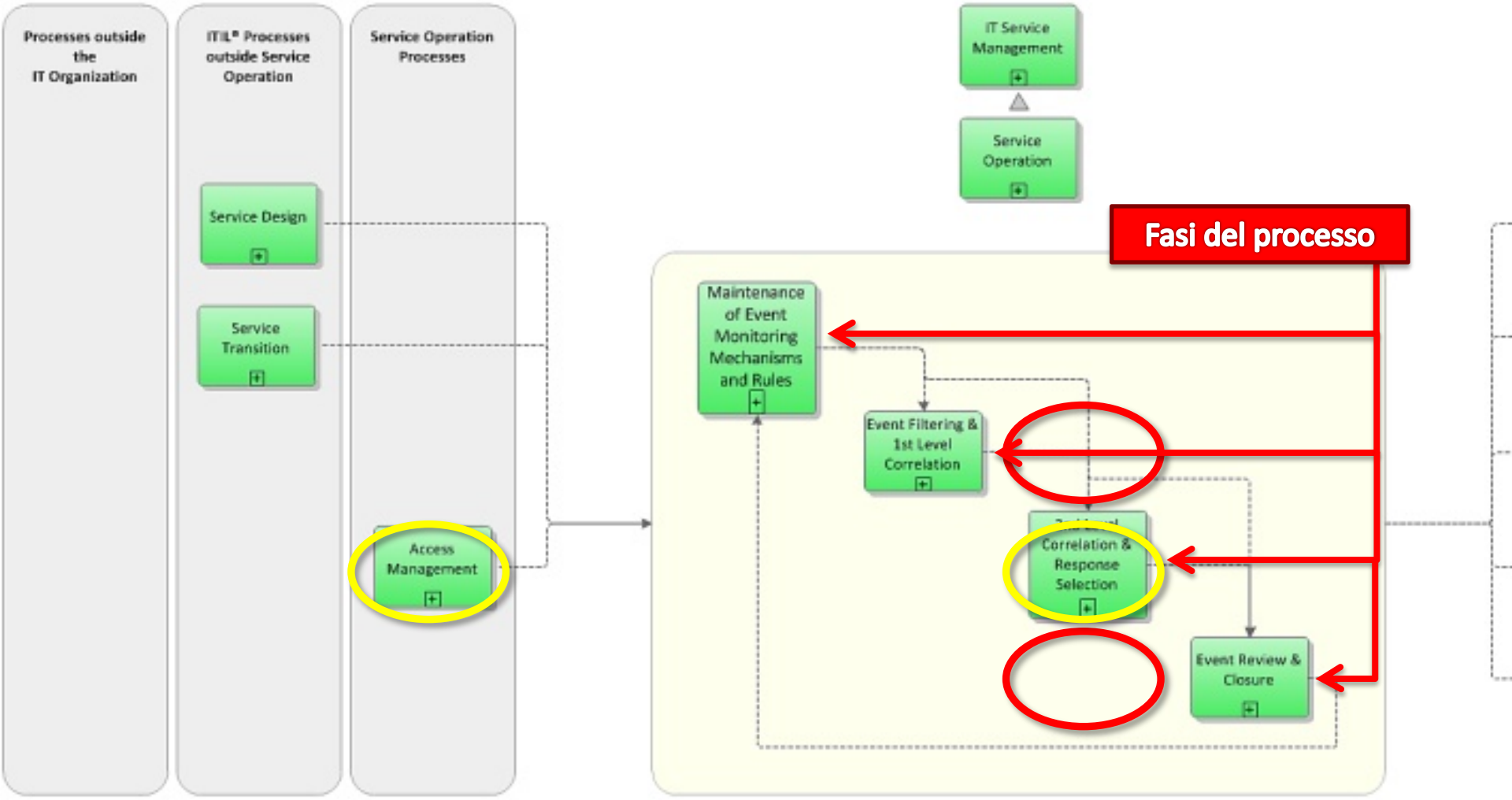
IL PROCESSO SECONDO ITIL V3

KPI:
% of Events turned into Incidents

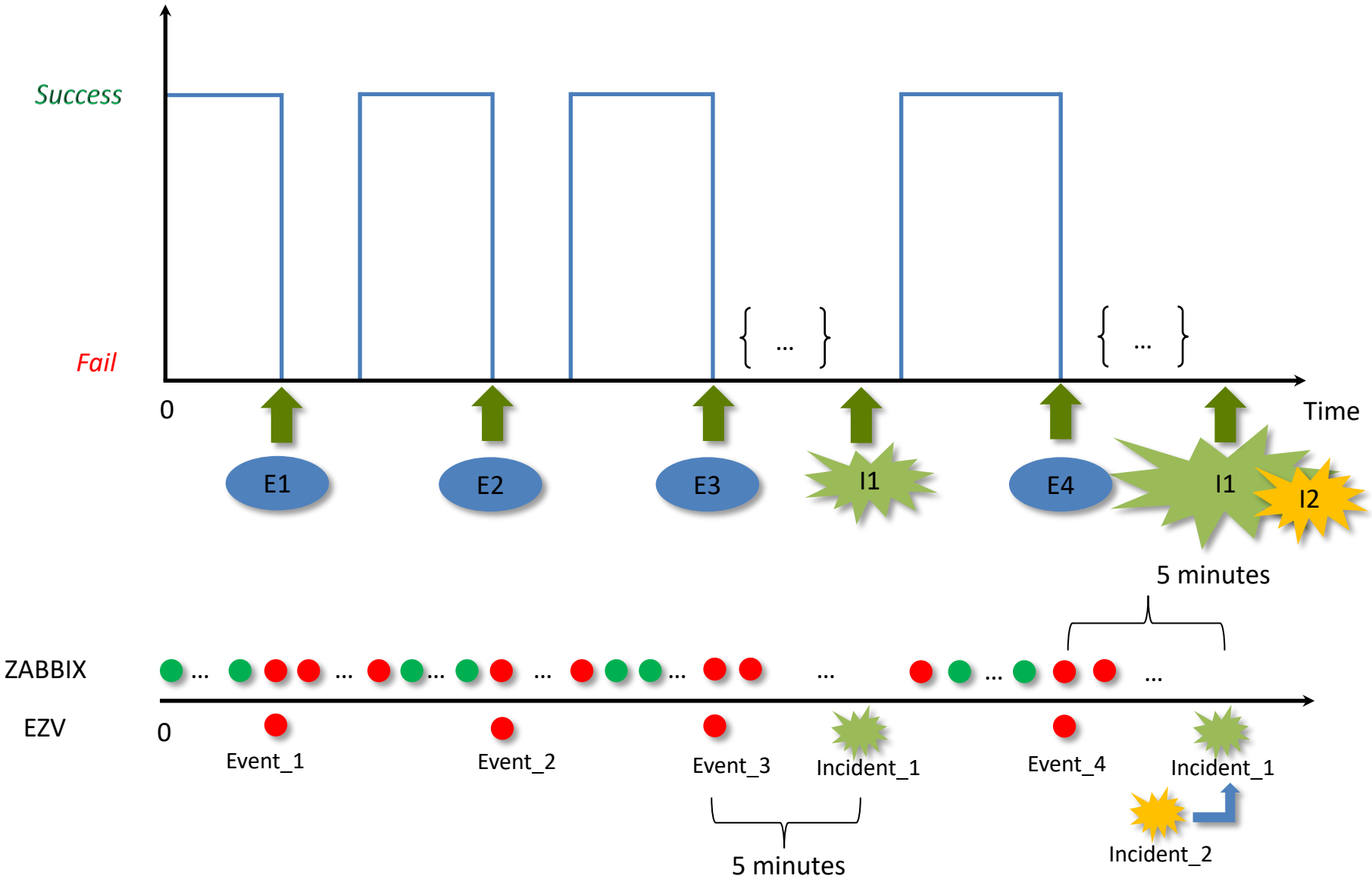
VFP:
Possible Incidents caught



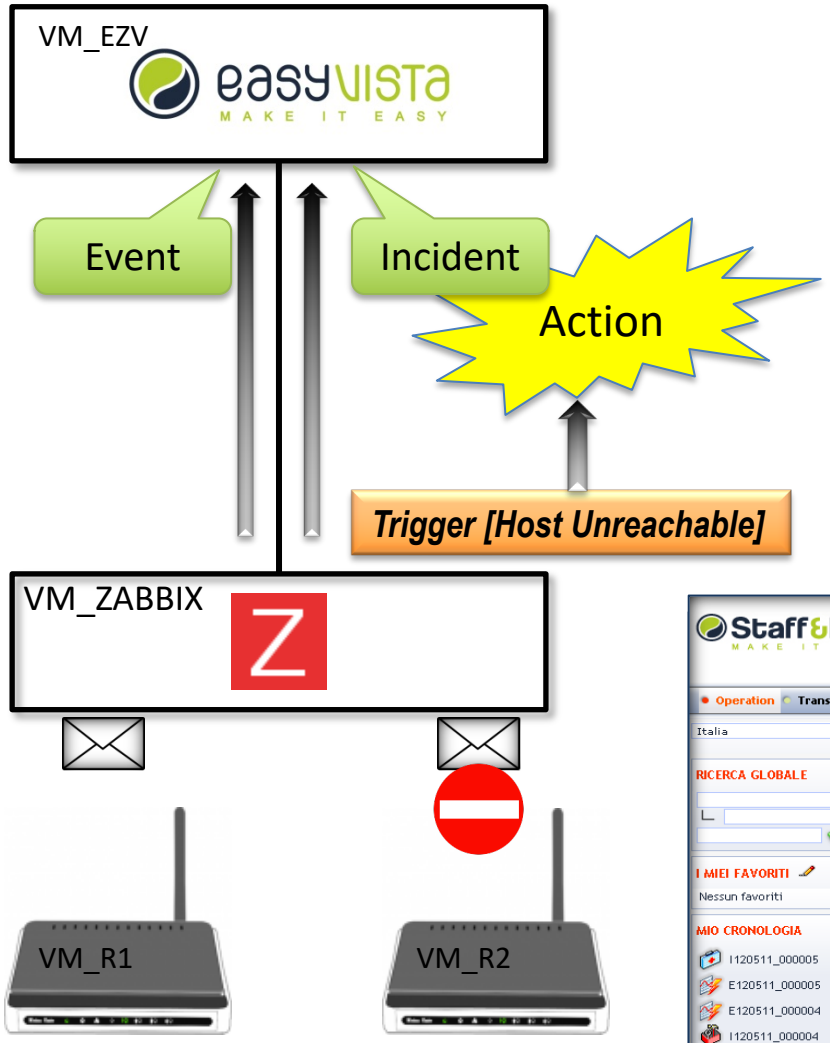
Il processo secondo ITIL v3



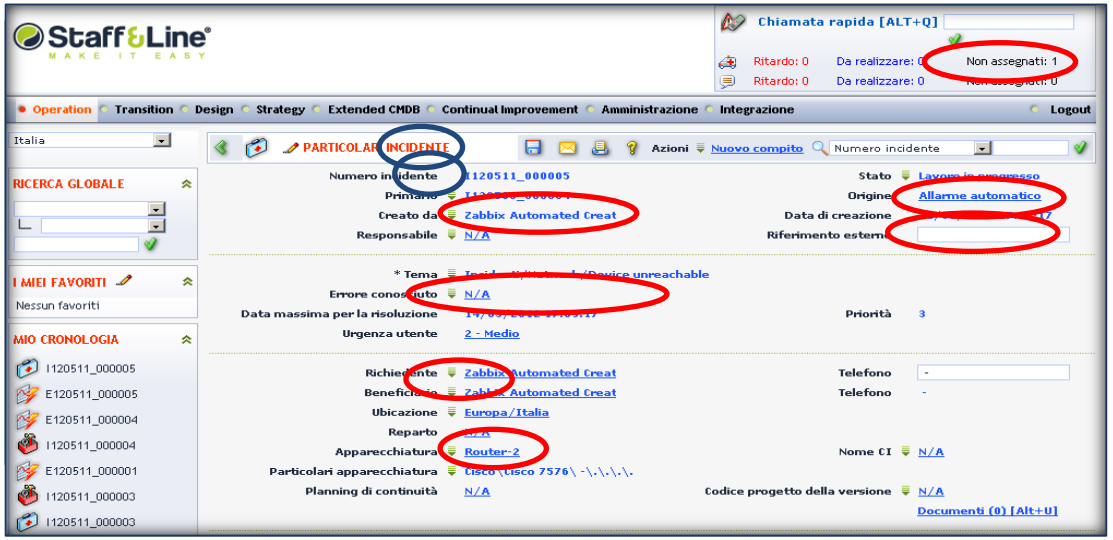
GESTIONE DEGLI EVENTI



ESEMPIO DI IMPLEMENTAZIONE



1. *Monitoring attivo*
2. Evento: spegnimento VM_R2
3. Zabbix rileva che il router VM_R2 non è più raggiungibile
4. Esecuzione azione associata al trigger
5. Creazione nuovo evento EasyVista
6. Generazione nuovo incidente EasyVista



CSF, Metriche e KPI

CSF Detecting all changes of state that have significance for the management of CIs and IT services

- **KPI** Number and ratio of events compared with the number of incidents
- **KPI** Number and percentage of each type of event per platform or application versus total number of platforms and applications underpinning live IT services (looking to identify IT services that may be at risk for lack of capability to detect their events)

CSF, Metriche e KPI

CSF Ensuring all events are communicated to the appropriate functions that need to be informed or take further control actions

- **KPI** Number and percentage of events that required human intervention and whether this was performed
- **KPI** Number of incidents that occurred and percentage of these that were triggered without a corresponding event

CSF, Metriche e KPI

CSF Providing the trigger, or entry point, for the execution of many service operation processes and operations management activities

- **KPI** Number and percentage of events that required human intervention and whether this was performed

CSF, Metriche e KPI

CSF Provide the means to compare actual operating performance and behavior against design standards and SLAs

- **KPI** Number and percentage of incidents that were resolved without impact to the business (indicates the overall effectiveness of the event management process and underpinning solutions)
- **KPI** Number and percentage of events that resulted in incidents or changes
- **KPI** Number and percentage of events caused by existing problems or known errors (this may result in a change to the priority of work on that problem or known error)
- **KPI** Number and percentage of events indicating performance issues (for example, growth in the number of times an application exceeded its transaction thresholds over the past six months)
- **KPI** Number and percentage of events indicating potential availability issues (e.g. failovers to alternative devices, or excessive workload swapping)

CSF, Metriche e KPI

CSF Providing a basis for service assurance, reporting and service improvement

- **KPI** Number and percentage of repeated or duplicated events (this will help in the tuning of the correlation engine to eliminate unnecessary event generation and can also be used to assist in the design of better event generation functionality in new services)
- **KPI** Number of events/alerts generated without actual degradation of service/ functionality (false positives – indication of the accuracy of the instrumentation parameters, important for CSI).

I Processi di Service Operation

Incident Management

IT Incident Management

Poiché l'IT Service Management è orientato all'erogazione di predeterminati livelli di servizio agli utenti finali, è importante creare un'organizzazione le cui direttive fondamentali siano:

- Monitorare l'ambiente IT in conformità con i suddetti livelli di servizio e scalare propriamente gli incidenti che si verificano nell'erogazione del servizio
- La funzione di IM ha la responsabilità di risolvere gli incidenti più in fretta possibile

Quando un utente incontra un incidente, il processo di IM farà sì che il servizio all'utente ritorni disponibile il prima possibile.

IT Incident Management: Obiettivi

I principali obiettivi sono:

- Risolvere gli incidenti del servizio prima possibile, o almeno entro il tempo stabilito nello SLA
- Mantenere un flusso costante di informazioni tra l'organizzazione IT e il suo cliente riguardo lo stato di un incidente (es. escalation, tempo stimato di risoluzione, etc.)
- Valutare un incidente per stabilire se è probabile che si ripresenti o se è sintomo di un problema cronico: in tal caso informare il PM a riguardo.

IT Incident Management: Obiettivi

Incident:	qualcosa che succede anche se non dovrebbe succedere (inaspettato)
Problem:	qualcosa di identificato (noto)

IT Incident Management: Responsabilità

- Individuazione e registrazione di un incidente
- Classificazione di tutti gli incidenti e supporto iniziale
- Investigazione e diagnosi
- Risoluzione e ripristino
- Chiusura di un incidente
- Incident control

IT INCIDENT MANAGEMENT: RESPONSABILITÀ

Individuazione e registrazione di un incidente:

- Il SD è responsabile della registrazione e del monitoraggio della risoluzione di tutti gli incidenti; questo è un processo estremamente reattivo.
- Per consentire una reazione efficiente ed efficace deve essere implementato un metodo di lavoro formale. Essi tracciano i dettagli di base dell'Incidente, allertano i gruppi di supporto specializzato nella misura necessaria e danno avvio alle procedure per gestire la richiesta di servizio.

IT INCIDENT MANAGEMENT: RESPONSABILITÀ

Classificazione di tutti gli incidenti e supporto iniziale:

- Questo è il processo di identificazione delle ragioni che hanno portato all'incidente e di conseguenza della relativa azione risolutiva.
- In questo caso il CMDB può essere consultato per controllare l'esistenza di known errors e problemi; una valutazione dell'impatto e dell'urgenza deve essere fatta per poter definire la priorità e deve essere fornito un supporto iniziale.
- Tipicamente il supporto iniziale consiste nel fornire un work around.

IT Incident Management: Responsabilità

Investigazione e diagnosi:

- Dopo una valutazione iniziale di un incidente, vengono raccolte e analizzate ulteriori informazioni.
- L'investigazione e l'individuazione possono diventare un processo iterativo, iniziando con vari gruppi di supporto specializzato e proseguendo con la definitiva eliminazione della possibile causa.
- Ciò può coinvolgere un supporto distribuito o anche vendor esterni.
- Questo richiede rigore e un approccio disciplinato oltre a una dettagliata attività di registrazione delle azioni intraprese e dei corrispettivi risultati.

IT INCIDENT MANAGEMENT: RESPONSABILITÀ

Risoluzione e ripristino:

- L'incidente è stato risolto o aggirato con successo oppure viene creata una RFC.

IT INCIDENT MANAGEMENT: RESPONSABILITÀ

Chiusura di un incidente:

- Questa può avvenire una volta che l'utente è soddisfatto riguardo la risoluzione o il workaround.
- Il Service Desk garantisce che:
  - I dettagli sulle azioni intraprese per risolvere l'incidente siano concisi e leggibili
  - La classificazione è completa e accurata in base alla causa di origine
  - La risoluzione è concordata con il cliente/utente
  - Tutti i dettagli applicabili a questo incidente vengono registrati

IT INCIDENT MANAGEMENT: RESPONSABILITÀ

Incident control:

- Ne parliamo successivamente, nella parte dove si descrive il Life Cycle dell'Incidente

IT INCIDENT MANAGEMENT: TERMINOLOGIA

Incidente:

- Ogni evento che non rientra nel servizio concordato è chiamato incidente.
- Interruzione del servizio o riduzione del servizio.
- E se l'incidente è in arrivo?

Workaround:

- E' un metodo per aggirare l'incidente o un problema con l'utilizzo di una fix temporanea.
- E' solitamente la prima soluzione di ripristino del servizio.
- Non è una soluzione definitiva, ma un espediente per mantenere il servizio "up and running"
- Solitamente riduce il servizio.

IT Incident Management: Terminologia

Service Request:

- Può essere pensato come un incidente che non è dovuto ad un malfunzionamento dell'infrastruttura IT.
- Può essere una richiesta di informazioni (es. l'utente non sa come si utilizza una certa funzionalità di un applicativo) o una change request (es. richiesta di cambio password) legata ad uno dei servizi che si stanno erogando.

Esempio di informazioni necessarie per la gestione degli Incidenti

- Unique reference number
- Incident categorization (often broken down into between two and four sub-categories)
- Incident urgency
- Incident impact
- Incident prioritization
- Date/time recorded
- Name/ID of the person and/or group recording the incident
- Method of notification (telephone, automatic, email, in person etc.)
- Name/department/phone/location of user
- Call-back method (telephone, mail etc.)
- Description of symptoms
- Incident status (active, waiting, closed etc.)
- Related CI
- Support group/person to which the incident is allocated
- Related problem/known error
- Activities undertaken to resolve the incident and when these took place
- Resolution date and time
- Closure category
- Closure date and time.

INCIDENT MANAGEMENT: CLASSIFICAZIONE

Classificare significa assegnare **Priorità** e **Categoria**

INCIDENT MANAGEMENT: PRIORITÀ

PRIORITA':

- Il SD determina la priorità degli incidenti non appena li riceve.
- La priorità viene stabilita in base ai criteri descritti nello SLA.
- La priorità si calcola in base all'impatto ed all'urgenza.

- **IMPATTO:** effetto che l'incidente ha sulle attività del business
- **URGENZA:** velocità con cui l'incidente deve essere risolto

INCIDENT MANAGEMENT: PRIORITÀ

L'impatto è sempre da intendersi come

Business Impact

- Critical period (i.e. night or day?)
- Critical applications
- Number of users
- Etc.

INCIDENT MANAGEMENT: PRIORITÀ

Nel determinare la priorità si deve considerare:

- I costi potenziali della non risoluzione
- La minaccia di danno per i clienti e per lo staff
- Le implicazioni legali
- Il “disturbo” arrecato ai clienti ed allo staff

- L’impatto non riguarda la complessità tecnica della risoluzione.

INCIDENT MANAGEMENT: PRIORITÀ

- Se si assegna subito la priorità della chiamata, il supporto di 2 livello può ottimizzare il suo funzionamento.
- La priorità non consiste solo nel mettere in code gli incidenti, riguarda anche le risorse che saranno allocate per la risoluzione (tempo, staff, esperienza, ricerca, etc.)
- In pratica, può capitare che un incidente a bassa priorità venga risolto oltre il tempo target in modo da permettere ad un altro a priorità maggiore di essere risolto entro il tempo prestabilito.

INCIDENT MANAGEMENT: PRIORITÀ

	Impact			
Urgency		High	Medium	Low
	High	1	2	3
	Medium	2	3	4
	Low	3	4	5

Priority code	Description	Target resolution time
1	Critical	1 hour
2	High	8 hours
3	Medium	24 hours
4	Low	48 hours
5	Planning	Planned

INCIDENT MANAGEMENT: PRIORITÀ

- Secondo lo SLA, **la priorità** corrisponde al tempo massimo di risoluzione
- Quanto tempo posso impiegare per la risoluzione del problema?
  - 1^ level: i.e. max 20 min
  - 2^ level: i.e. fino alla risoluzione etc.
  - 3^ level: …
- Non intestardirsi
- Knowledge Base …

INCIDENT MANAGEMENT: CATEGORIZZAZIONE

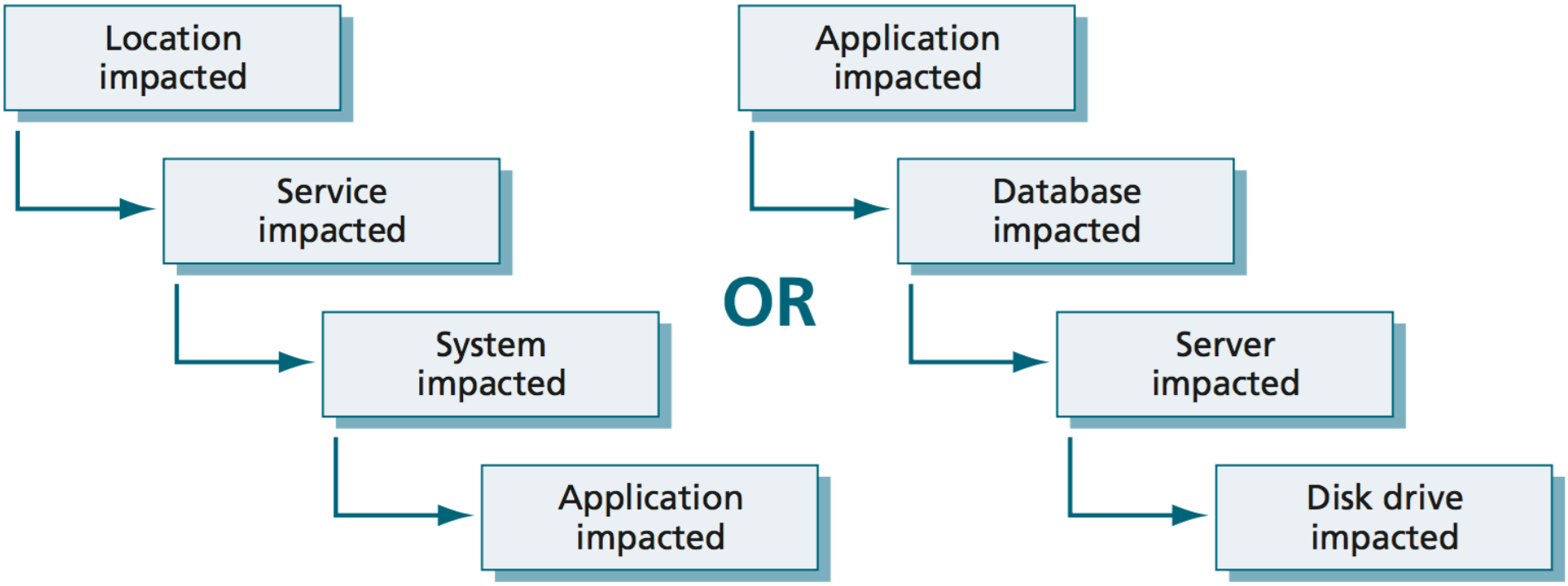
- Può fare muovere un primo passo verso la definizione
- E' necessario che IM e PM utilizzino un linguaggio comune per la categorizzazione
- Esistono 2 diversi tipi di categorie: in ingresso ed in uscita
- Differenza di linguaggio: registrare gli incidenti riportati (linguaggio dell'utente) – registrare le cause finali individuate (linguaggio tecnico)
- Se fatta bene può rivelare una tendenza (trend) e condurre all'identificazione di aree specifiche di problemi che necessitano di ulteriore investigazione

INCIDENT MANAGEMENT: CATEGORIZZAZIONE

Esempi di categorie:

- Application:
  - Servizio non disponibile
  - Bug di applicazione
- Hardware:
  - Un'alert automatico
  - Una stampante che non stampa
- Security Incident:
  - Virus

Multi-level Incident Categorization



Il processo di Incident Management

Input:

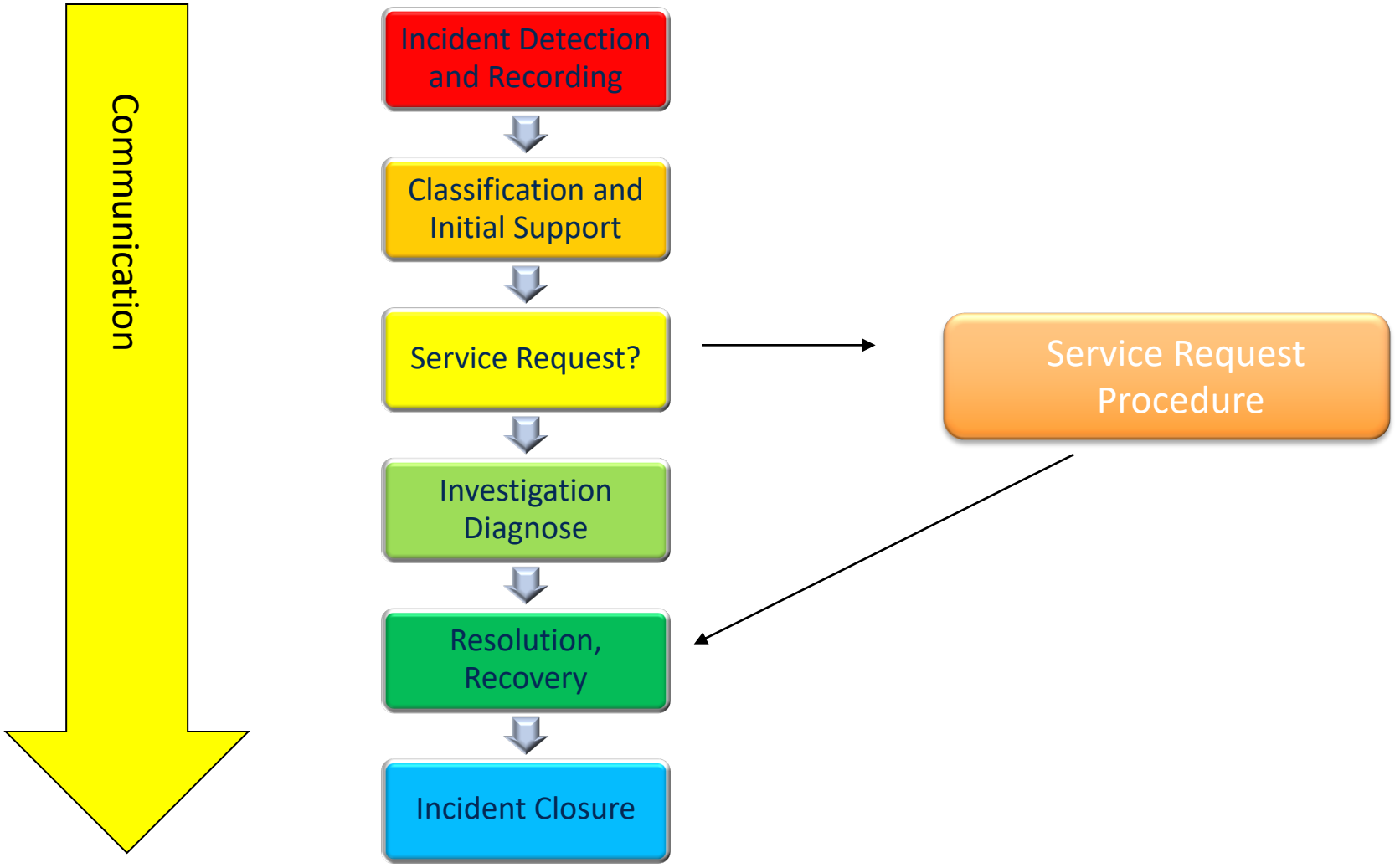
- Dettagli sull'incidente, forniti da più fonti
- Dettagli sulla Configurazione dal CMDB
- Esiti dei riscontri fatti fra incidente e problemi o known errors (Incident Matching)
- Dettagli sulla risoluzione
- Risposte a fronte di RFC

IL PROCESSO DI INCIDENT MANAGEMENT

Ouput:

- RFC per la risoluzione di un incidente; record sull'incidente aggiornato (inclusa soluzione e/o workaround)
- Incidenti risolti e chiusi
- Comunicazione ai clienti
- Informazione al management (reports)

Incident Life Cycle



INCIDENT LIFE CYCLE

Incident Detection and Recording:

- Tracciare l'incidente durante tutto il suo ciclo di vita
- Aggiungere utili informazioni che possono aiutare le organizzazioni di supporto a trovare una soluzione
- Registrare informazioni storiche per futuro utilizzo
- Raccogliere informazioni (es. per i reports)

Classification and Initial Support:

- L'SD determina la priorità degli incidenti appena li riceve
- Assegna una priorità in base all'impatto ed all'urgenza
- Viene assegnata una categoria alla chiamata (es. HW, SW) e l'operatore dell'SD procede con l'incident matching
- La consultazione del CMDB è necessaria per ottenere info riguardo il servizio che ha subito interruzione, i dati dell'SLA, i CIs legati al servizio, eventuali incidenti passati correlati, known errors e record di change

Service Request o Incident?:

- Se la chiamata è una SR l'operatore del SD segue una appropriata procedura di SR.
- Se è un incidente, dopo aver fornito un supporto iniziale, dovrà risolverlo o inoltrarlo al supporto di livello superiore per ulteriori investigazioni.

Investigation, Diagnose:

- Altri gruppi di supporto inizieranno ad analizzare l'incidente con l'unico scopo di trovare una soluzione permanente oppure, se ciò non fosse possibile, un workaround.

Resolution, Recovery:

- Dopo che la risoluzione od il workaround hanno avuto buon esito, può iniziare il ripristino del servizio, spesso svolto da uno staff specializzato (supporto di 2 e 3 livello).
- Il sistema di IM deve registrare eventi ed azioni intraprese durante la risoluzione ed il ripristino.

Incident Closure:

- Se viene trovate una soluzione permanente o un workaround, questi vengono implementati ed il servizio ripristinato. Il team che ha trovato la soluzione informerà l'SD che farà da intermediario con il cliente per verificare che la soluzione/workaround sia soddisfacente.
- In tal caso il SD potrà chiudere l'incidente.

INCIDENT LIFE CYCLE

- Nel corso di tutto il processo, l'IM ha la responsabilità di tracciare e monitorare i progressi e la qualità, oltre a fornire reports.
- Nella maggior parte dei casi il ruolo di Incident Manager sarà rivestito dal SD Manager.
- Il SD ha anche la responsabilità di tenere utente/cliente continuamente informati riguardo i progressi della chiamata.

ROUTING DEGLI INCIDENTI

- Il SD, in qualità di owner di tutti gli incidenti, deve coordinare il processo di Incident Management.
- Se vi sono discordanze di opinioni, il SD deve scalare il problema al PM.
- Da notare che il 2 e 3 livello di supporto possono comprendere anche fornitori esterni ai quali può essere dato accesso al tool di registrazione degli incidenti.

ESCALATION & REFERRAL

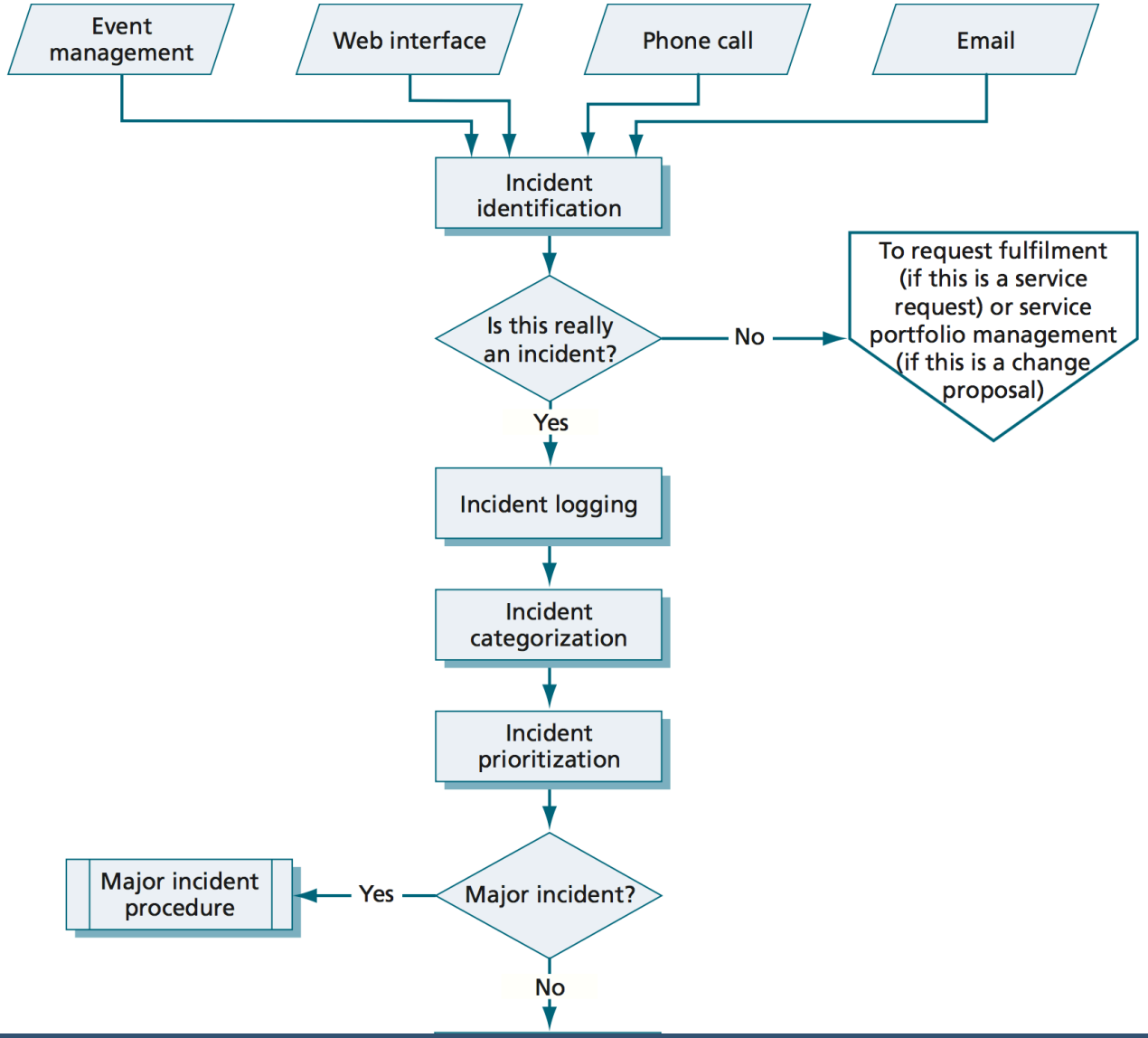
- L'incident routing è chiamato escalation orizzontale o referral ed ha luogo principalmente quando non ci sono la conoscenza o l'esperienza necessarie. Quando si fa un referral di un incidente, il SD deve fare attenzione a non superare i tempi di risoluzione indicati nello SLA.
- L'escalation gerarchica o verticale può verificarsi in ogni momento durante l'ILC. Di solito avviene quando vengono riportati incidenti di grossa entità o quando diventa evidente che non si potranno rispettare gli SLA di risoluzione. Questo permette all'autorità competente di intraprendere le dovute azioni correttive.

ESCALATION & REFERRAL

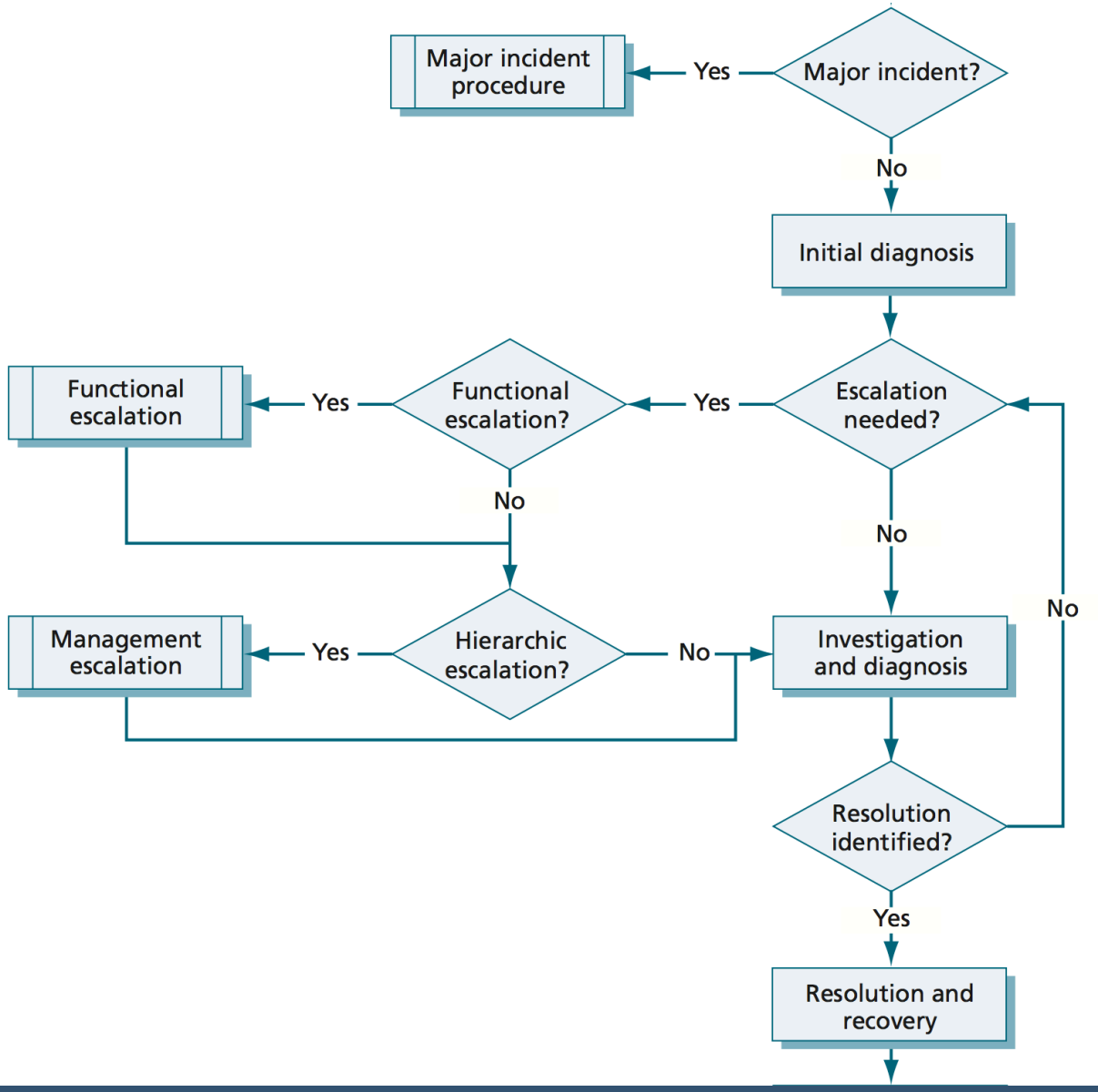
- **Hierarchical Escalation** = Inform / Support
- **Functional Escalation** = Knowledge

- L'Escalation ed il Referral non fanno MAI trasformare un incidente in un problema, anche quando l'ownership di un incidente parla al PM per ragioni amministrative, ed il PM dovesse procedere all'identificazione di un problema associato.
- I problemi NON sono incidenti seri.

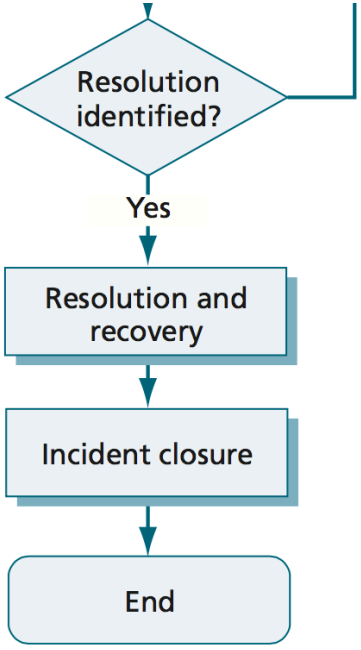
TIPICO WF PER IL PROCESSO DI IM



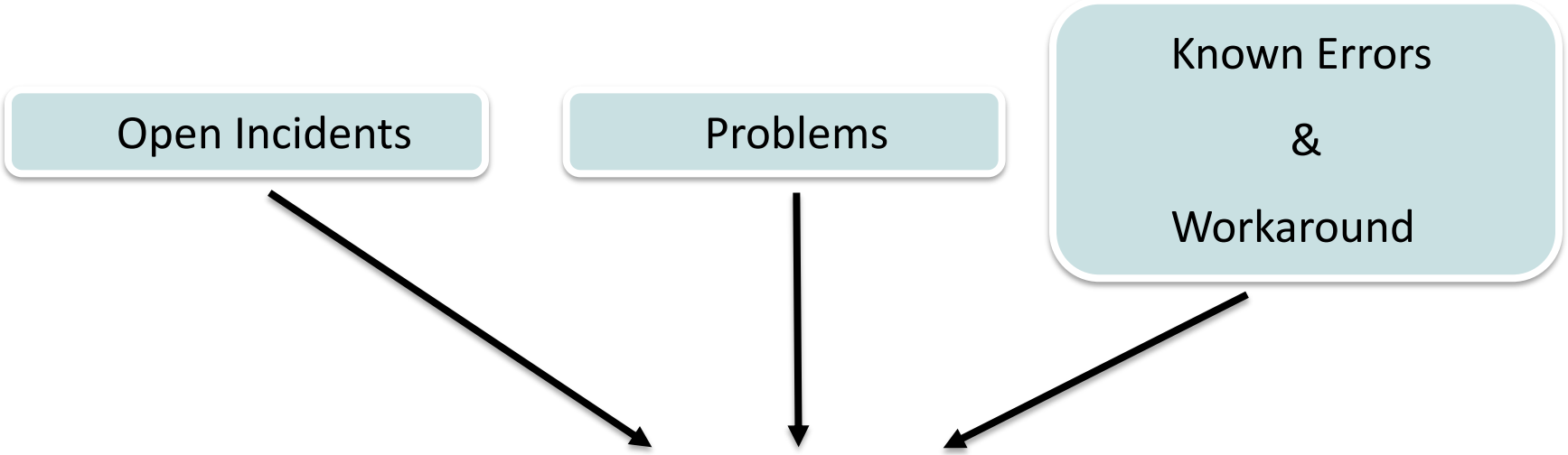
TIPICO WF PER IL PROCESSO DI IM



Tipico WF per il Processo di IM



INCIDENT MATCHING



Esistono già incidenti correlati a questo?

L'incidente è correlato ad un problema esistente?

Esiste un workaround?

INCIDENT MATCHING

Esempio di MATCHING:

- Un utente contatta il SD perché non gli funziona la posta elettronica
- Altri utenti chiamano con lo stesso problema
- Gli incidenti vanno messi in relazione
- Se l'incidente non trova un match allora è da considerarsi come un incident unico e deve essere registrato come tale.

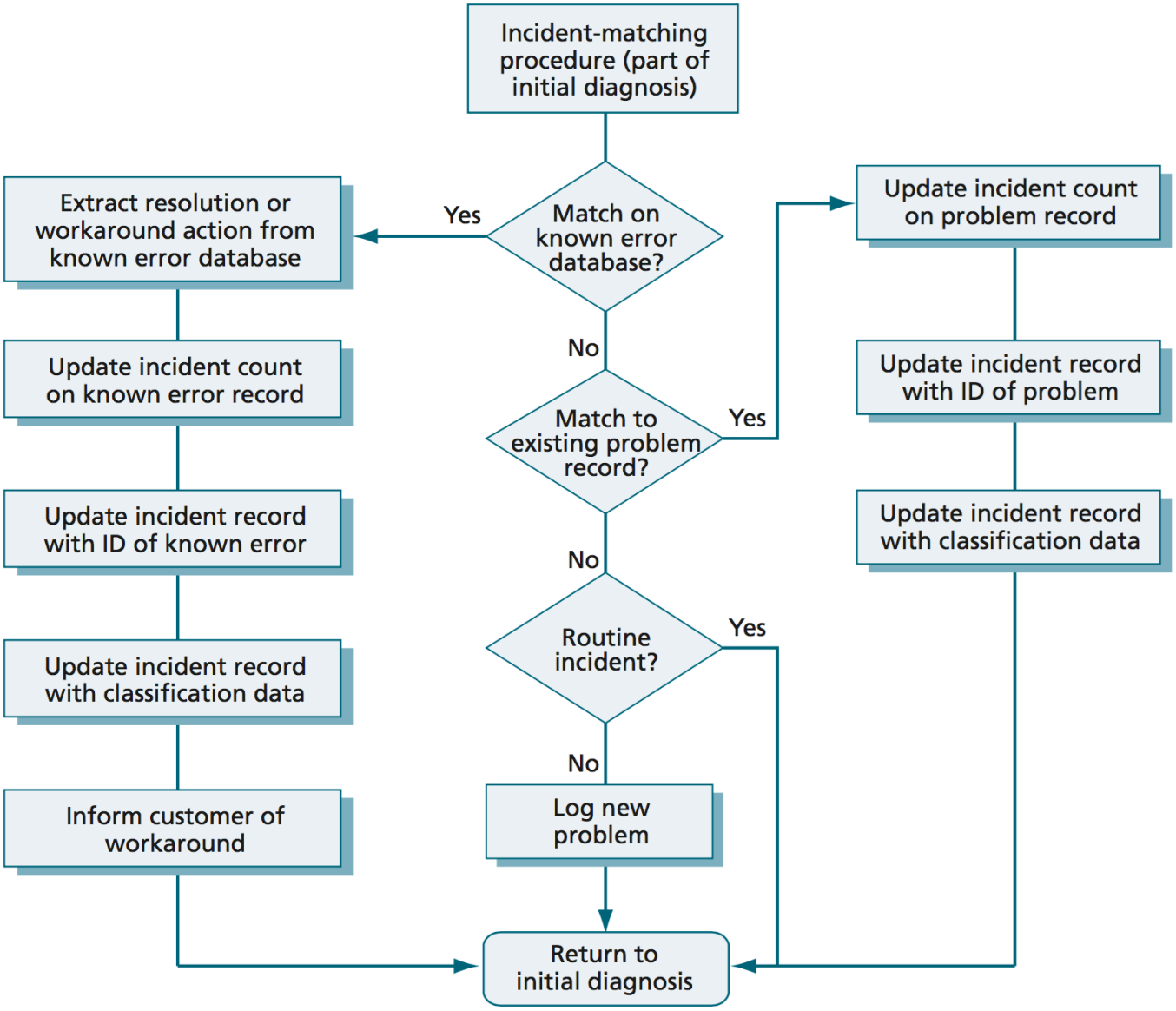
Incident Matching

Incident matching procedure

Many incidents are regularly experienced and the appropriate resolution actions are well known. However, it is necessary to have a procedure for matching incident classification data against that for problems and known errors. Successful matching gives efficient and quick access to proven resolution actions, reducing the time it takes to restore service back to users. The process of classification and matching allows incident management to be carried out more quickly and minimizes the need for escalation to other support staff.

Effective use of incident matching ensures that incidents are not redundantly being investigated for resolution over and over each time. A procedure can be developed to help service desk and other support staff match incidents to find resolutions quickly where possible. An example of an incident-matching procedure is shown in Figure 4.5.

Incident Matching



INCIDENT MANAGEMENT

Non è vero che gli incidenti vanno risolti “as quick as possible”, perché in ITIL dobbiamo fornire “STABLE SERVICES”, che significa “PREDICTABLE”.

Non interessa risolvere un incidente oggi in 3 minuti e domani in 3 giorni. Intesi in questo modo, gli SLA non avrebbero senso.

INCIDENT MANAGEMENT

A livello di Incident Management non possiamo alterare l'infrastruttura per risolvere i problemi: questo è, infatti, compito di altri processi con altre metodologie

Si possono risolvere i problemi senza modificare l'infrastruttura?

- Switch on – Switch off
- Problemi di conoscenza del prodotto
- Etc…

CSF, Metriche e KPI

CSF Resolve incidents as quickly as possible minimizing impacts to the business

- **KPI** Mean elapsed time to achieve incident resolution or circumvention, broken down by impact code
- **KPI** Breakdown of incidents at each stage (e.g. logged, work in progress, closed etc.)
- **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** Number and percentage of incidents resolved remotely, without the need for a visit
- **KPI** Number of incidents resolved without impact to the business (e.g. incident was raised by event management and resolved before it could impact the business)

CSF, Metriche e KPI

CSF Maintain quality of IT services

- **KPI** Total numbers of incidents (as a control measure)
- **KPI** Size of current incident backlog for each IT service
- **KPI** Number and percentage of major incidents for each IT service

CSF, Metriche e KPI

CSF Maintain user satisfaction with IT services

- **KPI** Average user/customer survey score (total and by question category)
- **KPI** Percentage of satisfaction surveys answered versus total number of satisfaction surveys sent

CSF, Metriche e KPI

CSF Increase visibility and communication of incidents to business and IT support staff

- **KPI** Average number of service desk calls or other contacts from business users for incidents already reported
- **KPI** Number of business user complaints or issues about the content and quality of incident communications

CSF, Metriche e KPI

CSF Align incident management activities and priorities with those of the business

- **KPI** Percentage of incidents handled within agreed response time (incident response- time targets may be specified in SLAs, for example, by impact and urgency codes)
- **KPI** Average cost per incident

CSF, Metriche e KPI

CSF Ensure that standardized methods and procedures are used for efficient and prompt response, analysis, documentation, ongoing management and reporting of incidents to maintain business confidence in IT capabilities

- **KPI** Number and percentage of incidents incorrectly assigned
- **KPI** Number and percentage of incidents incorrectly categorized
- **KPI** Number and percentage of incidents processed per service desk agent
- **KPI** Number and percentage of incidents related to changes and releases.