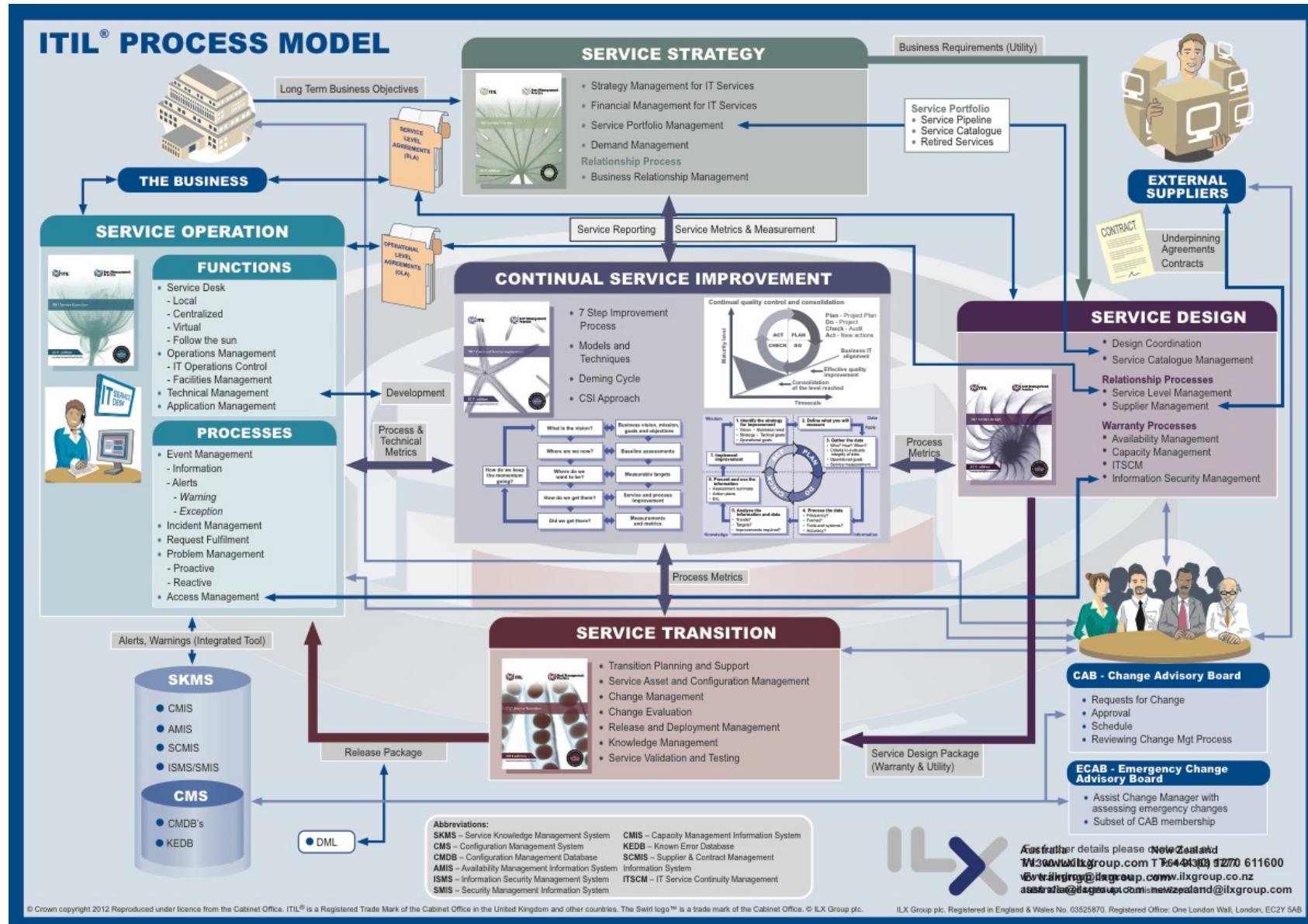


ITIL 2011 – ITIL Service Design

FRANCESCO CLABOT

ITIL: IL FRAMEWORK



ITIL CORE Books



Core ITIL lifecycle publication	Processes described in the publication
<i>ITIL Service Strategy</i>	Strategy management for IT services Service portfolio management Financial management for IT services Demand management Business relationship management
<i>ITIL Service Design</i>	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

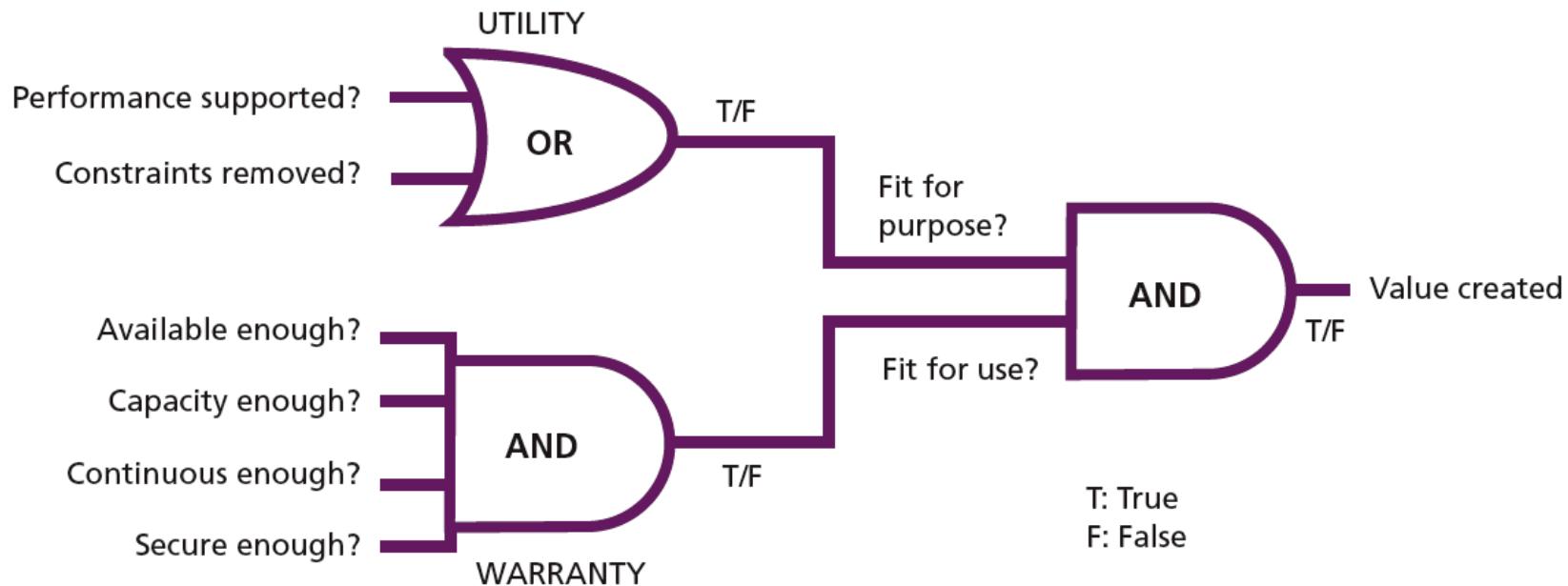
Seven-step improvement process

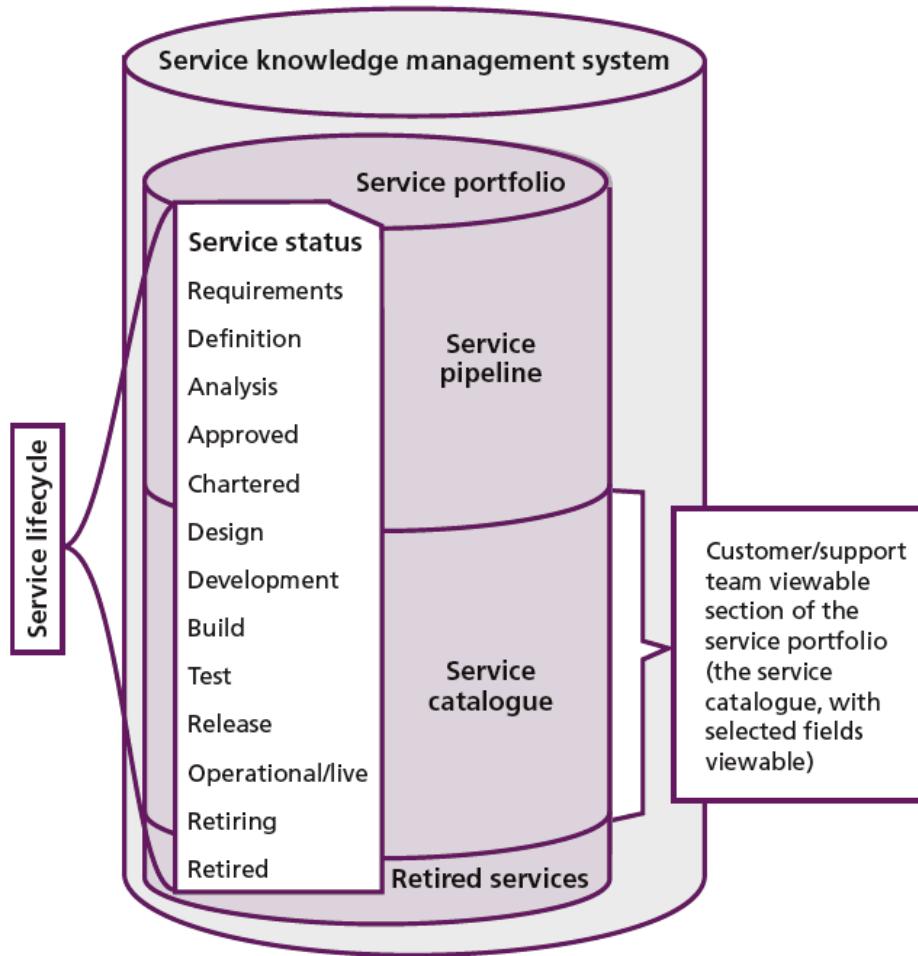
IT SERVICE DESIGN

PRINCIPI BASE

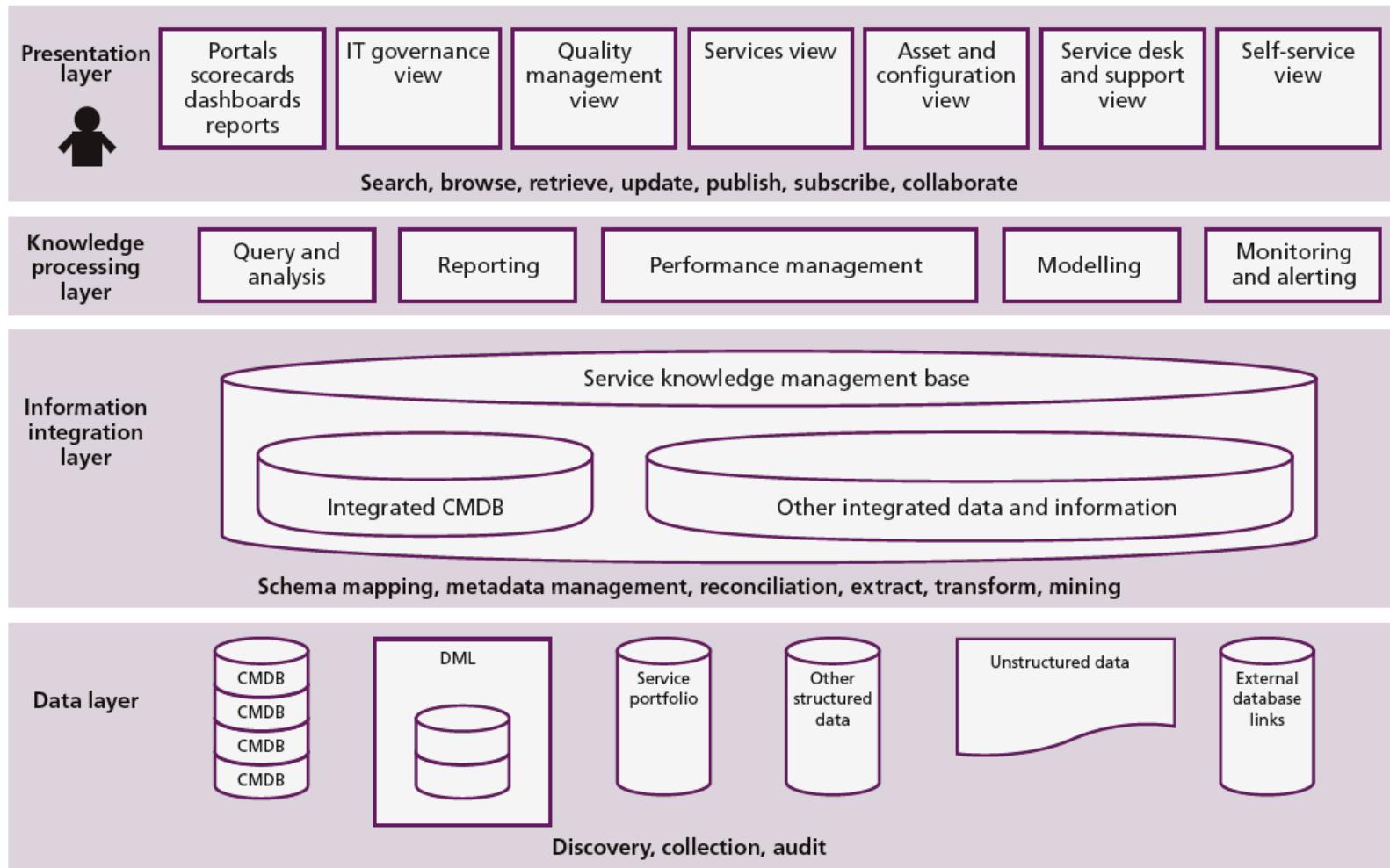


Value = Utility + Warranty





PRINCIPI BASE

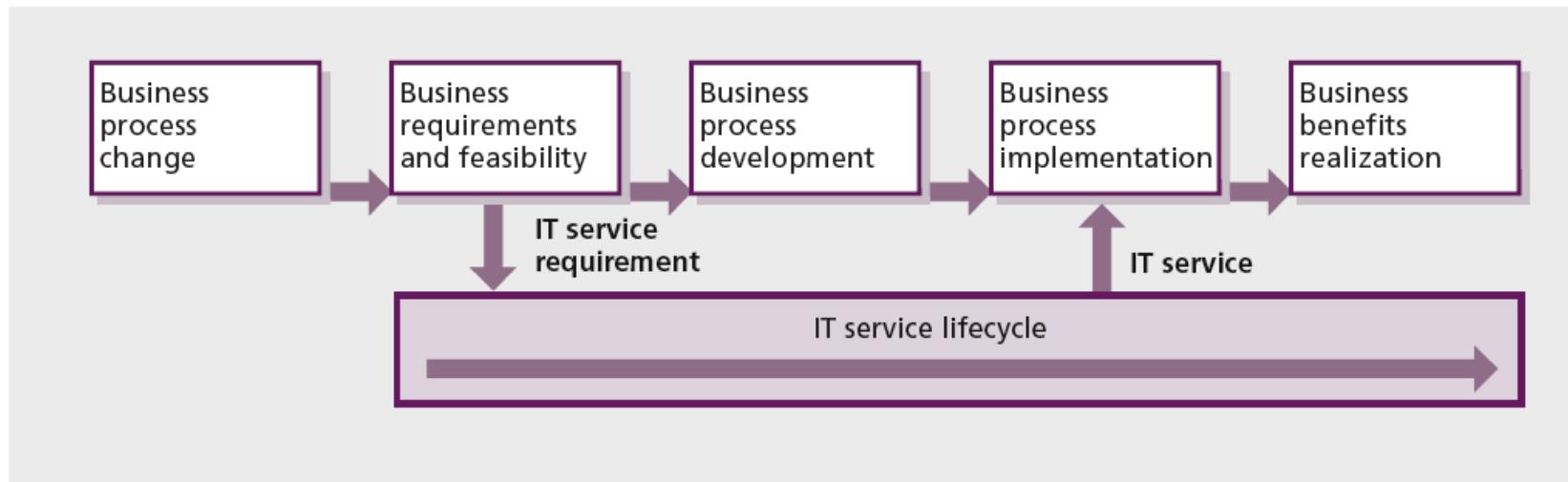


APPROCCIO OLISTICO AL SERVICE DESIGN

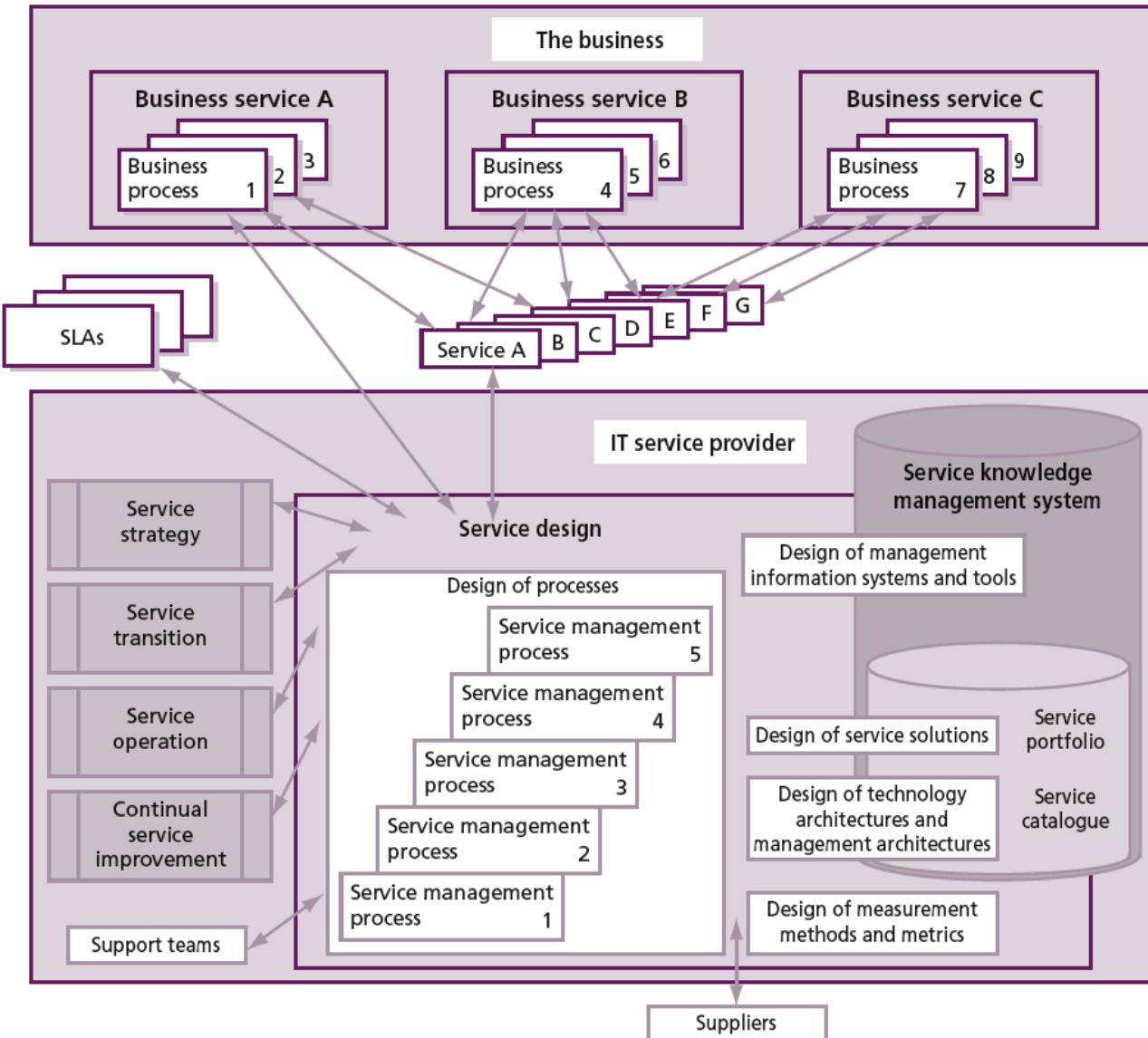


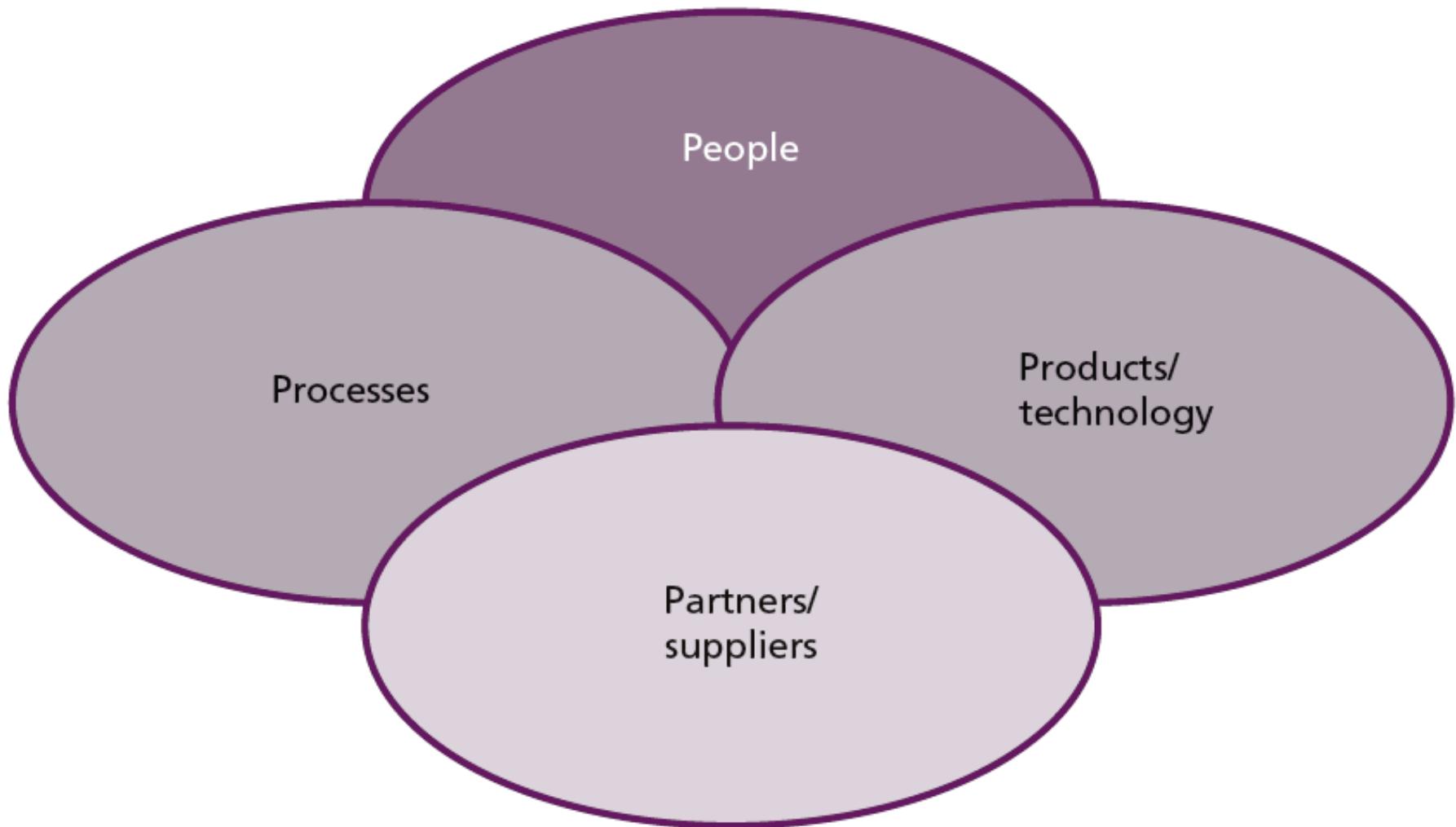
Ci sono 5 aspetti da tenere in conto quando si progetta un servizio:

- La soluzione per i servizi nuovi o modificati
- Le informazioni da gestire
- Le architetture tecnologiche e la gestione di queste
- Il processo richiesto
- I metodi di misura e le metriche

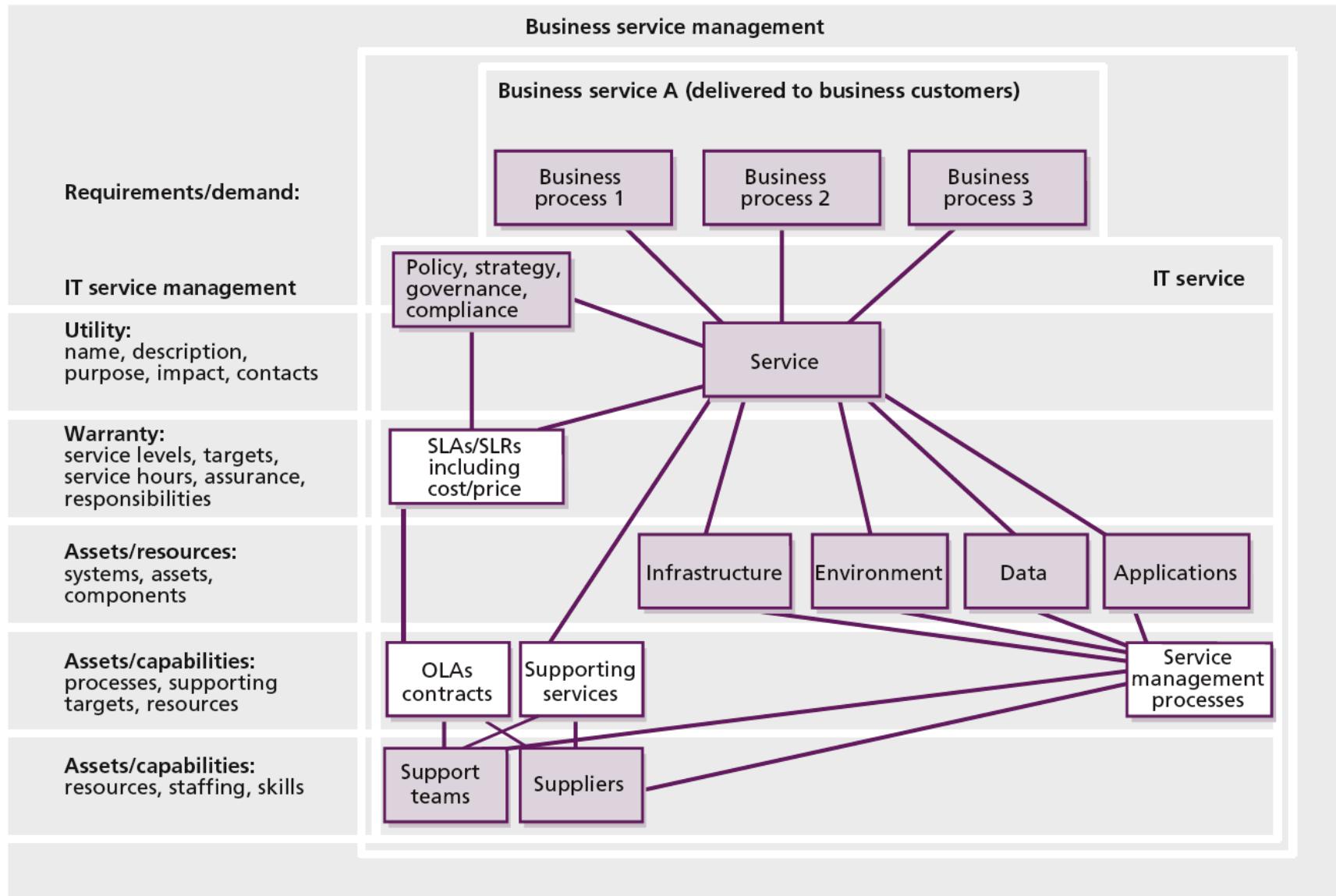


SCOPE DEL SERVICE DESIGN

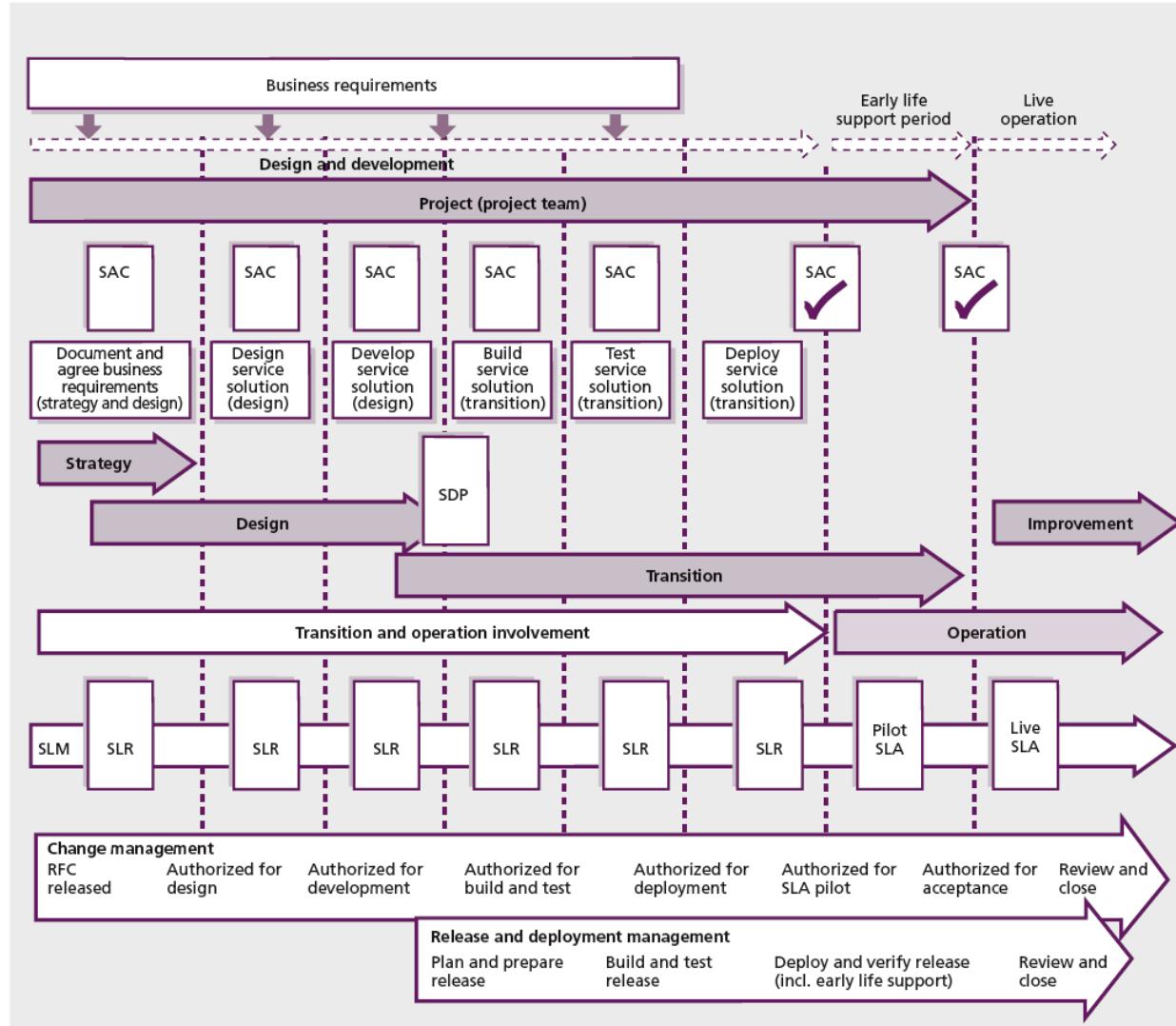




COME È COMPOSTO UN SERVIZIO



ALLINEAMENTO DEI NUOVI SERVIZI AI REQUISITI DI BUSINESS





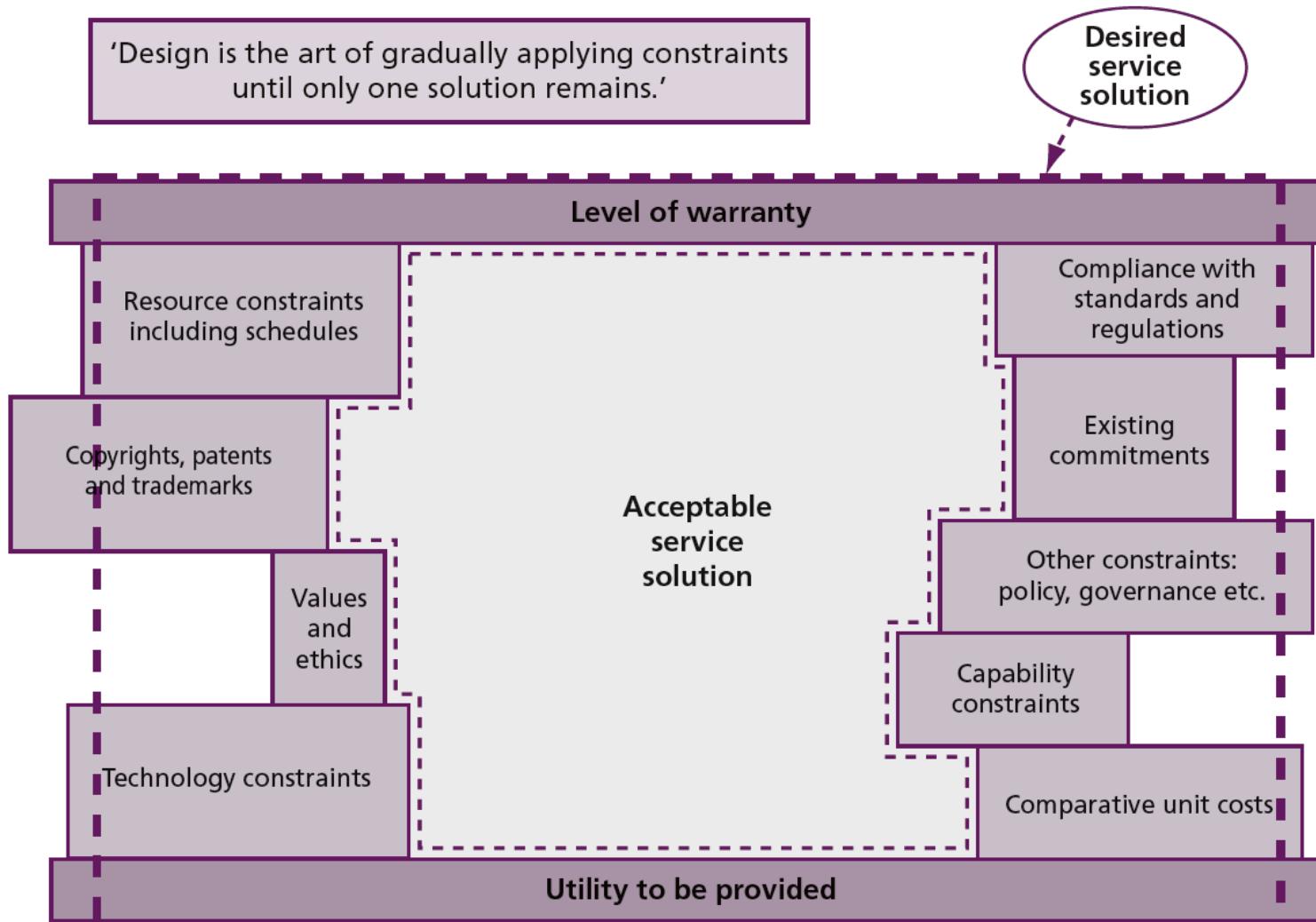
MATRICE RACI PER UN PROGETTO DI SVILUPPO DI UN SERVIZIO

	Director service management	Service level manager	Problem manager	Security manager	Procurement manager
Activity 1	A	R	I	I	C
Activity 2	A	R	C	C	C
Activity 3	I	A	R	I	C
Activity 4	I	A	R	I	
Activity 5	I	R	A	C	I

VINCOLI DI PROGETTO IMPOSTI DA STRATEGY



'Design is the art of gradually applying constraints until only one solution remains.'



THE SERVICE DESIGN PROCESSES



SERVICE DESIGN



- Design Coordination
- Service Catalogue Management

Relationship Processes

- Service Level Management
- Supplier Management

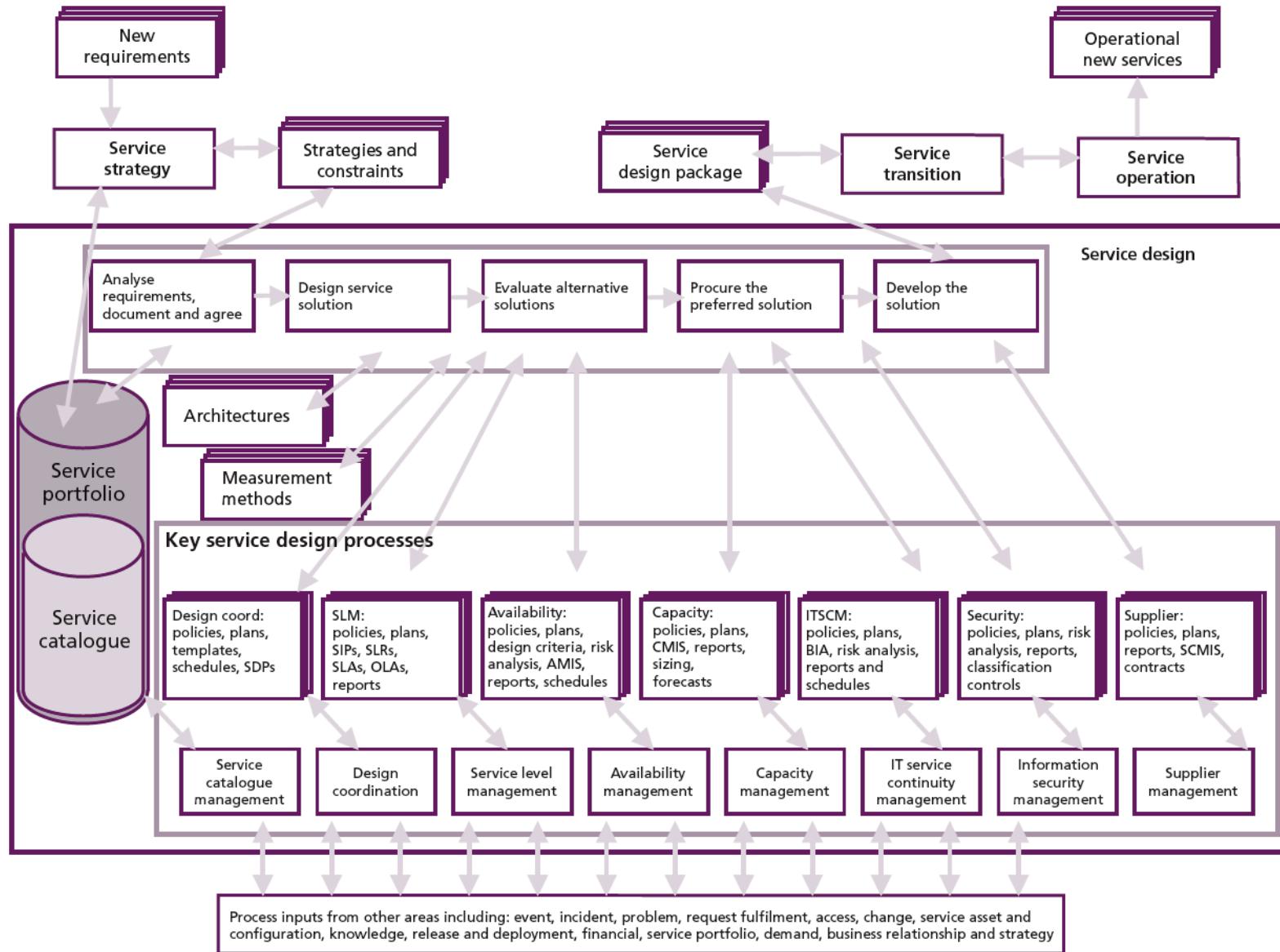
Warranty Processes

- Availability Management
- Capacity Management
- IT Service Continuity Management
- Information Security Management

IT SERVICE DESIGN

I PROCESSI

OVERVIEW SUL SERVICE DESIGN

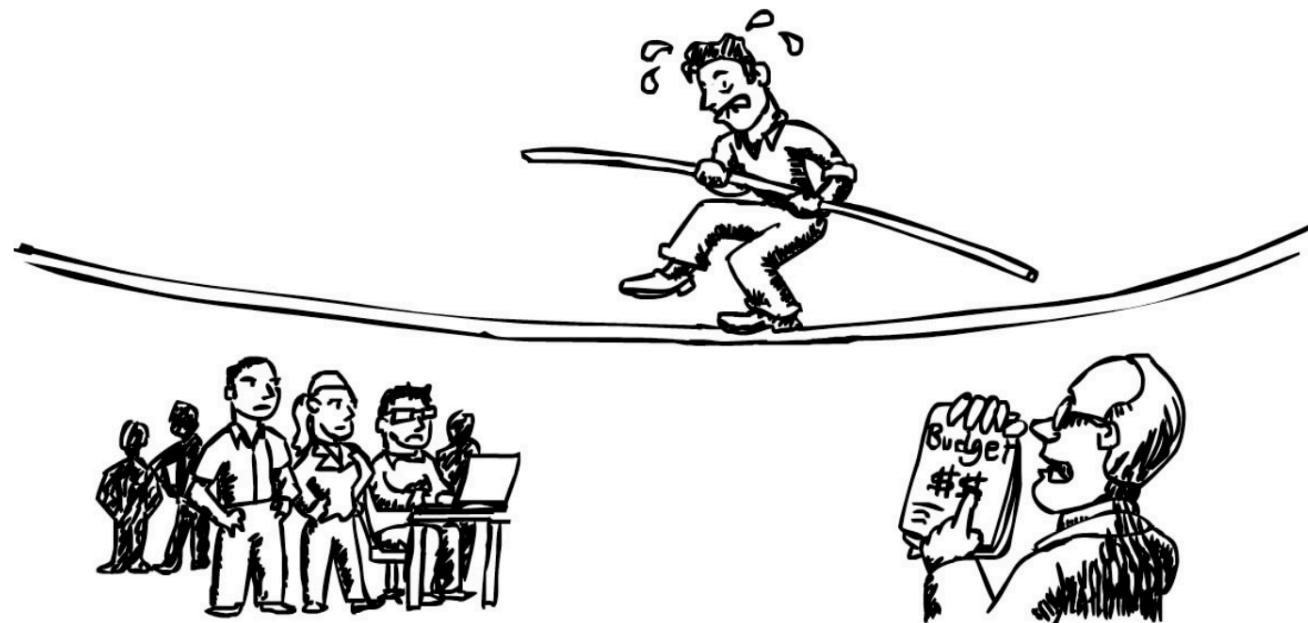


I PROCESSI DEL SERVICE DESIGN

CAPACITY MANAGEMENT



Lo scopo di questa disciplina consiste **nell'assicurare che esista sempre riserva di capacità dell'IT i cui costi siano giustificabili e che vada incontro alle esigenze del business.**





Determina la domanda del business (in termini di risorse IT), prevede i carichi di lavoro ed **effettua la schedulazione delle risorse IT.**

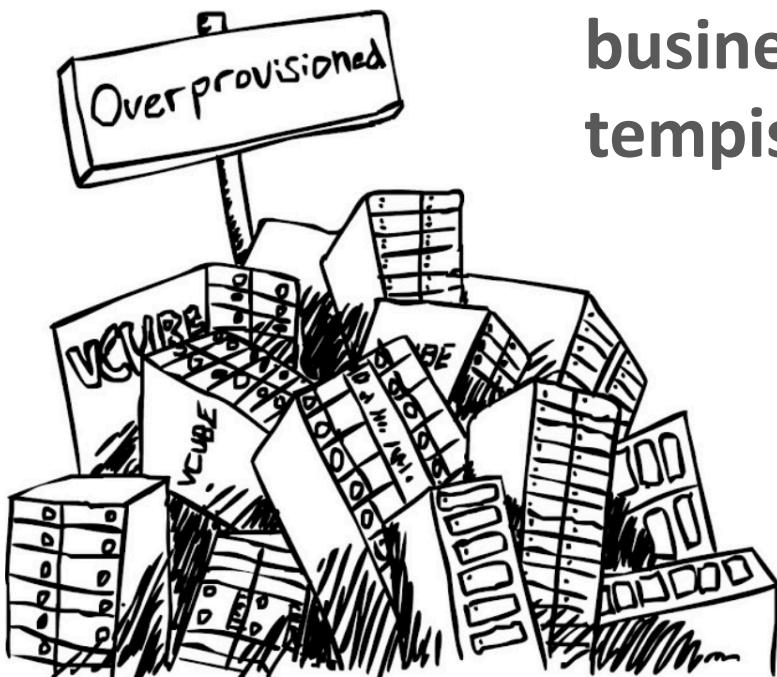


*Are you buying the right amount of infrastructure
at the right time?*

Uno dei maggiori contributi del processo consiste nel fornire un **Capacity Plan** ben documentato.



Il Capacity Management ha la responsabilità di garantire che la capacità di elaborazione e di memoria vadano incontro alla **domanda del business** nel modo **economicamente e tempisticamente più conveniente**



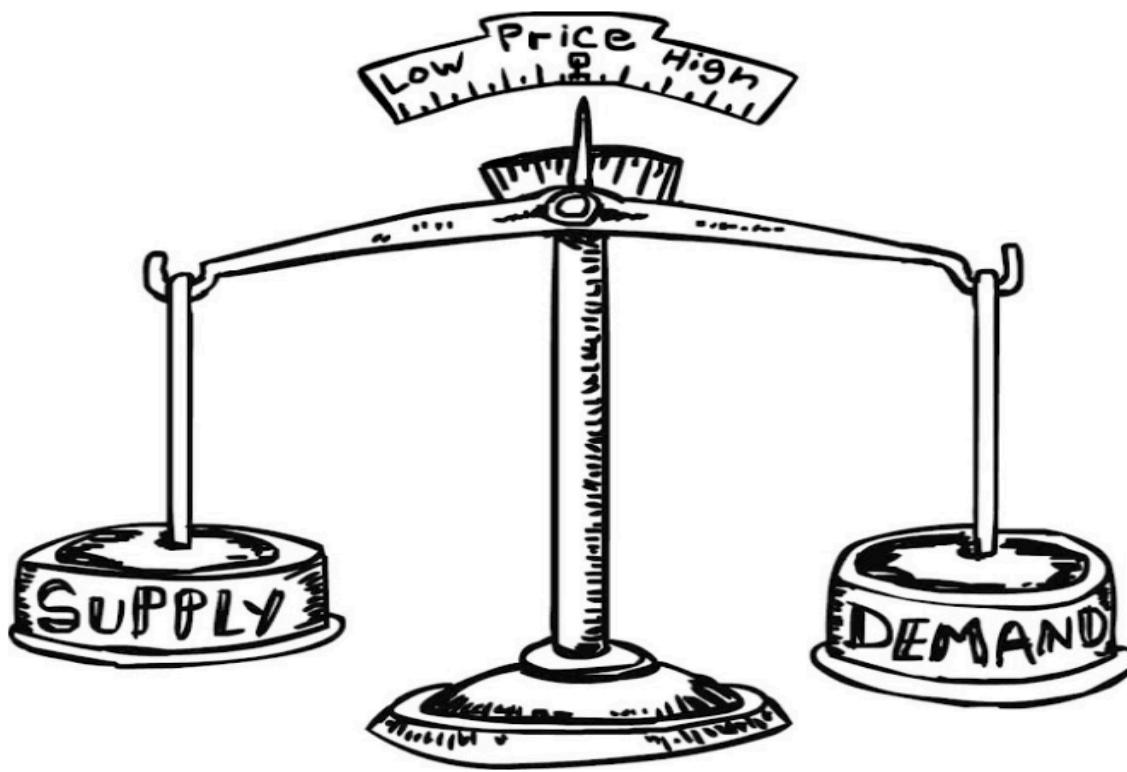


Il processo comprende:

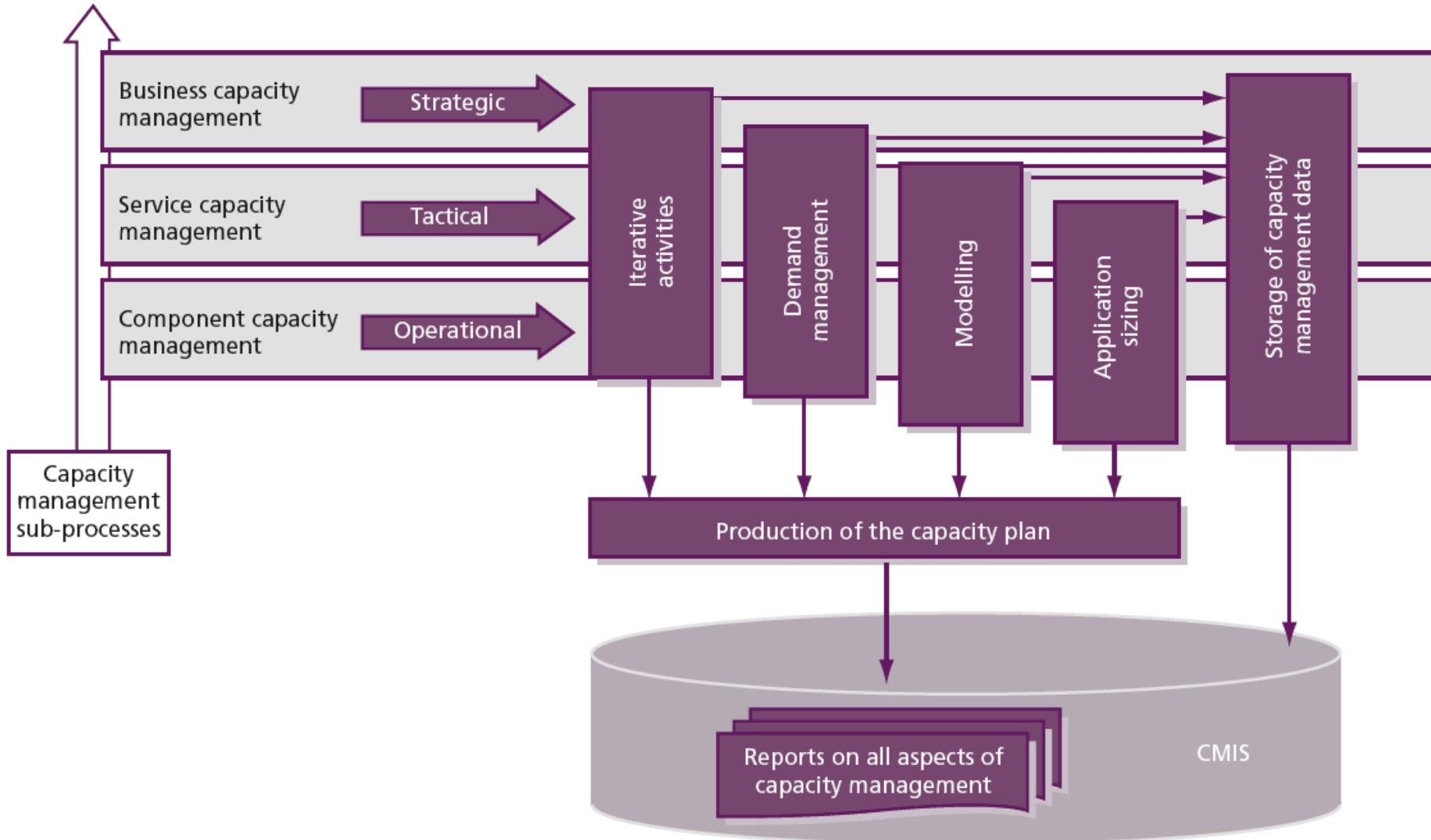
- Il **Monitoraggio delle performance** dei servizi IT e dei componenti infrastrutturali di supporto
- **Svolgere attività di tuning** per rendere l'uso delle risorse esistenti il più efficiente possibile
- Comprendere chiaramente ciò che viene correntemente richiesto alle risorse IT e **generare previsioni** per i requisiti futuri
- **Influenzare la domanda di risorse**, eventualmente con la collaborazione del Financial Management
- **Generare un Capacity Plan** che consenta al fornitore di servizi IT di offrire dei servizi coerenti con quanto concordato negli SLA



Capacity Management è essenzialmente una questione di bilanciamento



IT CAPACITY MANAGEMENT - RESPONSABILITÀ





Ciascuno dei sottoprocessi svolge numerose attività, ma ognuno di essi ha focus differenti

BUSINESS CAPACITY MANAGEMENT

è focalizzato sui requisiti del business attuali e futuri



SERVICE CAPACITY MANAGEMENT

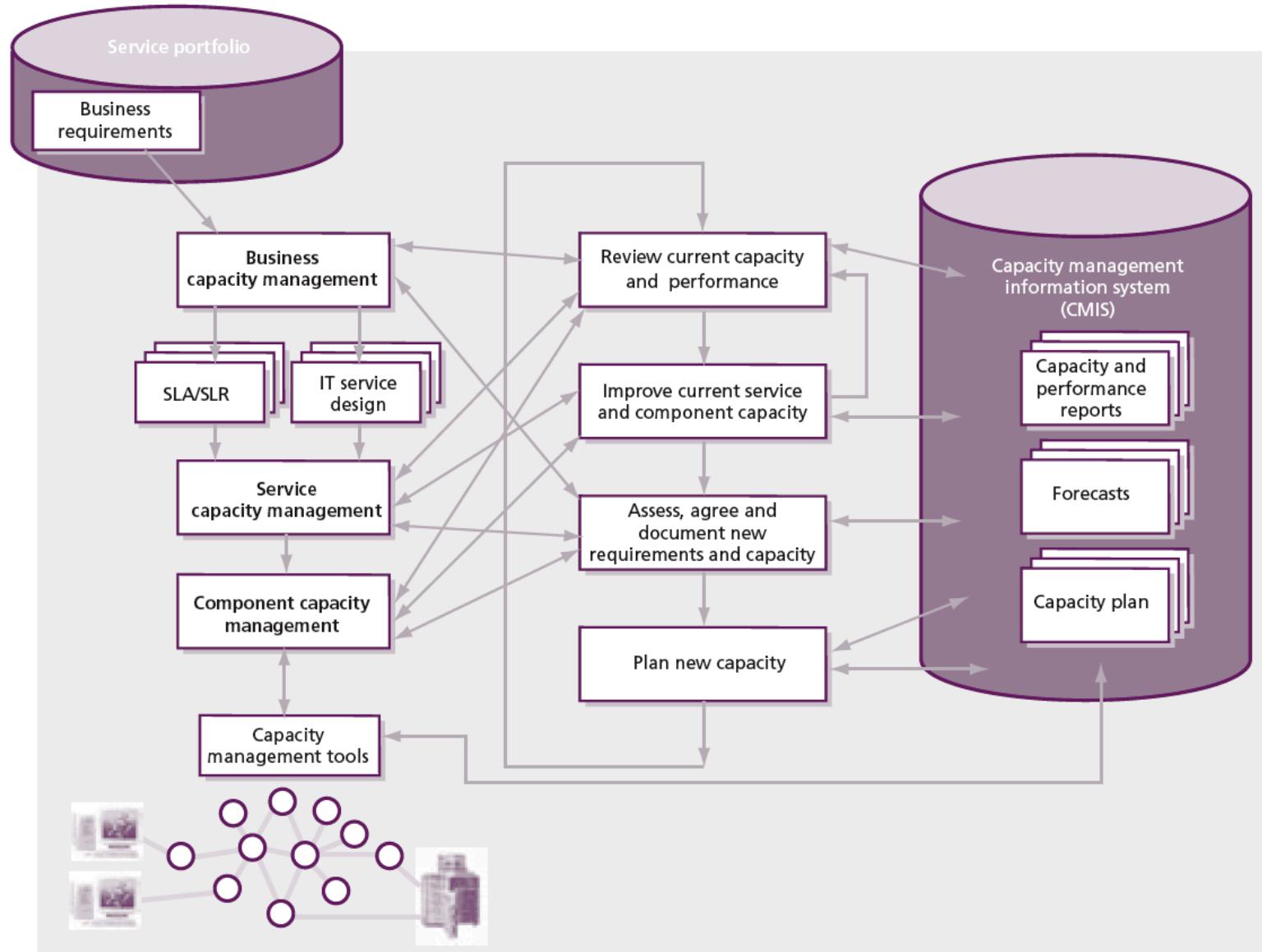
è focalizzato sull'erogazione dei servizi esistenti che supportano il business



COMPONENT CAPACITY MANAGEMENT

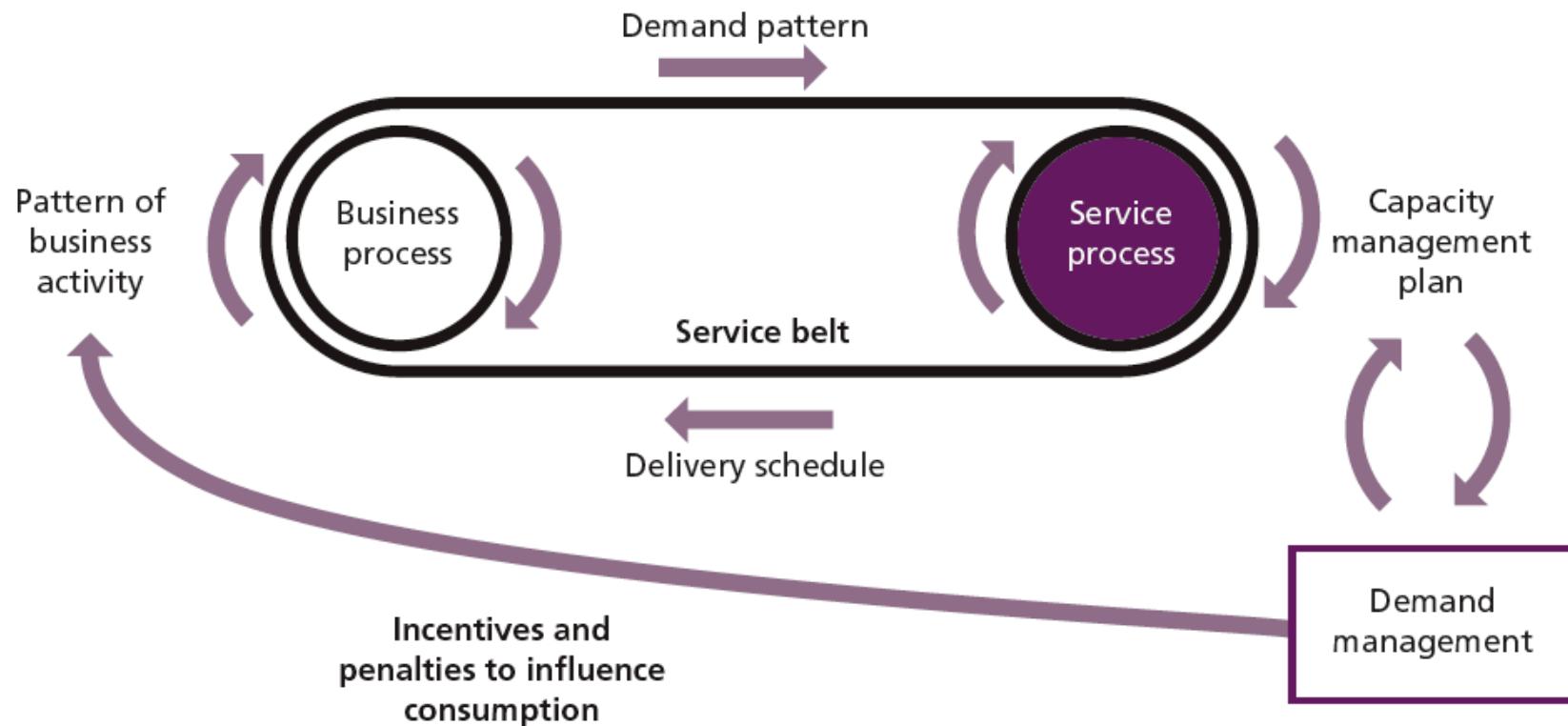
è focalizzato sulla tecnologia sottostante alla fornitura di tutti i servizi

IT CAPACITY MANAGEMENT - RESPONSABILITÀ



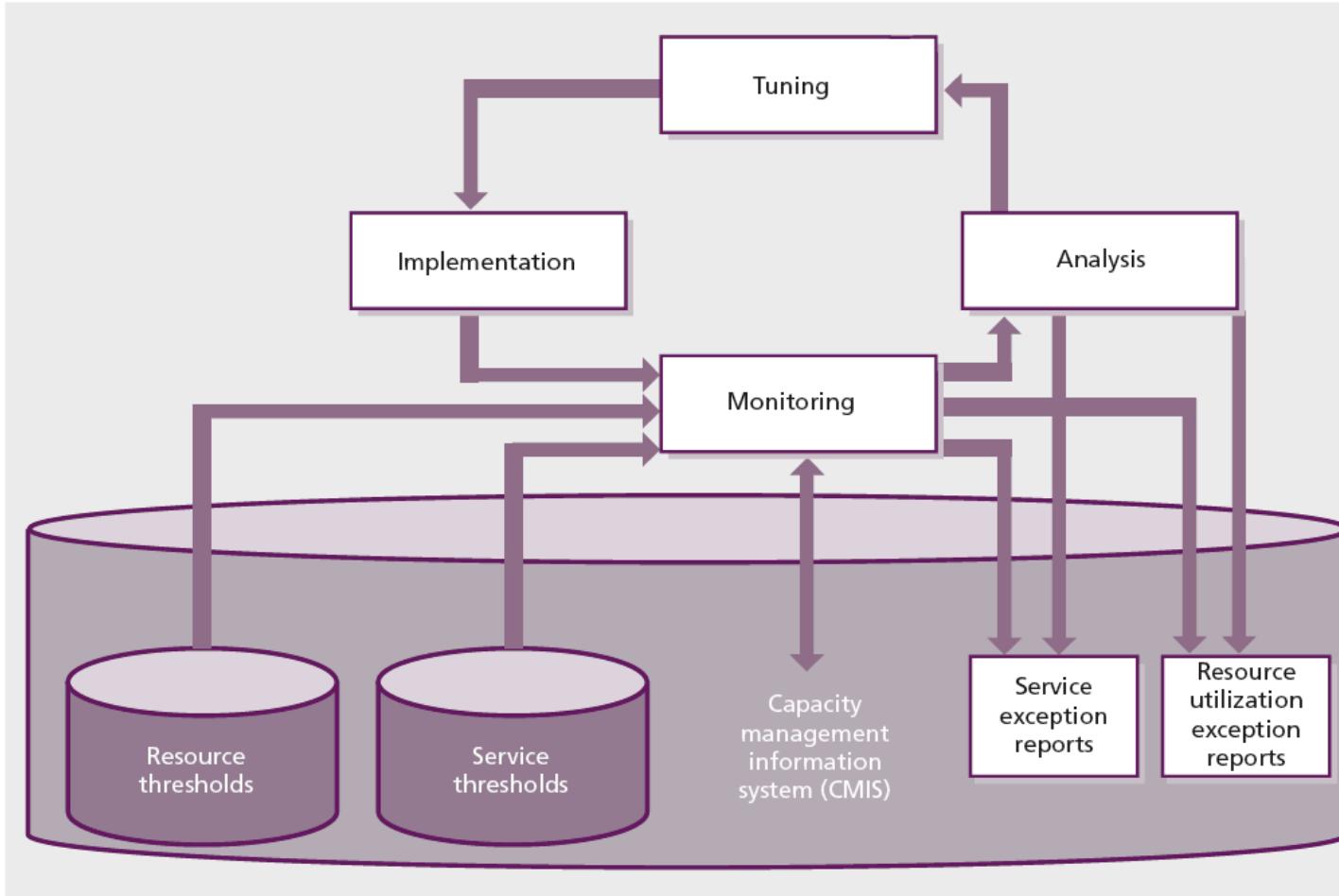


Il Capacity Management prende particolare rilievo nella gestione dei Demand Pattern





Componente iterativa del processo di Capacity Management





La componente iterativa del processo prevede attività che, senza soluzione di continuità, monitorino, analizzino ed, infine, ottimizzino le performance del sistema

Il ruolo di **Performance Manager**:

- Garantisce che le risorse tecniche dell'infrastruttura forniscano il miglior valore aggiunto in termini economici
- Ciò avviene monitorando, raccogliendo dati, svolgendo trend analysis e attività di tuning



- Il **Capacity Planning** garantisce una pianificazione appropriata
- Si basa sul **Capacity Management Information System (CMIS)** per la reportistica riguardante dati tecnici sui server e sulle reti, i dettagli del cliente e le previsioni, i dettagli del servizio e le previsioni, i volumi del business e i dati di finance
- Il Capacity Plan è anche il piano su cui viene analizzata la situazione corrente
- Le esigenze previste in base al cliente ed all'Availability Manager vengono dichiarate e la pianificazione su come giungere alla nuova situazione viene descritta, così come i costi previsti per le modifiche



E' l'attività necessaria alla comprensione dei requisiti di risorse necessarie per supportare l'implementazione di una nuova applicazione o un grosso cambiamento ad una applicazione esistente.

**Forecast Hardware
resources for new
applications**

**Provides cost
indicators for
Hardware and
additional resources**



- L'AS ha un ciclo di vita finito
- Inizia quando si è nella fase di Project Initiation per una nuova applicazione o quando sta per essere fatto un Major Change ad una applicazione esistente, e si conclude quando l'applicazione viene portata in ambiente live
- L'obiettivo primario è quello di stimare le risorse necessarie per supportare la modifica ad una applicazione o una nuova applicazione
- Ciò viene fatto per garantire che vada incontro ai livelli di servizio richiesti
- Per raggiungere tale fine, l'AS deve essere parte integrante del ciclo di vita delle applicazioni



- Un primo obiettivo del Cap. M è quello di predire il comportamento del sistema informatico quando è sottoposto ad un certo volume e varietà di lavoro
- Il **modeling** è un attività che può essere usata a beneficio di qualunque dei sotto-processi del Cap.M
- I vari tipi di **modeling** spaziano dal fare stime basate sull'esperienza e informazioni sull'uso corrente delle risorse, a studi pilota, prototipi e benchmarks ad ampio raggio
- Il primo tipo è economico ed è un approccio ragionevole per piccole decisioni quotidiane, mentre l'ultimo è costoso ma consigliabile quando si implementa un nuovo ed ampio progetto



Alcune tecniche di modeling sono:

Trend Analysis

- Possono essere fatte in base all'utilizzo delle risorse e alle informazioni relative alle performance del servizio che sono state raccolte dai sotto-processi di Service e Resource Capacity Management
- Si può fare in varie forme, per esempio valutando l'utilizzo di una particolare risorsa in un intervallo di tempo passato a stimare quanto tale utilizzo potrebbe cambiare in futuro



Analytical Modeling

- E' una rappresentazione del comportamento del sistema informatico tramite l'impiego di tecniche matematiche, i.e. la teoria del "multi-class networking queuing"
- Tipicamente un modello viene generato usando un pacchetto SW su un PC, specificando nel package i componenti e le strutture della configurazione che deve essere modellata, e l'utilizzo di tali componenti, i.e. CPU, memoria e dischi, da parte delle varie applicazioni o delle attività che vengono svolte
- Quando il modello ha girato, viene usata la teoria delle code per calcolare i tempi di risposta del sistema informatico
- Se i tempi di risposta previsti dal modello sono sufficientemente vicini ai tempi riscontrati nella realtà, il modello può essere ritenuto un'accurata rappresentazione del sistema informatico



Simulation Modeling:

- Coinvolge la modellazione di eventi discreti, i.e. tempi di risposta delle transazioni, relativamente ad una certa configurazione hardware
- Questo tipo di modeling può essere molto accurato per fare il “sizing” di nuova applicazioni o per predire gli effetti che potrebbero avere dei changes sulle applicazioni esistenti, ma può anche essere molto impegnativo in termini di tempo e di conseguenza costoso
- Comunque i suoi costi possono essere giustificati in organizzazioni con sistemi particolarmente grossi dove i costi (milioni di Euro) e le relative implicazioni delle performance assumono grossa importanza



Baseline Modeling

- E' quando viene creato un modello che riflette accuratamente il livello di performance raggiunte
- Una volta che questo modello viene creato, si può fare il predictive modeling i.e. chiedendosi "cosa succederebbe se...?"



- Il primo obiettivo è quello di produrre un piano che documenti gli attuali livelli di utilizzo delle risorse e le performance del servizio e, dopo attente considerazioni sulla strategia e i piani del business, prevedere i futuri requisiti richiesti alle risorse per supportare i servizi IT che supportano le attività del business
- Il piano deve indicare chiaramente ogni assunzione fatta
- Deve inoltre includere ogni raccomandazione in termini di risorse necessarie, costi, benefici, impatto, etc.

I PROCESSI DEL SERVICE DESIGN

AVAILABILITY MANAGEMENT



E' la disciplina che consente all'IT Manager di ottimizzare l'utilizzo delle risorse, anticipare e calcolare anomalie imminenti, implementare policy di sicurezza e monitorare i livelli di servizio concordati.

Availability Management

Security

Serviceability

Recoverability

Maintainability

Resilience



- Ottimizzare la capacità dell'infrastruttura IT e dell'organizzazione di sviluppo di fornire un livello di disponibilità elevato ed economicamente conveniente, che permetta al business di soddisfare i suoi obiettivi
- Ciò avviene determinando i requisiti di disponibilità del business e facendo un match fra essi e la capacità dell'infrastruttura IT e dell'organizzazione di supporto
- Quando non c'è il match, l'AM garantisce che il business avrà a disposizione delle alternative con relative opzioni di costo associate
- L'AM deve garantire che il livello di disponibilità richiesto sia fornito



- La misurazione e il monitoraggio della disponibilità IT è una attività chiave per garantire livelli di disponibilità consistenti
- L'AM deve cercare continuamente di ottimizzare la disponibilità dell'infrastruttura IT e dell'organizzazione di supporto, al fine di fornire miglioramenti alla disponibilità che siano economicamente convenienti e che diano benefici tangibili al business e agli utenti



Le principali responsabilità del processo sono:

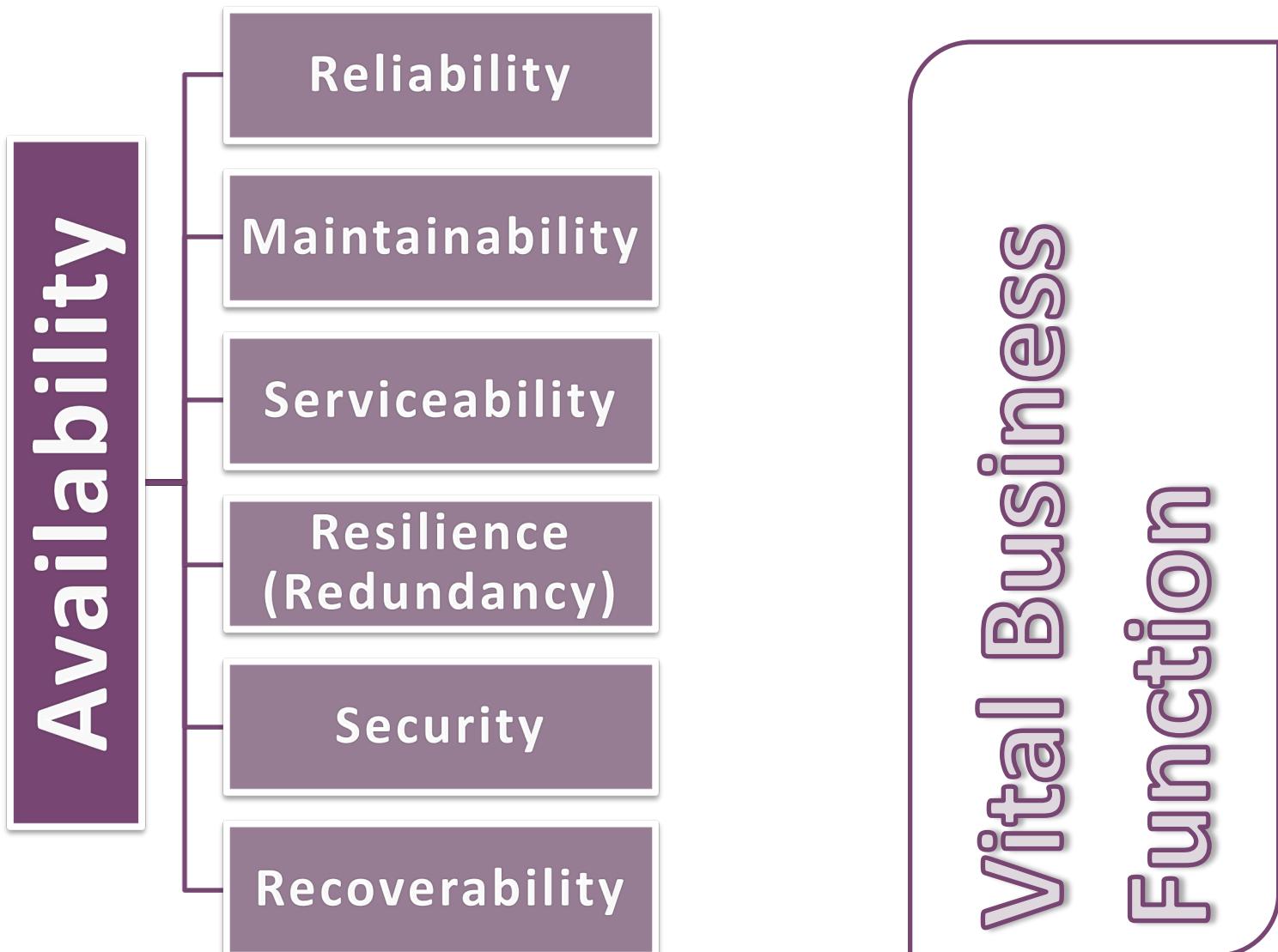
- Determinare i requisiti di disponibilità del business per un nuovo servizio IT o per il miglioramento di uno esistente e formulare opzioni di design dell'infrastruttura IT per la disponibilità ed il ripristino
- Lavorare a stretto contatto con l'ITSCM per determinare le funzioni di business vitali (vital business functions) e l'impatto derivante dal malfunzionamento di un componente IT
- Definire i target per l'Availability, la Reliability e la Maintainability per i componenti dell'infrastruttura IT che sostengono il servizio, documentandoli e concordandoli contrattualmente



- Definire, misurare e generare reporting sull'Availability, la Reliability e la Maintainability, in modo che riflettano le prospettive del business, degli utenti e dell'organizzazione di supporto IT
- Monitorare e fare Trend Analysis sulla Availability, la Reliability e la Maintainability dei componenti
- Rivedere la disponibilità del servizio IT e dei componenti e identificare se vi sono dei livelli inaccettabili



- Investigare sulle ragioni sottostanti a livelli di disponibilità inaccettabili
- Produrre e manutenere un **Availability Plan** che assegna una priorità e pianifichi i vari miglioramenti alla disponibilità IT





Availability

- La Capacità di un componente o di un servizio di svolgere la funzione ad esso richiesta in un certo momento o per un certo periodo di tempo
- Si esprime solitamente come il rapporto di disponibilità, i.e. la proporzione di tempo in cui il servizio è effettivamente disponibile al cliente durante le ore di servizio



Reliability

- La capacità di un componente di fornire le funzionalità desiderate per un certo periodo di tempo e in certe circostanze
- La Reliability non considera solo l'aspetto tecnico, ma considera anche le persone e i processi
- Un servizio sarà più affidabile se il CM stabilizza l'ambiente controllandolo ed il PM elimina con successo le cause di origine e/o previene il verificarsi di incidenti e problemi



Recoverability

- Composta da 3 aspetti
- E' la capacità di un servizio di essere ripristinato



Maintainability

- La capacità di un componente o un servizio di tornare ad una stato nel quale le funzionalità desiderate sono ripristinate
- Qui si dipende fortemente dai processi e dalle persone, poiché un componente viene ripristinato in fretta se si ha un efficiente ed efficace processo di Incident e Problem e se lo staff ha sufficienti competenze per rimediare al problema



Resilience

- La capacità di un componente o di un servizio di continuare a funzionare quando uno o più dei suoi componenti hanno dei malfunzionamenti
- L'Availability si riduce sempre nei componenti in serie e aumenta in quelli in parallelo
- Ecco perché la Resilience è, il più delle volte, l'unica soluzione quando i clienti richiedono una Availability molto elevata



Serviceability

- Un termine contrattuale usato per definire il supporto desiderato da parte di un fornitore esterno che si vuole ricevere in caso di mancata disponibilità di uno o più servizi



Security

- L'implementazione di controlli giustificabili per garantire continuità al servizio IT entro parametri sicuri, i.e. Confidenzialità, Integrità e Disponibilità



Vital Business Function (VBF)

- Questi sono gli elementi critici dei processi di business supportati dal servizio IT
- Un servizio IT può supportare funzioni del business che sono meno critiche i.e. in un servizio Bancomat, una VBF è l'erogazione di denaro, mentre la possibilità di ricevere lo scontrino potrebbe non essere considerata vitale

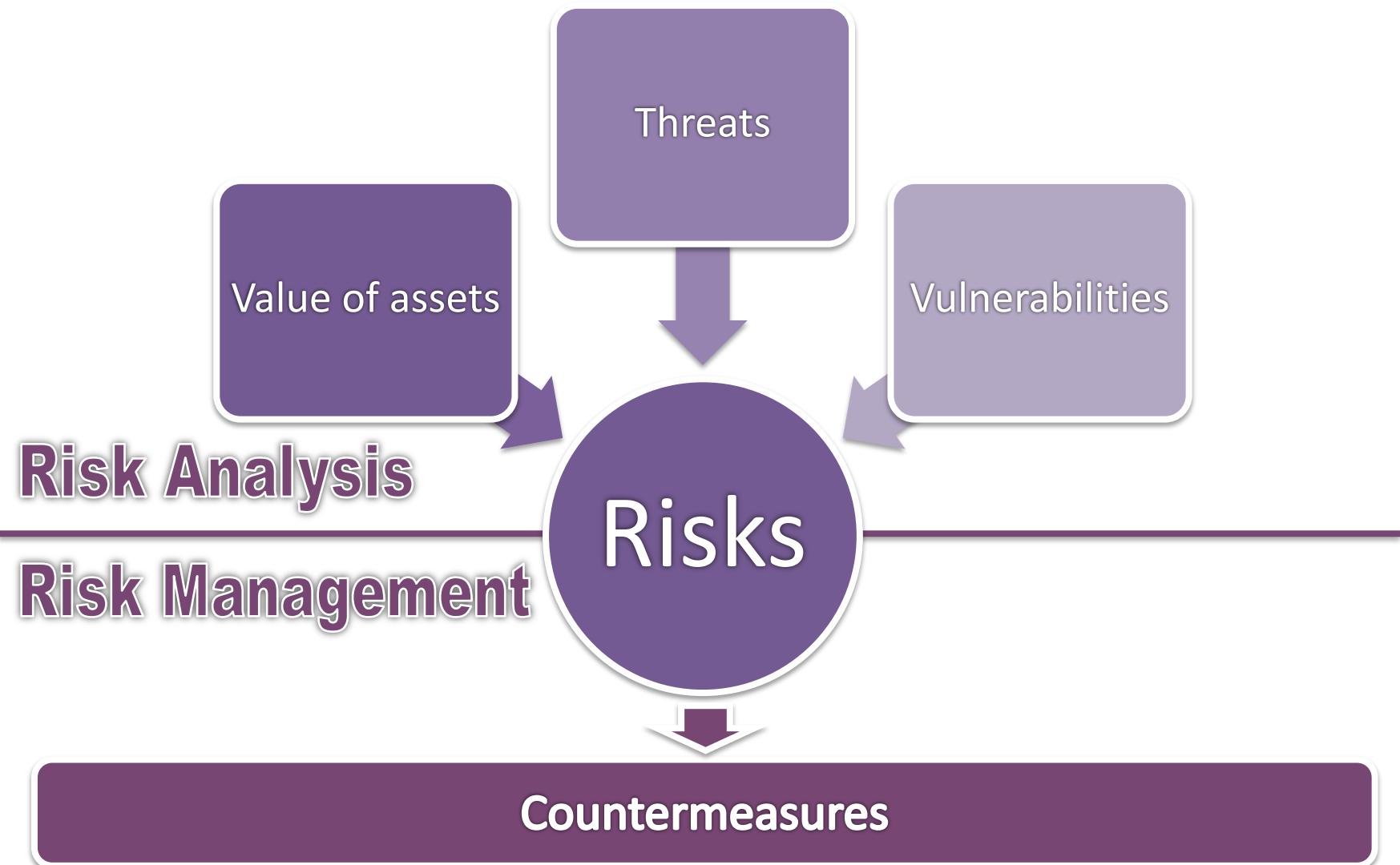


CRAMM

- CCTA Risk Analysis and Management Method

CCTA

- The United Kingdom's Central Computer and Telecommunications Agency





- Per valutare la vulnerabilità della configurazione e la capacità dell'organizzazione di supporto IT è raccomandabile che sia il design dell'infrastruttura IT proposta che l'organizzazione di supporto (sia essa interna od esterna) siano soggetti ad una Risk Analysis formale
- Il rischio è una stima di livello di pericolo e del livello di vulnerabilità dell'organizzazione a quel pericolo



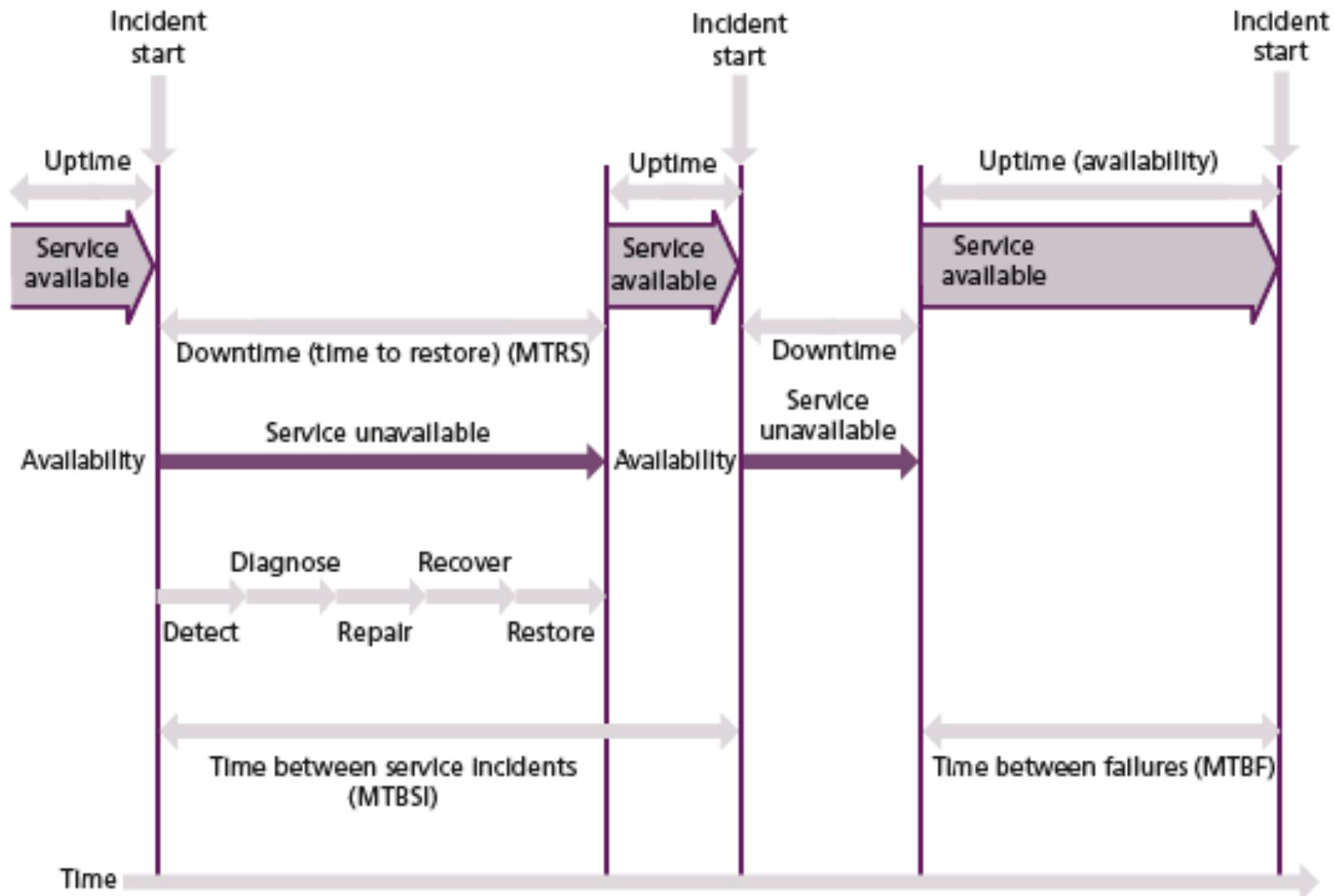
Almeno le seguenti attività di Risk Assessment devono essere svolte:

- Identificare i rischi, i.e. i rischi a cui è esposto un particolare componente di un servizio IT che supporta un processo di business e la cui rottura causerebbe un'interruzione del servizio
- Valutare le minacce e i livelli di vulnerabilità. La minaccia è la “probabilità con cui avverrà un degrado del servizio” mentre la vulnerabilità indica “se, ed in che misura, l’organizzazione sarà impattata dal presentarsi di una minaccia”



- Valutare i livelli di rischio per poter successivamente misurare il rischio complessivo. Questo può essere fatto attraverso misure se sono stati raccolti dati quantitativi, o qualitativi usando una valutazione soggettiva, i.e. basso, medio, alto

IL CICLO DI VITA DI UN INCIDENTE



IL CICLO DI VITA DI UN INCIDENTE



- Il tempo totale necessario viene calcolato dal momento in cui il problema tecnico è stato riferito al servizio e può essere diviso in:
 - Tempo necessario allo spostamento (nel caso fosse necessario l'intervento di una terza parte)
 - Tempo necessario per la diagnosi e la riparazione
- Restoration
 - È il tempo necessario per riportare il servizio a funzionare correttamente, incluse le attività come la configurazione e l'inizializzazione e il tempo necessario per rendere nuovamente il servizio disponibile all'utente
 - Il downtime dipende in parte dalla rapidità della reazione dell'organizzazione IT e/o di potenziali fornitori esterni

IL CICLO DI VITA DI UN INCIDENTE



- Per avere una idea chiara di tutto ciò, vengono presi i valori medi di quanto è stato misurato
- Queste medie vengono utilizzate per fare previsioni sui livelli di disponibilità che ci si può aspettare in futuro da un servizio e per discutere l'urgenza delle migliorie da realizzare
- I valori più importanti per l'AM sono:
 - **Mean Time To Repair (MTTR)** è il tempo medio che intercorre tra il verificarsi di un problema tecnico e la sua riparazione, anche detto “**Downtime**”. Questo tempo è la somma del tempo di individuazione e quello di ripristino. Questo valore esprime l'elasticità e la recuperabilità di un servizio. L'MTTR misura la Maintainability e/o la Serviceability

IL CICLO DI VITA DI UN INCIDENTE



- **Mean Time Between Failures (MTBF)** è il tempo medio che intercorre tra la riparazione di un incidente ed il verificarsi dell'incidente successivo, anche detto **“Uptime”**. Questo valore esprime l'affidabilità di un servizio. Il MTBF misura la Reliability
- **Mean Time Between System Incidents (MTBSI)** è il tempo medio che intercorre tra il momento in cui due incidenti consecutivi vengono riportati ed è la somma dell'MTTR e del MTBF. L'MTBSI indica la Availability
- Dalla relazione fra **MTBF** e **MTBSI** è possibile estrapolare informazioni per stabilire se prevalgono i piccoli problemi tecnici o i problemi tecnici più gravi



- E' fondamentale stabilire le regole base dell'Availability Management
- Il termine è spesso oggetto di varie interpretazioni
- Cosa si intende per 98% di Availability se quel 2% si verifica nei momenti cruciali per il business?
- L'IT e il Business devono essere sicuri di essere d'accordo sull'interpretazione delle metriche dell'Availability



Un servizio è Available quando il cliente riceve il servizio offerto come indicato nello SLA

Un calcolo semplicistico della % di Availability nei testi ITIL è:

$$\text{Availability} = (\text{AST} - \text{DT}) / \text{AST} \times 100$$

AST = Agreed Service Time

DT = Actual Downtime during AST

QUAND'È CHE UN SERVIZIO È AVAILABLE?



- La percezione del downtime da parte del Cliente può differire da quella del dipartimento IT, i.e. a causa dei ritardi nel riportare gli incidenti, a causa della percezione del business di ripristino del servizio che viene estesa al recupero di tutto il back log che il business ha accumulato
- I fornitori possono anch'essi parlare di MTTR in modo differente al dipartimento IT interno
- Anche per il cliente il “luogo di consegna” è la loro scrivania e non il dipartimento IT, che ha una diversa percezione della availability fornita

QUAND'È CHE UN SERVIZIO È AVAILABLE?



- L'IT pensa di fornire il 98% ma in realtà, rispetto alla scrivania dell'utente, è solo il 94% poiché un servizio end-to-end si basa su molte componenti, e l'availability del servizio è il risultato dell'availability di tutte quelle componenti
- Quando si riportano i dati di availability al business, si deve usare il linguaggio usato dal business
- Per il business **downtime** significa: forza lavoro non utilizzabile, guadagni perduti, clienti finali insoddisfatti, minacce di azioni legali e l'impossibilità di essere conformi alla legislazione
- Sia la durata totale del downtime che la sua frequenza inficiano la qualità del servizio

QUAND'È CHE UN SERVIZIO È AVAILABLE?



Esempio:

- SLA: servizio funzionante 5ggx8ore/week
- La settimana n.43 il servizio è stato giù per 4 ore, pertanto la disponibilità era = $(40-4)/40 \times 100 = 90\%$
- Non è così semplice: dipende da ciò che è stato concordato, come e cosa viene misurato, quanti etc.
- Se solo uno dei 1000 utenti ha un downtime di 4 ore si può realmente parlare di downtime del 10% oppure deve essere considerato $10/1000 = 0,01\%$?
- Per quell'utente è il 10% ma per tutta la compagnia è molto meno



Anche quando si rientra nello SLA il servizio può essere percepito come non disponibile

- I.e. una applicazione di Invoicing viene usata dalla divisione Finance dal Lunedì al Venerdì dalle 9 alle 17. ogni giorno dal Lun. al Ven., fra le 20 e le 22, viene fatto il backup (che la rende non disponibile). La schedulazione del backup è stata concordata con il cliente ed è nello SLA. Un utente del Finance lavora in orario straordinario: alle 20 perde il suo accesso all'applicazione a causa del backup in corso. Per l'utente il servizio non è disponibile, mentre lo SLA non è stato infranto.



Si può evitare un calcolo troppo complesso della previsione di Availability stabilendo un livello di dettaglio corretto

(A dei PC) x (A della rete) x (A dei Mainframe)

- L'Availability diminuisce sempre per i componenti in serie e aumenta per quelli in parallelo
- Comunque si noti che si sta parlando di previsioni a lungo termine e che non garantiscono il livello che sarà raggiunto nella realtà
- Si noti anche che alcuni componenti possono essere solo in serie



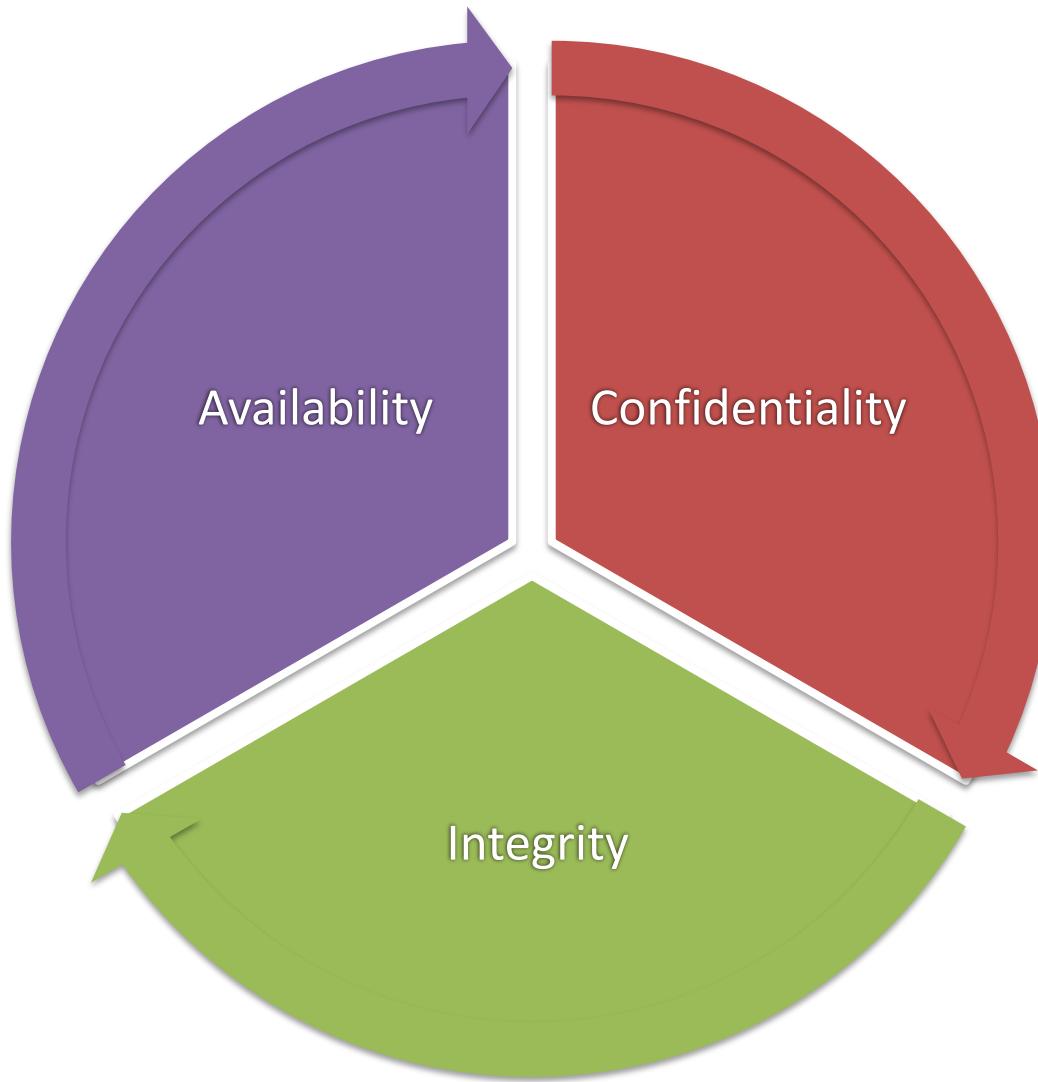
- Quando si calcola l'Availability per elementi in parallelo risulta

$$\text{Availability} = 100 - \text{non Availability}$$

- L'Availability di sistemi in parallelo si calcola

$$\text{Availability} = 100 - (\text{A e B down})$$

$$= (100 - \text{A down}) \times (100 - \text{B down})$$





- La funzione **Security Management** si interfaccia con i processi di IT Service Management che coinvolgono la sicurezza
- Questa comprende la CIA dei dati, la sicurezza dei componenti HW e SW, la documentazione e le procedure
- Il Security Management si interfaccia con il CM per valutare l'impatto di change alla sicurezza, per emettere RFC in risposta a problemi di sicurezza, etc.



- Il processo di Incident Management è il principale punto di contatto per gli incidenti sulla sicurezza (security incidents)
- I Security Incidents devono essere definiti in base ai requisiti di sicurezza concordati e specificati nella sezione security dello SLA, per permettere una loro corretta identificazione e classificazione nel processo di incident Management

CONSIDERAZIONI SULLA SICUREZZA



- Ogni SLA deve contenere una sezione sulla sicurezza
- L'AM segue le direttive derivanti dalle policy di sicurezza dell'organizzazione IT e dalle procedure e metodi associati
- Quelle che seguono sono le tipiche considerazioni sulla sicurezza che devono essere osservate:
 - I prodotti ed i servizi devono essere disponibili solo a persone autorizzate
 - Dopo un malfunzionamento, i prodotti ed i servizi devono essere recuperati garantendo che la confidentiality e l'integrity non siano compromesse e assicurando che l'availability del servizio non sia impattata
 - I prodotti ed i servizi devono essere recuperabili entro i parametri di sicurezza, i.e. non devono essere compromesse le policy IT sulla sicurezza

CONSIDERAZIONI SULLA SICUREZZA



- L'accesso fisico a computer e/o apparecchiature di rete deve essere riservato solo a personale autorizzato
- L'accesso logico al software deve essere riservato solo a personale autorizzato
- I diritti di amministratore di sistema devono essere assegnati coerentemente con il ruolo e la responsabilità
- I dati devono essere disponibili solo a persone autorizzate nei momenti concordati come indicato nello SLA
- Gli Operational Level Agreement (OLA) e gli Underpinning Contracts (UC) devono riflettere i controlli di sicurezza richiesti dall'organizzazione IT di supporto



Underpinning Contracts (UC)

- un contratto con un fornitore esterno che copre la fornitura di alcuni servizi che supportano l'IT directorate nella fornitura dei loro servizi

Operational Level Agreement (OLA)

- un accordo interno che copre la fornitura di servizi, che supporta l'IT directorate nella loro erogazione dei servizi



- Per evitare confusione fra i processi, il Security Management può essere visto come quel processo che garantisce l'aderenza alle policy di sicurezza IT relative all'implementazione di nuovi servizi IT
- L'AM garantisce che i requisiti di sicurezza siano definiti e inclusi nel quadro di Availability complessivo
- Il Security Management NON è uno dei processi ITIL affrontato dall'ITSM ma ci si riferisce ad esso quando emergono problemi sulla sicurezza. C'è un testo ITIL a parte sul Security Management

I PROCESSI DEL SERVICE DESIGN

IT SERVICE CONTINUITY MANAGEMENT



- E' la disciplina che si occupa della perdita di servizio non prevista
- Involge la pianificazione di Cls alternativi
- Può includere un singolo CI o una intera struttura di Cls (**Disaster Recovery**) con risorse IT alternative
- Parti di questa disciplina sono:
 - Analisi dei rischi
 - Studio delle opzioni
 - Pianificazione delle alternative
 - Documentazione del piano
- E' inoltre responsabile del **Contingency Plan**

IT CONTINUITY MANAGEMENT – PERCHÉ?



Una sempre maggiore dipendenza del business dall'IT

Risparmio dei costi e nel tempo di ripristino

Il costo di mantenere delle **Customer Relationship**

Sopravvivenza

Molte aziende falliscono ogni anno a causa di IT disaster

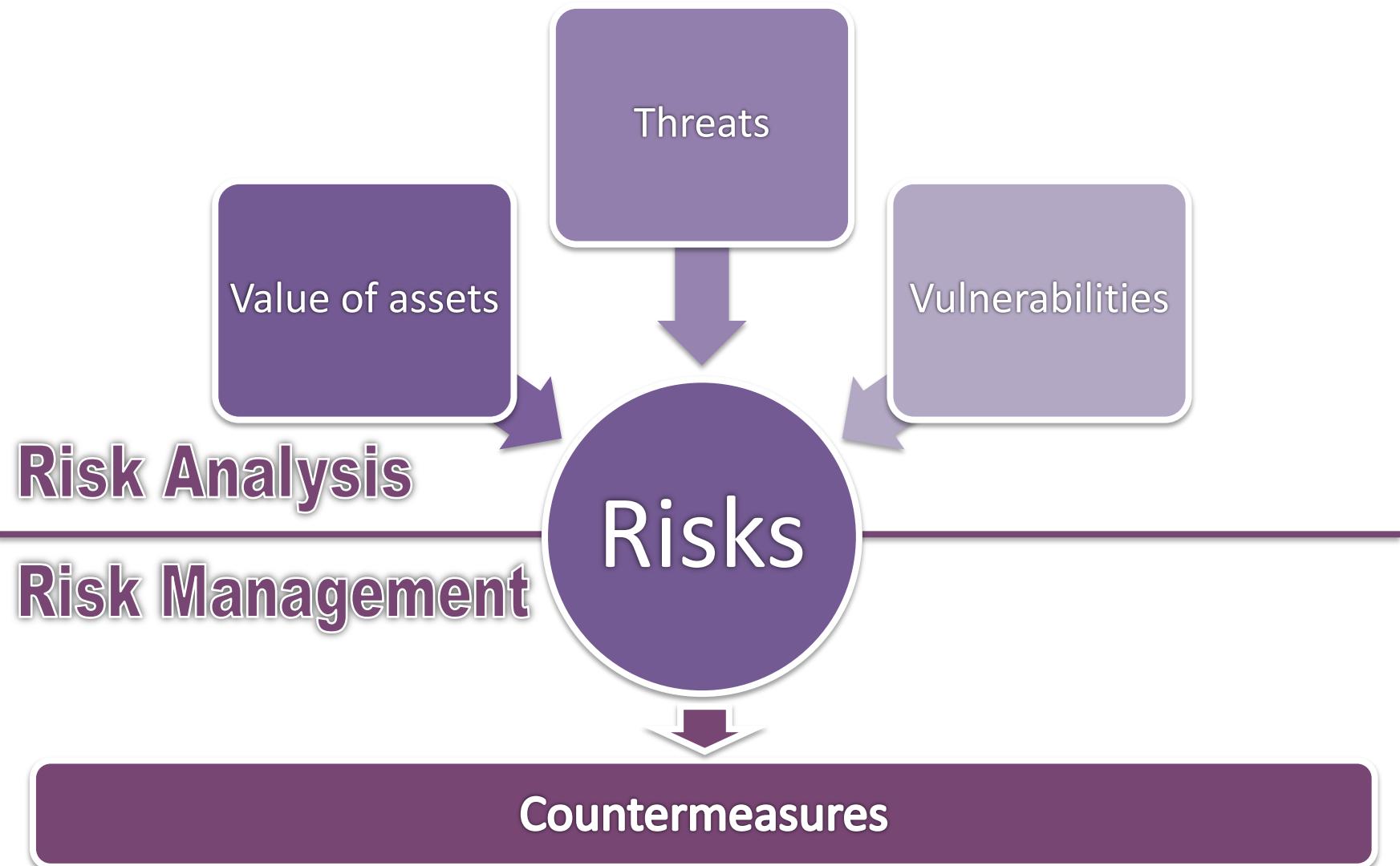


- Da quando l'ITIL ha prodotto un testo sul “Contingency Plan”, ci sono stati molti cambiamenti nella tecnologia e nel suo utilizzo nel business
- La dipendenza fra i processi di business e la tecnologia è oggi talmente forte che il Contingency Plan (il Business Continuity Planning come viene talvolta chiamato) incorpora sia l'elemento business (Business Continuity Planning) che l'elemento tecnologico (IT Service Continuity Management Planning)
- La loro dipendenza reciproca fa sì che uno sia un sottoinsieme dell'altro, a seconda del tipo di business e del livello a cui la tecnologia è penetrata nell'organizzazione



- In questa sede presupporremo che la **Business Continuity** sia l'elemento guida e la **ITSCM** un sottoinsieme del processo di **BCM**
- L'obiettivo dell'ITSCM è quello di supportare l'intero processo di BCM assicurando che le necessarie attrezzature tecniche e strutture di servizio IT possano essere ripristinati nei tempi richiesti e concordati con il business

BUSINESS IMPACT ANALYSIS (BIA)





- Il secondo fattore per determinare i requisiti dell'ITSCM è la probabilità che si verifichi una calamità o un'altra grave interruzione del servizio
- Deve essere, quindi, fatta una valutazione delle possibili minacce e della misura in cui un'organizzazione è vulnerabile ad esse
- La parte superiore del modello (basata sul CRAMM) si riferisce ai beni (assets)
- A questo punto si applicano contromisure per gestire i rischi del business proteggendo i beni



Come minimo devono essere effettuate le seguenti attività di valutazione dei rischi

Identificazione dei rischi

Assess Threat and Vulnerability levels

Assess the level of risk



Identificazione dei rischi

Danneggiamento o impossibilità di accesso ai locali adibiti

Perdita di sistemi IT, reti, PABX, firewall, sistemi di crittografia

Perdita dei dati o dell'integrità dei dati

Perdita dei servizi di rete inclusi i carrier di telecomunicazioni

Indisponibilità delle persone chiave

Mancanza di un fornitore

Perdita di servizio a causa di eccessiva domanda di servizio

Rottura dei meccanismi di sicurezza

Danni alle strutture



Una minaccia dipende da vari fattori, fra cui...

Assess Threat and Vulnerability levels

Possibile motivo,
capacità e risorse
per affrontare
un'interruzione di
servizio

L'ubicazione
dell'organizzazione,
l'ambiente e la
qualità dei sistemi e
delle procedure
interne

I processi di business
sono vulnerabili
quando ci sono
singoli punti di
rottura (single points
of failure) per
l'erogazione del
servizio



Assess the level of risk

Il rischio complessivo può a questo punto essere misurato

In seguito all'analisi dei rischi è possibile determinare adeguate contromisure o misure di riduzione dei rischi (ITSCM mechanisms)

Il Risk Management si occupa dell'identificazione e della selezione delle azioni che riducono i rischi ad un livello accettabile

Il Contingency Plan si occupa dei rischi residui

IT CONTINUITY MANAGEMENT – IL PROCESSO



Phase 1 - Initiation

Initiate Continuity Management



Phase 2 - Requirement Analysis and Strategy Definition

Business Impact Analysis

Risk Assessment

Business Continuity Strategy



Phase 3 - Implementation

Optimization and
Implementation Planning

Develop Recovery Plans

Implement Risk
Reduction Measures

Implement Stand-by
Arrangements

Develop Procedures

Initial Testing



Phase 4 – Operational Management

Education and Awareness

Training

Review

Testing

Change

Assurance



- Fase 1 – Initiation
 - Le attività che devono essere considerate in questa fase dipendono dalla misura in cui le strutture di Contingency sono state adottate nell’organizzazione
 - Alcune parti del business potrebbero aver definito dei Continuity Plan individuali basati su workaround manuali e l’IT potrebbe avere sviluppato dei Contingency Plan per i sistemi percepiti come critici
 - Questo è un buon input per il processo: comunque un ITSCM efficace si basa sul supportare le funzioni del business critiche (Critical Business Function) e sul garantire che il budget disponibile sia impiegato nel modo più adeguato



- Fase 2 – Requirement Analysis and Strategy Definition
 - Questa fase fornisce le basi per l'ITSCM ed è una componente critica per determinare la misura in cui una organizzazione può resistere ad una interruzione del business o ad una grossa calamità ed i costi a cui andrebbe incontro
 - Questa fase può essere divisa in due sezioni:
 - Requirements: effettuare BIA e valutazione del rischio
 - Strategy: determinare e concordare le contromisure per la riduzione del rischio e le opzioni di ripristino per soddisfare i requisiti



- Fase 3 – Implementation

- Una volta che è stata concordata la strategia, il ciclo di vita del Business Continuity passa alla fase di implementazione, coinvolgendo l'IT nella parte di maggior dettaglio
- La fase di implementazione è costituita dai seguenti processi:
 - Analizzare l'organizzazione e sviluppare i piani di implementazione
 - Implementare le sistemazioni temporanee (stand-by arrangements)
 - Implementare le contromisure per la riduzione del rischio
 - Sviluppare i piani di ripristino IT
 - Sviluppare le procedure
 - Procedere con i test iniziali



- Fase 4 – Operational Management
 - Una volta che l'implementazione e la pianificazione sono completate è necessario garantire che il processo sia mantenuto come parte del normale business
 - Questo è possibile tramite l'Operational Management e comprende i seguenti punti
 - **Education and Awareness** attraverso tutta l'organizzazione in particolare presso il dipartimento IT per le questioni specifiche sulla Service Continuity. Questo garantisce che tutto lo staff sia al corrente delle implicazioni della Business Continuity e della Service Continuity e considera queste come parte del loro normale lavoro e budget
 - **Training** affinché il personale sia sempre istruito sugli argomenti di Business Recovery non-IT, per garantire che il team abbia le competenze necessarie per facilitare il ripristino



- **Review.** Sono necessarie regolari revisioni di tutti gli output del processo per garantire che siano sempre attuali. Saranno necessarie per le **major change**, per le modifiche agli **assets** o agli **edifici**, per nuovi **sistemi** o **infrastrutture di rete**, per il cambio di un **fornitore**, oppure quando avvengono cambiamenti sulla **direzione del business**, della **strategia del business** o della **strategia IT**. Poiché le organizzazioni sono soggette a rapidi cambiamenti, è necessario investire in continue revisioni ed includere l'ITSCM fra i processi organizzativi del business. I nuovi requisiti vengono implementati in accordo con il processo di controllo delle modifiche
- **Testing.** In seguito ai test iniziali è necessario definire un programma di regolari verifiche per garantire che i componenti critici della strategia siano testati almeno annualmente o come stabilito dai Senior Manager. Ogni modifica deve essere adeguatamente testata!



- **Change Control.** Dopo i test e le revisioni ed in risposta alle modifiche quotidiane, è necessario che i piani dell'ITSCM siano aggiornati. L'ITSCM deve essere incluso come parte del processo di CM per garantire che ogni modifica all'infrastruttura si rifletta nelle strutture di Contingency fornite dall'IT o da terze parti. Piani non accurati o capacità di ripristino non adeguate possono far fallire l'ITSCM
- **Assurance.** Il processo finale del ciclo di vita dell'ITSCM coinvolge l'ottenimento del benessere della qualità degli output dell'ITSCM da parte del Senior Business Management e che i processi di Operational Management siano funzionanti



La scelta delle opzioni solitamente dipende molto dalle finanze disponibili o da quanto il business vuole investire





- Do nothing
 - Sarebbe difficile da giustificare poiché se un sistema non necessita di essere ripristinato, allora significa che la sua effettiva necessità deve essere riconsiderata
 - Ai clienti questo va detto se hanno scelto questa opzione
- Manual workaround
 - Può essere un'efficace misura provvisoria fino a quando i normali servizi IT non sono stati ripristinati
- Reciprocal Arrangements
 - Alcune organizzazioni concordano sul farsi da back-up reciprocamente in caso di emergenza
 - Raramente usato ad oggi eccetto che per soluzioni di storage off-site a causa di difficoltà pratiche, i.e. ridotta capacità IT in eccesso

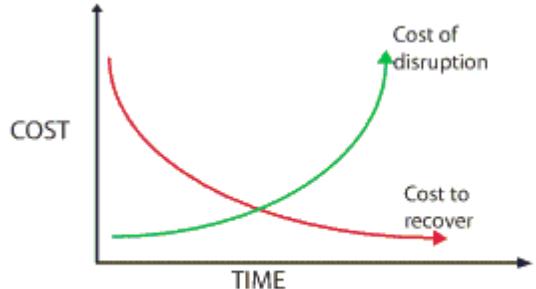


- Gradual Recovery (cold standby)
 - Solitamente consiste di una struttura informativa vuota, eccetto che per l'alimentazione ed il cablaggio, nella quale un'organizzazione può installare le sue attrezzature
 - Può essere usata quando un business può funzionare fino a 72 ore circa senza bisogno dei servizi IT
 - Può essere interna od esterna, fissa o portatile, possibilmente con la consegna delle attrezzature garantita
- Intermediate Recovery (warm standby)
 - Solitamente coinvolge il ripristino dei sistemi critici e dei servizi entro un periodo di 24 ore circa
 - Può essere interna od esterna, fissa o portatile, e consiste di una struttura informativa contenente delle attrezzature di ripristino IT che possono essere configurate per supportare il business



- Immediate Recovery (hot standby)
 - Prevede l’impiego di stabilimenti alternativi con un continuo mirroring dell’ambiente live, inclusi i dati
 - Può essere interna od esterna ed è l’opzione più costosa
 - Dovrebbe essere usata solo per quei servizi più critici per il business, la cui perdita comporterebbe un impatto immediato per il business

CONTINGENCY PLAN

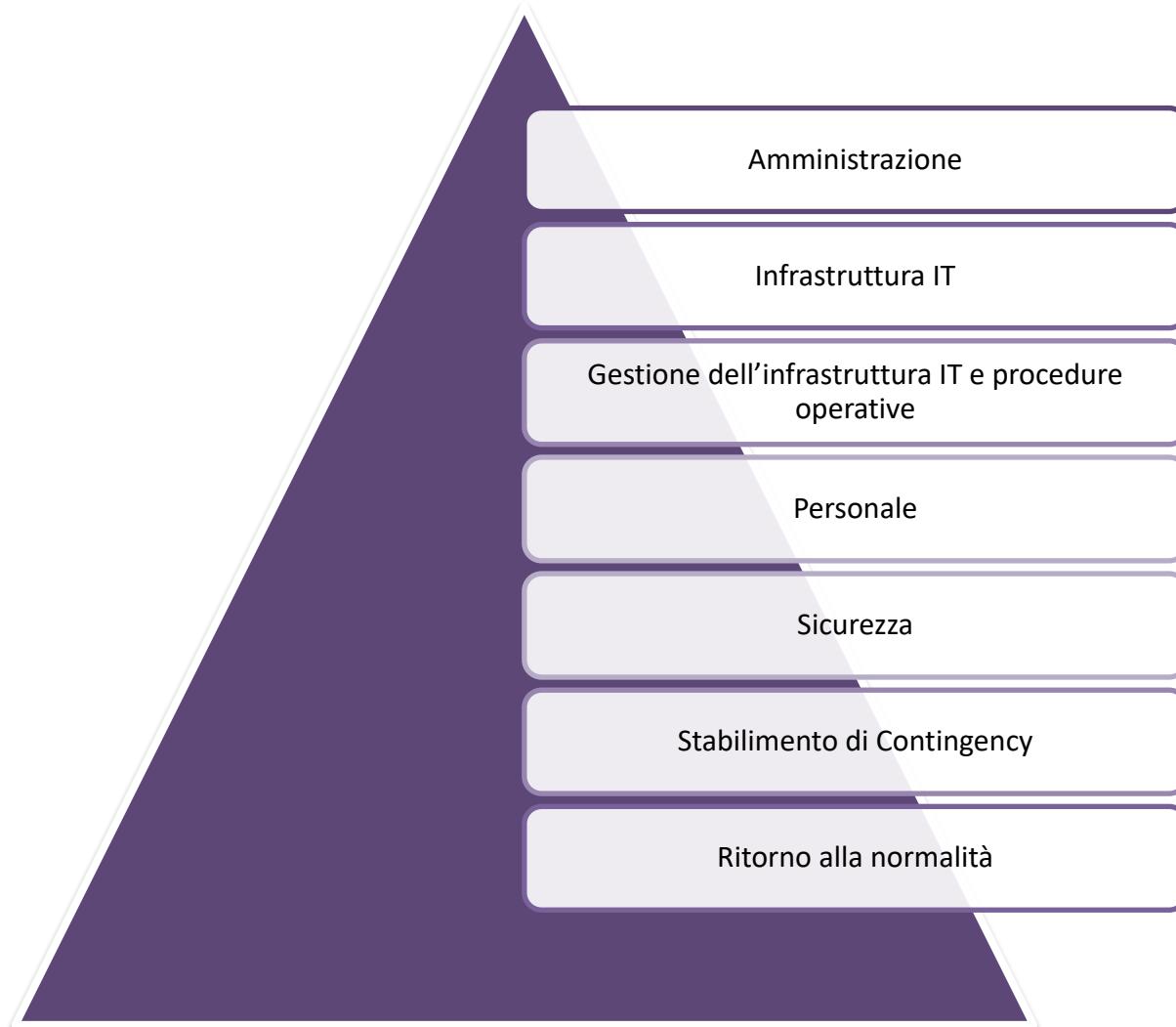


What is your firm's tolerance for risk?

Evaluate Your Firm's Contingency Plan

Plan Rating	Nonexistent	Poor	Okay	Good	Excellent
Preparedness	Backup only	Own a backup server	Co-located facility where systems reside	Ability to restore systems manually on a regular basis	Automated synchronization or equivalent on a daily basis
Philosophy	"I can't imagine I'd ever need to, but I'm confident that everything will be restored with the tape."	"I assume my IT folks will drop everything else to get my firm going again if there is a disaster."	"I've established a site to house my equipment and realize that I still need to have a more robust plan."	"I realize that it's going to take time to restore my data, but I'm prepared to make do without all of my systems for a couple of business days."	"My firm made a substantial investment to ensure that my systems are up and running ASAP, but I know the switch will take time to implement."
Recovery Time	1-2 weeks	1 week	3-4 days	1-2 days	2-4 hours
Stage	Denial	Acceptance	Planning	Implementing	Validation
Cost	\$	\$\$	\$\$\$	\$\$\$\$	\$\$\$\$\$

CONTINGENCY PLAN – LE 7 SEZIONI DEL PIANO





- Amministrazione
 - Quando e come applicare il piano: i piani d'azione e le persone coinvolte
 - Infrastruttura IT: dettagli dell'HW, dei sistemi di telecomunicazione e SW, inclusi i sistemi sostitutivi e gli accordi contrattuali per il supporto nel ripristino
- Infrastruttura IT
 - La parte dell'infrastruttura che è sottoposta al Continuity Management
- Gestione dell'infrastruttura IT e procedure operative
 - Istruzioni necessarie per fare ripartire l'operatività, inclusi i dettagli dello SLA ed i manuali



- Personale
 - Informazioni riguardanti le persone da trasferire allo stabilimento di Contingency
 - In casi di calamità lo staff è ovviamente più preoccupato della situazione dei propri familiari e dei propri beni piuttosto che dello stato dell'IT
 - Deve, pertanto, essere stabilito un piano per sostituire lo staff
- Sicurezza
 - Dettagli sull'edificio principale, sugli stabilimenti di Contingency e sulle strutture di storage remote
- Stabilimento di Contingency
 - Ubicazione, contatti, strutture, sicurezza e attrezzature per il trasporto allo stabilimento, come preparare lo stabilimento, come ripristinare l'infrastruttura e le applicazioni, i dati, etc.



- Ritorno alla normalità
 - Come avverrà, dove avverrà e quanto tempo richiederà il ripristino di tutta l'infrastruttura specialmente nel caso in cui non si ripristini tutto ma solo i servizi più importanti

ESEMPIO DI CONTINGENCY PLAN



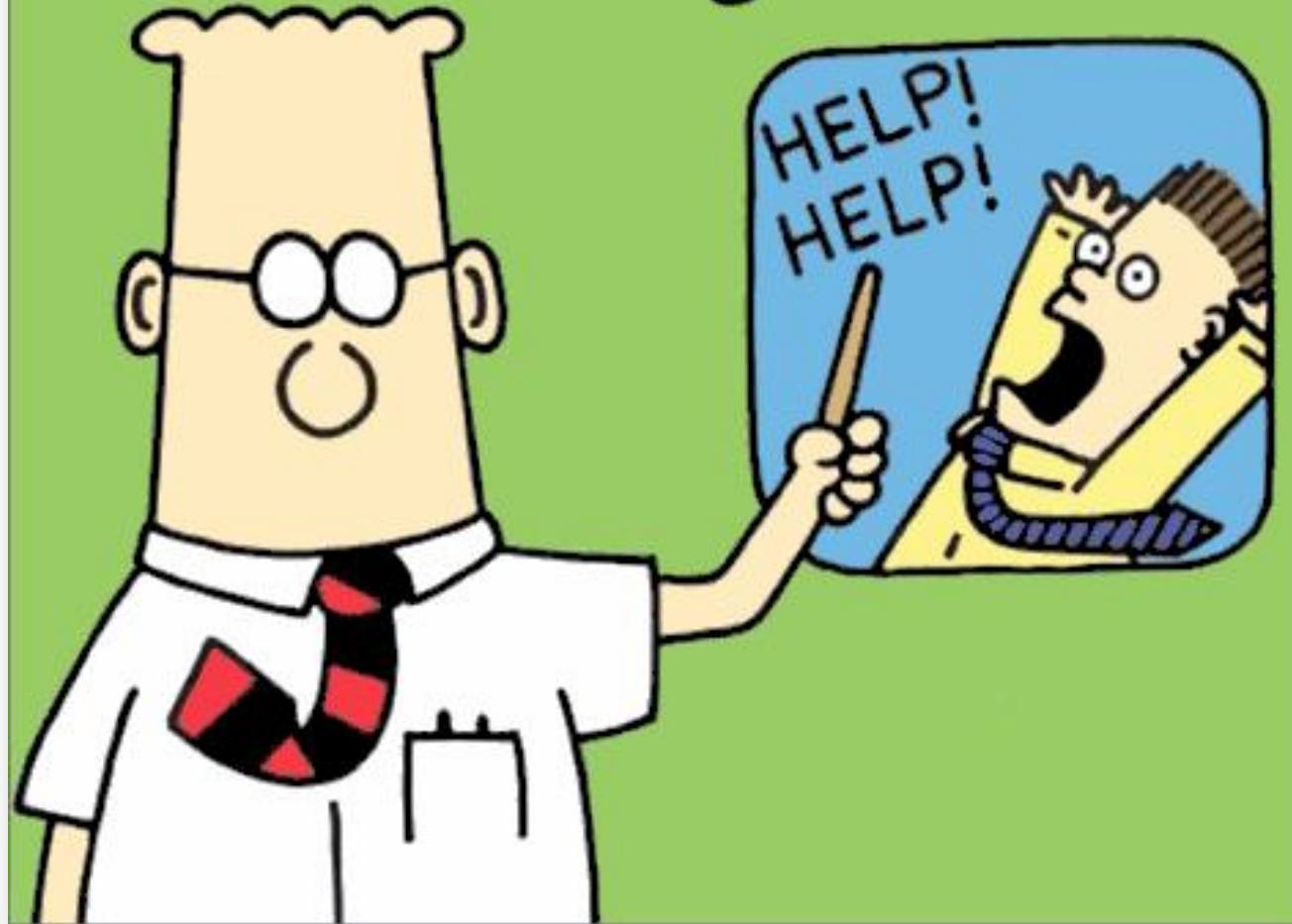
SAMPLE EVENT

CONTINGENCY PLAN

ITEM	WHAT CAN GO WRONG	SEVERITY	CONTINGENCY PLAN
Keynote Speaker	No-show	High	Fall back to alternate speaker
Wi-Fi	Doesn't work	Medium	Have a backup hot-spot available
Catering	Food isn't delivered	High	Have list of local restaurants that can cater event at last minute.
Registration desk	Registration sheets go missing	Low	Have extra copies of registration sheets separate from original sheets.



Our Disaster Recovery Plan Goes Something Like This...



I RUOLI IN SITUAZIONI NORMALI E DI CRISI



Normal Operation	In a Crisis
Livello Board (del Consiglio)	
Avviare la Continuità dei Servizi Informatici, impostare la politica, allocare le responsabilità, indirizzare ed autorizzare	Gestione delle crisi, decisioni aziendali, affari esterni
Senior Management	
Gestire la Continuità dei Servizi Informatici, accettare parti da consegnare, comunicare e mantenere la consapevolezza, integrare in tutta l'organizzazione	Coordinazione, indirizzamento e arbitrati, autorizzazione delle risorse
Junior Management	
Intraprendere l'analisi della Continuità dei Servizi Informatici, definire parti da consegnare, contattare i servizi, gestire i test e le assicurazioni	Richiamo, leadership del team, gestione del sito, collegamento e rapporto
Supervisori e staff	
Sviluppare parti da consegnare, negoziare i servizi, eseguire i test, sviluppare ed eseguire i processi e procedure	Esecuzione delle attività, partecipazione ai team, collegamenti



- Le responsabilità devono essere chiaramente definite, comunicate ai manager coinvolti e documentate in una adeguata descrizione dei ruoli e delle mansioni
- Le mansioni e le responsabilità cambiano a seconda che si appartenga a posizioni di management, di controllo od operative, come indicato nei piani di controllo e ripristino
- Vi sono responsabilità per intraprendere azioni correttive, per minimizzare l'impatto, per la gestione del ripristino o delle strutture di Contingency



- I test vanno effettuati inizialmente, poi ogni 6/12 mesi e dopo ogni calamità
- Svolgere i test rigorosamente ed in situazioni realistiche
 - Devono essere progressivi ed iterativi in modo che la fiducia cresca stabilmente
 - Devono coprire un lasso di tempo realistico: non basta dimostrare di saper ripristinare il servizio, deve anche risultare che il servizio può essere supportato dopo il ripristino nonostante lo staff ridotto ed un contesto non familiare e non agevole
- Muovere / proteggere i servizi live per primi!



- Rivedere e modificare il piano
 - Un Contingency Plan è subordinato alla manutenzione
 - Gli aspetti più complessi sono gli aggiustamenti all'infrastruttura e le modifiche a determinati livelli di servizio
 - I.e. una migrazione ad una nuova piattaforma midrange, con un warm external start può comportare che una macchina simile non è più disponibile
 - Il Conf. M gioca pertanto un ruolo importante nella protezione delle configurazioni standard che riguardano anche il Contingency Plan
- Quali Change?
 - Clienti / Servizi / SLRs / Rischi
 - Dipendenze / Asset / Cls / Staff
 - Contratti / SLAs / Contromisure / etc.



- Tutti i Change devono essere fatti con il CAB
- Test di un Plan
 - Il Contingency Plan deve essere testato frequentemente
 - Sono molte le cose che possono andare male durante una emergenza, pertanto un piano deve essere attentamente studiato
 - Inoltre, il test mostra quali sono le aree del piano carenti e quali modifiche non sono state considerate
 - A volte le modifiche possono essere testate sulle locazioni di ripristino per vedere se tutto funziona anche lì, prima di processarle nell'infrastruttura IT

I PROCESSI DEL SERVICE DESIGN

SERVICE LEVEL MANAGEMENT



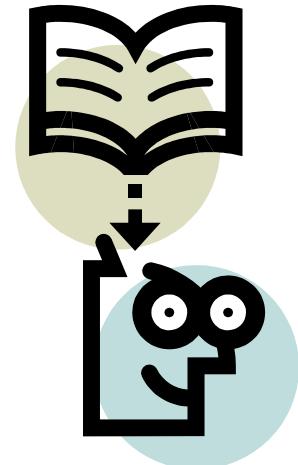
È la disciplina per la gestione della qualità e quantità del servizio offerto ai clienti dell'organizzazione dei servizi IT



L'essenza del SLM è il “Service Level Agreement” (SLA), un contratto virtuale fra l'organizzazione IT ed i clienti che stabilisce in dettaglio quali servizi devono essere offerti e con quali caratteristiche di qualità e quantità, quali le loro performance e la loro availability

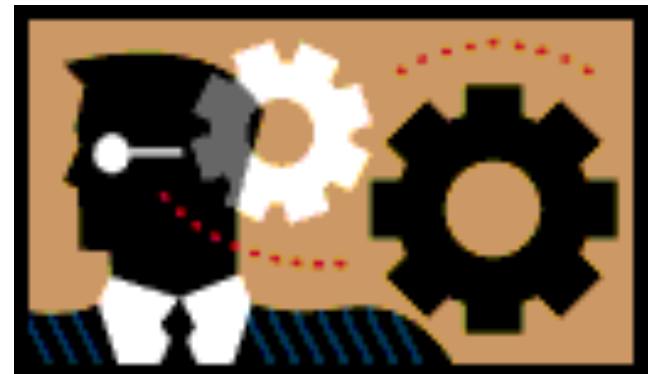


- Quando è ben articolato, lo SLA fornisce all'organizzazione IT un criterio di valutazione definitivo rispetto al quale le attività dell'organizzazione possono essere misurate
- I dettagli dello SLA facilitano la misurazione delle reali dinamiche del sistema, dando all'organizzazione IT dei numeri concreti per considerazioni e successive azioni





- Questa disciplina è forse una delle più complesse dal punto di vista delle sue implicazioni organizzative e culturali
- È tanto potente quanto complesso formalizzare relazioni tra il cliente e l'organizzazione IT
- Lo SLA può fungere da catalizzatore per introdurre altre discipline di ITSM valevoli anche in termini del loro contributo all'adempimento dello SLA





- Il SLM è essenziale quando i dipartimenti IT vogliono dimostrare il loro impegno verso una fornitura di servizi al business che siano orientati al cliente (customer oriented)
- Poiché l'IT serve solo per fornire servizi, e tutte le attività all'interno dell'IT hanno un impatto sulla fornitura del servizio, il team dell'SLM deve avere un ruolo centrale nella gestione dell'IT
- La missione per il SLM è quella di mantenere e migliorare gradualmente la qualità dei servizi IT, attraverso un costante ciclo di accordi, il monitoraggio ed i report sui risultati del servizio IT e l'esortazione a compiere azioni per non avere un servizio scandente



- Service Catalog
 - Contiene i dettagli su tutto lo spettro di servizi che il dipartimento IT può offrire e i differenti livelli di servizio a disposizione dei clienti
- Service Level Agreement (SLAs)
 - Viene negoziato per raggiungere un accordo attraverso un compromesso fra SLRs del cliente e la capacità del dipartimento IT di fornire servizi richiesti con le risorse a sua disposizione
- Service Level Requirements (SLRs)
 - Sono documenti che forniscono una dettagliata visione delle necessità del cliente e vengono usati per definire, aggiustare e rinnovare i servizi
 - Questo documento può servire come punto di partenza per disegnare un servizio e il suo corrispondente SLA e può essere firmato come un ordine per un piano, se necessario



- Operational Level Agreement (OLA) e Underpinning Contract (UC)
 - Sono documenti che supportano lo SLA e sono fatti in base agli OLA interni e UC con fornitori esterni, per descrivere le modalità di erogazione di uno o più componenti dell'intero servizio
- Service Specsheets
 - È un documento dettagliato che fa da ponte tra ciò che è stato concordato nello SLA e le specifiche tecniche interne necessarie a fornire il servizio
 - Fornisce anche degli input per lo SLA, gli OLA e i contratti in generale



- Service Quality Plan

- È un documento molto importante che contiene tutte le informazioni necessarie al management per guidare l'organizzazione IT
- Nell'SQP vengono registrati i parametri del processo di Service Management della gestione operativa
- Per ogni target di processo vengono definiti dei valori nella sezione delle Performance Indications.
- In questo modo si definiscono i tempi di risoluzione ed i livelli di impatto per l'IM, per il CM vengono definiti i tempi per la continuità e i costi di un fermo per delle modifiche e per tutti i processi vengono decisi quali report sono necessari ed in che momento
- Le Performance Indications vengono prese dai SLRs e documentate nel Service Specsheets



- Quando dei fornitori esterni sono coinvolti nella fornitura dei servizi, i.e Service Desk in outsourcing, allora le Performance Indications vengono registrate anche negli UC
- Monitoraggio, Review e Report
- Service Improvement Programs (SIP)
 - È formalmente realizzato come un progetto
 - Vengono documentate le azioni, le fasi ed i dati di release che servono per migliorare un servizio IT
- Customer Relationship Management (CRM)
 - Serve al mantenimento delle relazioni con il cliente

IL PROCESSO DI SERVICE LEVEL MANAGEMENT



- Il processo è un ciclo completo di qualità
- Una volta che lo SLA è stato definito, il ciclo inizia





- Definire la funzione
 - Se il SLM non è ancora presente, allora il primo passo da fare è quello di pianificare il processo stesso
 - Attività come la definizione delle procedure, la creazione del Service Catalogue, la stesura della bozza dello SLAs e le campagne informative rientrano tra le cose che devono essere pianificate
 - Pianificazione iniziale delle attività
 - Pianificare la capacità di monitoraggio
 - Rilevare la percezione iniziale dei servizi
 - Definire/Controllare gli UCs e gli OLAs

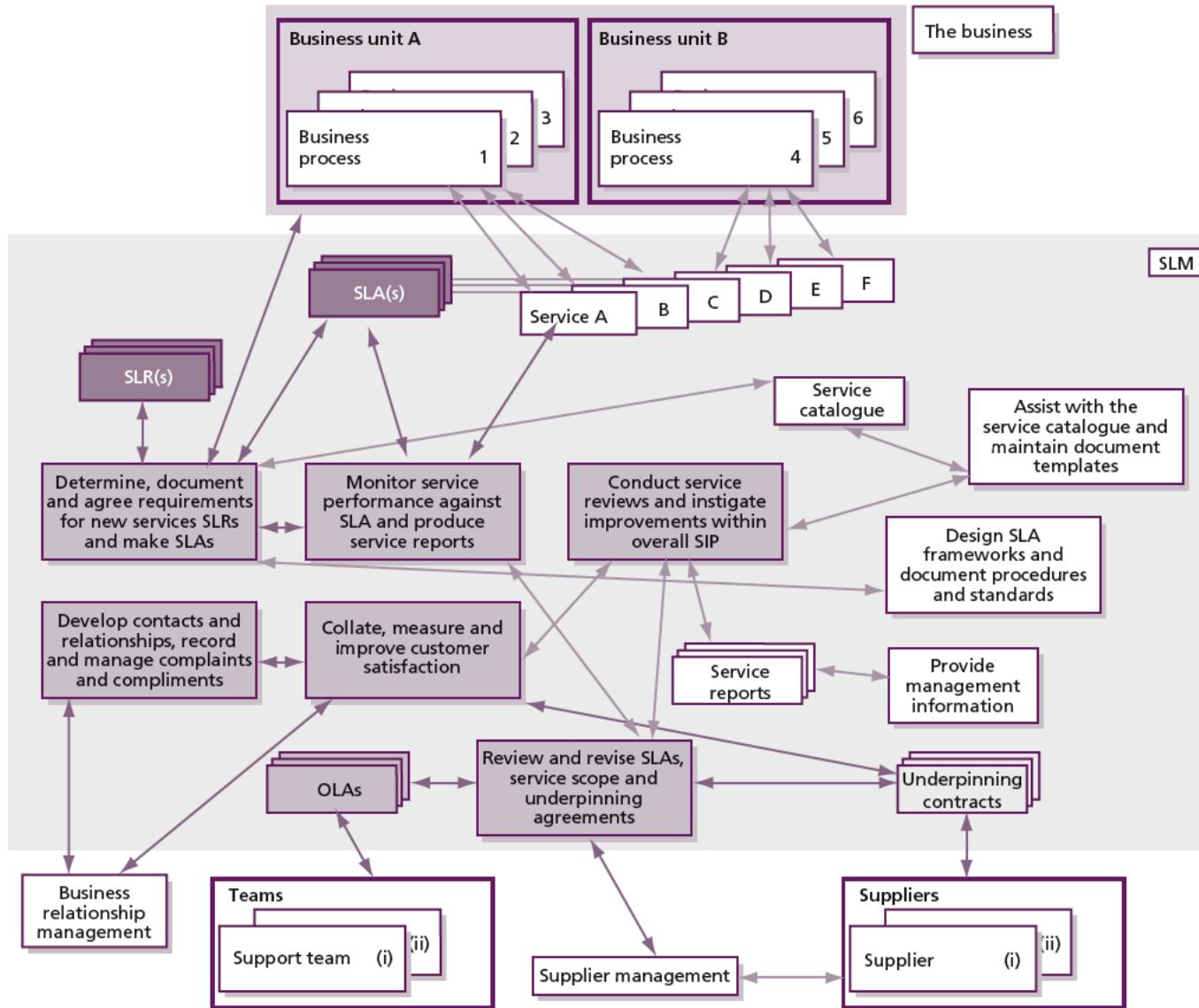


- Implementazione dello SLAs
 - Nella fase di implementazione si deve fare quanto segue:
 - Produrre un Service Catalog
 - Gestire le aspettative del Management
 - Pianificare la struttura dello SLA
 - Definire i SLRs e preparare la bozza dello SLA
 - Redigere lo SLAs
 - Creare un accordo
 - Stabilire le capacità di monitoraggio
 - Rivedere gli UCs e gli OLAs
 - Definire i processi di Reporting e Review
 - Pubblicizzare l'esistenza dello SLAs



- Managing
 - Gestire il processo in corso d'opera
 - In questa fase devono essere condotte le seguenti attività:
 - Monitoraggio e Reporting
 - Incontri di Service Review ad-hoc
- Revisioni periodiche
 - In questa fase devono essere condotte le seguenti attività:
 - Incontri di Service Review periodici
 - Creazione di Service Improvement Programs (SIP)
 - Manutenzione dello SLA, dei contratti e degli OLAs

IL PROCESSO DI SERVICE LEVEL MANAGEMENT



SERVICE LEVEL REQUIREMENTS (SLRs)



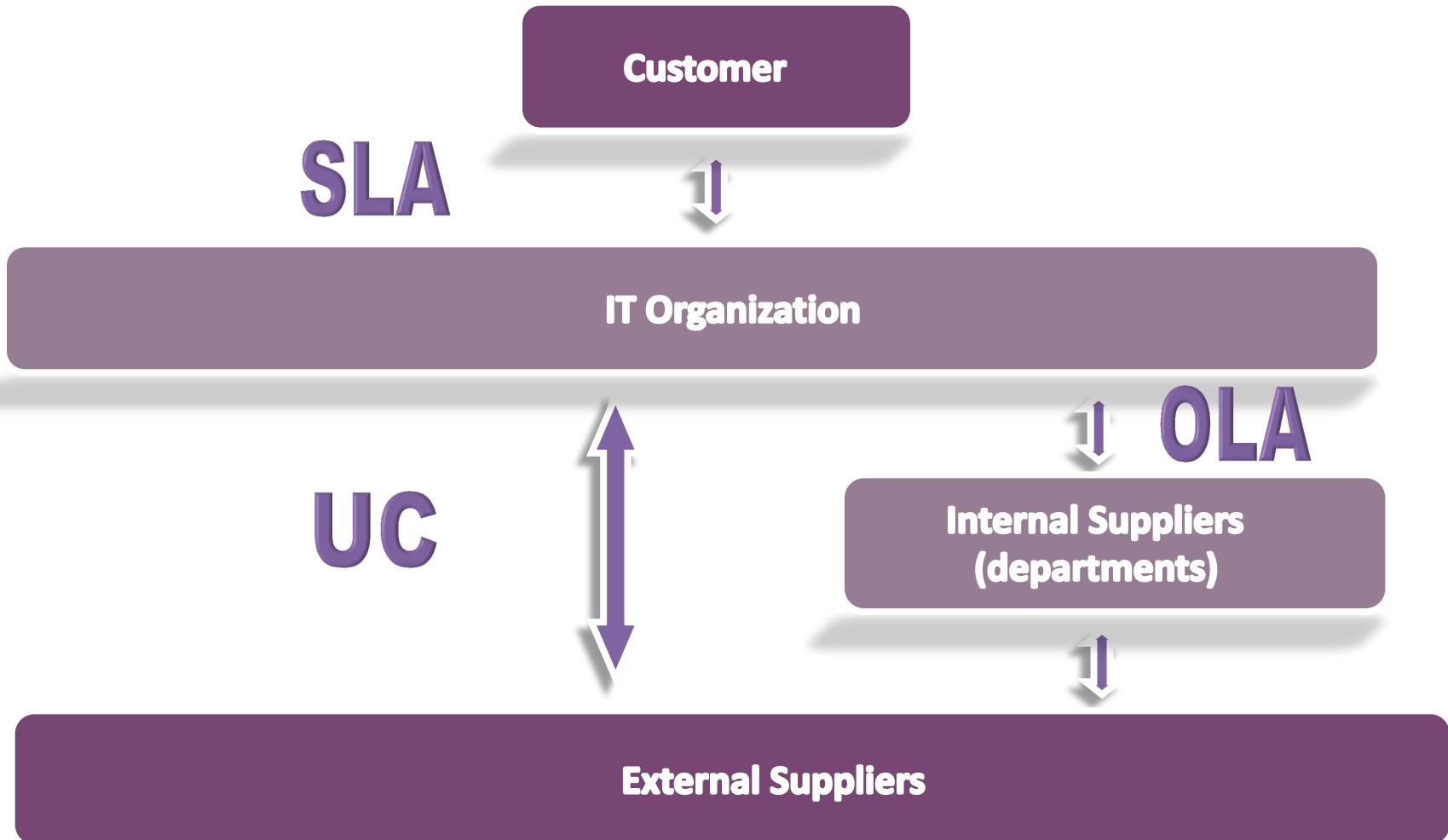
- La definizione di SLRs appropriati è uno dei fattori critici di successo (Critical Success Factors)
- È consigliabile coinvolgere i clienti sin dall'inizio, ma piuttosto che partire da zero, è meglio produrre una prima bozza di schema come punto di partenza per poi entrare più nel dettaglio nel corso della discussione con il cliente
- Si deve stare attenti a non andare troppo lontano e presentarsi al cliente con un fatto compiuto

SERVICE LEVEL REQUIREMENTS (SLRs)



- Può essere difficile progettare i requisiti, poiché il cliente potrebbe non sapere cosa vuole, specialmente se non gli è stato chiesto prima
- Inoltre, potrebbe aver bisogno di aiuto per comprendere e definire le proprie esigenze di business
- Si osservi che i requisiti espressi all'inizio potrebbero non essere quelli su cui ci si accorda alla fine – è più probabile che subiscano delle modifiche una volta che il Charging è stato introdotto
- Possono essere necessarie molte sedute di negoziazione prima di avere un bilancio accettabile tra ciò che è desiderato e ciò che è effettivamente reggiungibile ed ottenibile

AGREEMENTS E CONTRATOS





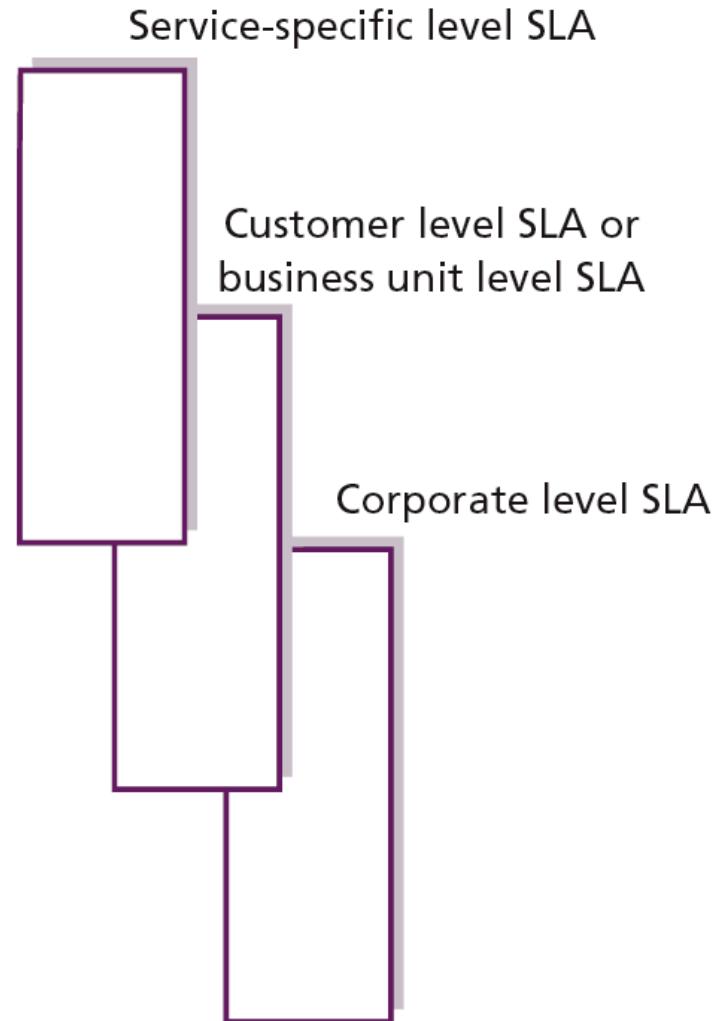
- I contratti e gli OLAs devono essere sviluppati in modo tale da permettere che gli obiettivi dello SLA siano raggiungibili
- I fornitori interni forniscono solitamente servizi di infrastruttura e varie forme di supporto tecnico
- Se necessario gli SLAs possono essere modificati affinché siano allineati ai contratti esistenti, in tal caso è comunque preferibile rinegoziare i contratti
- Ovvi benefici derivano dal gestire i contratti con i fornitori affinché siano rigorosamente allineati a livello organizzativo con il Management degli SLAs



- Un **Operational Level Agreement** è un impegno preso con un altro dipartimento IT interno nel quale gli accordi sulla manutenzione di certi componenti di un servizio vengono stabiliti, i.e. uno SPA sulla availability della rete o dei server di stampa. Uno SPA funge da supporto per l'organizzazione IT che fornisce il servizio
- Un **Underpinning Contract** è un contratto con un fornitore esterno con il quale vengono determinati gli accordi sulla manutenzione di certi componenti di un servizio. Ciò è paragonabile a uno SPA esterno con l'obiettivo, i.e., di raggiungere un accordo con un fornitore esterno sull'eliminazione di problemi tecnici sulle WS o sull'availability di una connessione perm.



Alcune organizzazioni
scelgono di adottare
strutture di SLA multi-level



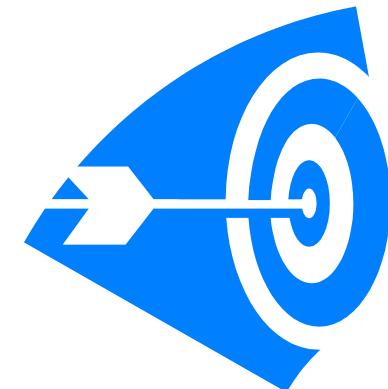


i.e. una struttura a 3 livelli del tipo seguente:

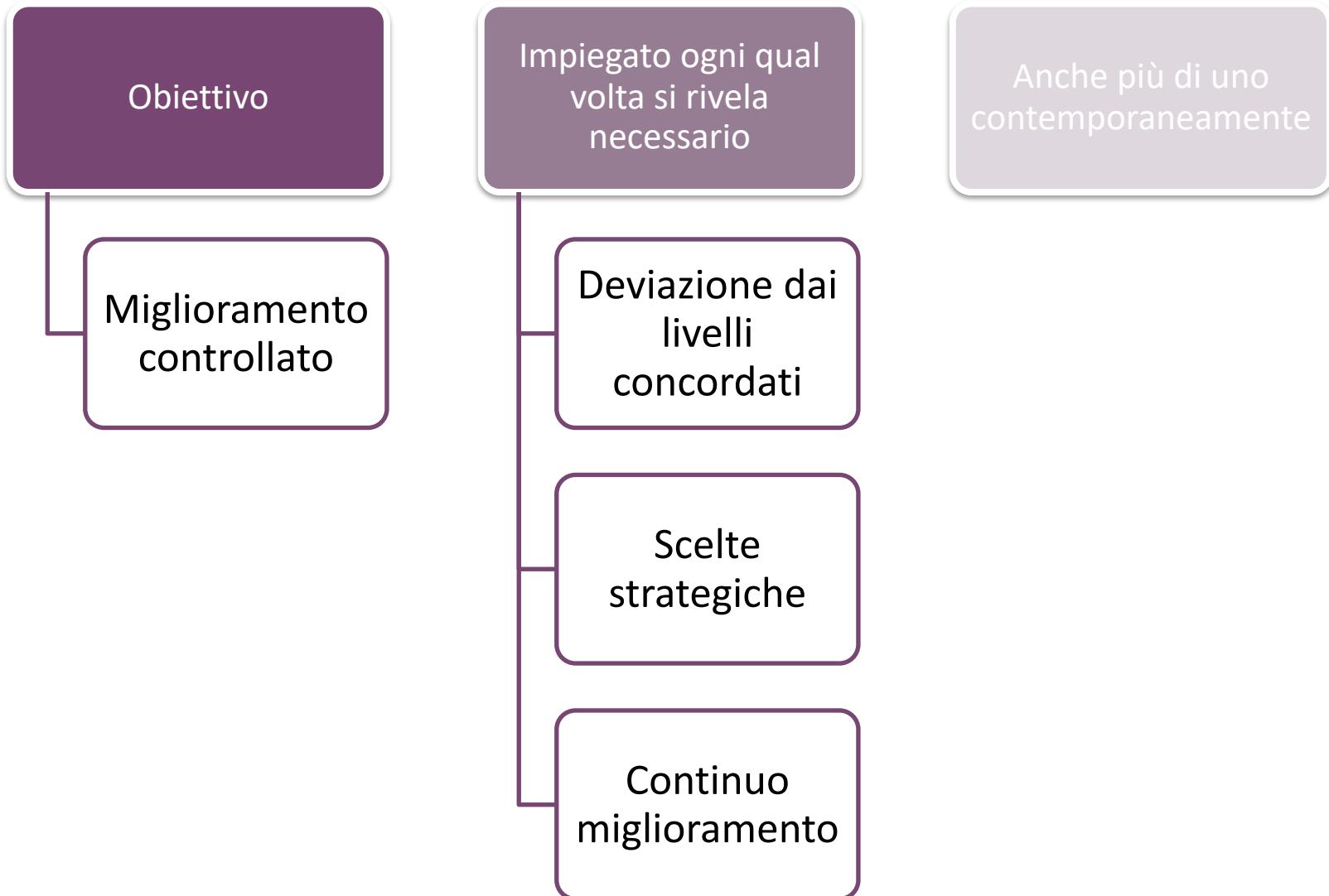
1. Corporate Level: copre tutte le problematiche di SLM a carattere generico. Queste problematiche sono spesso meno variabili e pertanto il loro aggiornamento è meno frequente
2. Customer Level: copre tutte le problematiche di SLM relative ad un particolare gruppo di Clienti, a prescindere dal servizio utilizzato
3. Service Level: copre tutte le problematiche di SLM relative ad uno specifico servizio, e ad uno specifico gruppo di clienti (uno Service Level per ogni servizio coperto dallo SLA)



- Il SQP è una descrizione interna di tutto ciò che deve essere fatto per poter fornire la qualità concordata di servizio ai clienti
- Contiene la responsabilità in termini di tempistiche interne di erogazione per raggiungere il livello di servizio concordato
- È disegnato per lo staff IT
- Descrive le azioni da intraprendere quando non viene fornito il giusto livello di qualità



SERVICE IMPROVEMENT PROGRAM (SIP)



SERVICE IMPROVEMENT PROGRAM (SIP)



- Il processo di SLM spesso rappresenta un buon punto di partenza per un SIP, ed il processo di revisione può fungere da guida per esso
- Laddove viene identificato un problema di base che sta impattando negativamente la qualità del servizio, il SLM deve, in collaborazione con il PM e l'AM, indurre all'impiego di un SIP per identificare e implementare qualunque azione sia necessaria per superare le difficoltà e ripristinare la qualità del servizio
- Le iniziative di tipo SIP possono anche focalizzarsi su problemi quali la formazione agli studenti, test e documentazione di sistemi

SERVICE IMPROVEMENT PROGRAM (SIP)



- In tali circostanze le persone di pertinenza devono essere coinvolte e deve essere necessaria una valutazione obiettiva ed adeguata per realizzare migliorie per il futuro
- In ogni momento possono essere in corso iniziative in parallelo che costituiscono un SIP al fine di affrontare difficoltà in certi servizi

ELEMENTI DI UNO SLA



- I Service Level Agreement sono accordi tra l'organizzazione IT ed il cliente e sono determinati sulla base dei servizi che è necessario fornire
- Il SLA descrive il servizio in termini non tecnici ed è impostato nella lingua del cliente
- Il SLA, durante la fase operativa, funge da norma rispetto alla quale misurare ed orientare il servizio IT
- L'ambito e l'impostazione di uno SLA può cambiare in corso d'opera
- Le clausole devono riflettere il fatto che ci sono degli obblighi sia da parte del cliente che da parte del fornitore



- Le misure incluse nello SLA devono essere significative
- Anche se le misure incluse nello SLA dovessero rappresentare solo il minimo accettabile, gli obiettivi previsti sui livelli di servizio devono essere chiaramente dichiarati
- È, inoltre, importante specificare quali servizi non sono forniti, così come lo è specificare quali servizi lo sono – i.e. un cliente deve sapere se un servizio ha dei sottosistemi di sicurezza inclusi

ELEMENTI DI UNO SLA



General	Support	Delivery
Introduction	Service Hours	Availability
Parties	Support	Reliability
Signatures	Change Procedures	Transaction Response Times
Service Description	Escalation	Throughput
Period / Lease		Batch Turnaround Times
Reporting & Review		Contingency & Security
Content		Charging
Frequency		
Incentives & Penalties		



Esempi di elementi di servizi di supporto

- **Orario di servizio:** 24x7, 5x8, con intervento, senza, etc.
- **Supporto:** orario di supporto, extra, estensioni, tempi di risposta, tempi di riparazione, etc.
- **Sistema di Escalation:** chi, quando, come, per cosa, etc.
- **Change:** Categoria, tempo medio, numerosità, standard requests, etc.



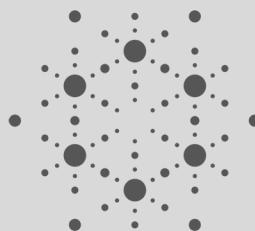


Esempi di elementi di Erogazione del Servizio

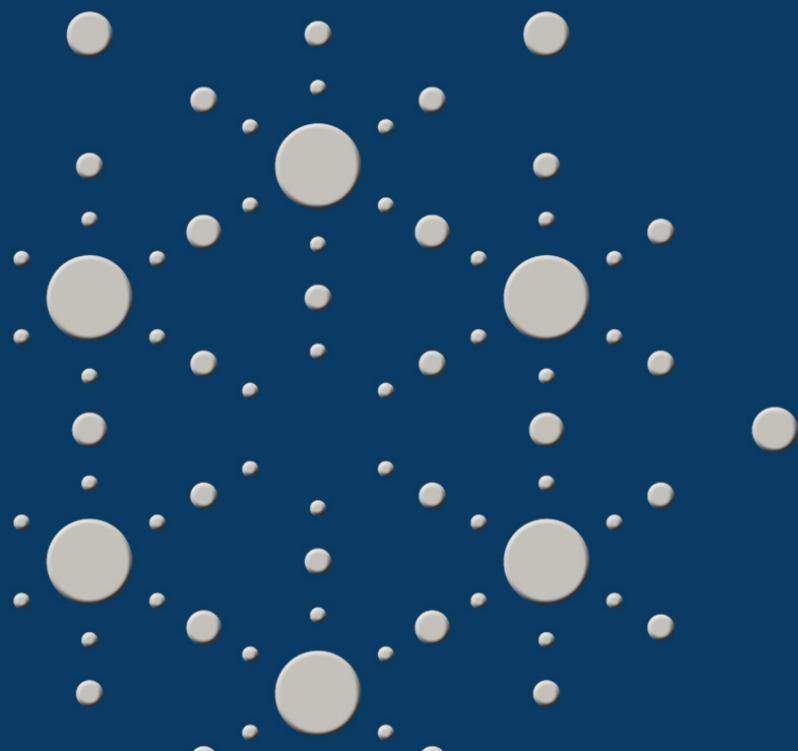
- **Availability:** 99%, target durante le ore di servizio, etc.
- **Reliability:** quante volte si verifica un'interruzione di servizio in un certo periodo, MTBF, MTBSI, etc.
- **Continuity e Security:** cosa, come, ruoli, responsabilità, procedure, etc.
- **Charging:** formule, pricing, metodologia, etc.
- **Tempi di esecuzione dei Batch:** input ed output: quando, dove, come, etc.
- **Tempi di risposta delle Transazioni:** tempo di apertura di 1 documento da 1Mb \leq 15 sec., nel 95% dei casi il tempo è \leq 2 sec., etc.
- **Carico di lavoro sostenibile (Throughput):** volume, num. utenti, traffico di rete, pagine, etc.

DOMANDE?

GRAZIE PER L'ATTENZIONE.



NETCOM
IT Life Cycle Management



N E T C O M
IT Life Cycle Management