

# Sicurezza dei sistemi informatici in internet



"Master lock with root password" di Scott Schiller - Flickr: Master lock, "r00t" password. Con licenza CC BY 2.0 tramite Wikimedia Commons

Università di Ferrara

Corso di Laurea Magistrale in Ingegneria Informatica e dell'Automazione

Ing. Massimo Carnevali

Anno Accademico 2015 - 2016

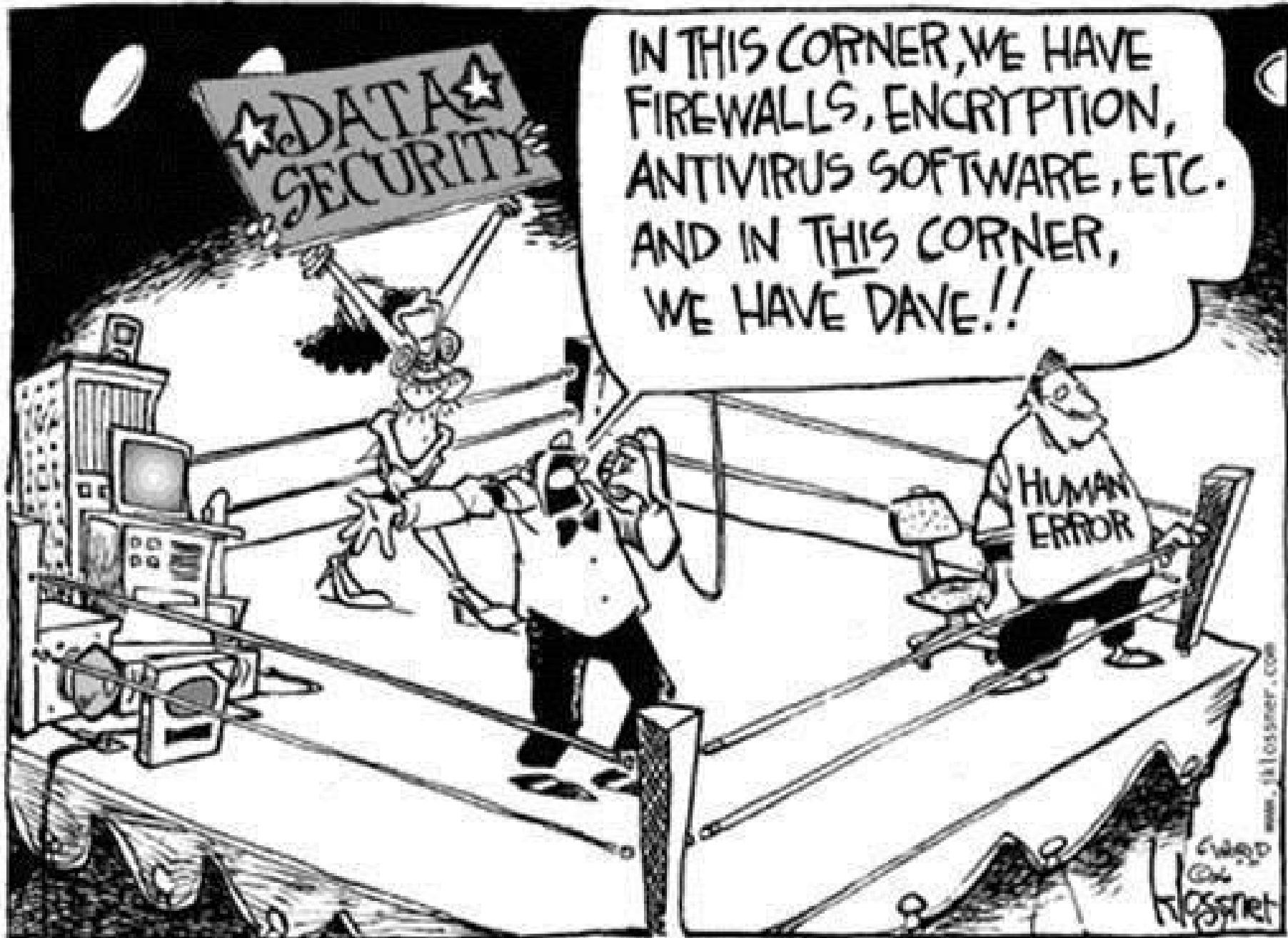
## Il fattore umano e organizzativo

- Concetti base
- Social engineering
- Spam, phishing e dintorni
- Cenni di gestione dei processi IT

## Il fattore umano e organizzativo

- **Concetti base**
- Social engineering
- Spam, phishing e dintorni
- Cenni di gestione dei processi IT

# Il fattore umano e organizzativo



# Il fattore umano e organizzativo

Molti temi tecnologici hanno una loro controparte umana/organizzativa: sicurezza della navigazione, gestione dispositivi mobili, la posta elettronica, l'antivirus i salvataggi dei dati ecc.

*“Se non conosci te stesso e non conosci il tuo nemico, sii certo che ogni battaglia sarà per te fonte di pericolo gravissimo.”*

(Sun Tsu - L'arte della guerra)

Attaccare i server e i DataCenter sta diventando sempre più complesso; è più facile provare a passare dal client e dall'utente finale, normalmente molto più fragili e attaccabili.

## Problemi base (non tecnologici)

- scarsa comprensione del problema (awareness)
- fallibilità degli esseri umani (soprattutto in condizioni di sovraccarico, frustrazione, ...)
- gli esseri umani hanno una naturale tendenza alla fiducia
- interfacce/architetture complesse che facilitano gli errori
- calo di prestazioni dovuto all'applicazione delle misure di sicurezza
- Shadow IT (chi usa Dropbox in azienda ? Il mio PC/smartphone/tablet personale è meglio di quello aziendale !) ..... **da cui segue --->**

## Bring your own device (BYOD)

- Varie declinazioni: “Bring your own technology (BYOT)”, “Bring your own phone (BYOP)”, “Bring your own PC” (BYOPC), “Bring your own cloud (BYOC)” ecc.
- COPE (Company Owned, Personally Enabled) vs POCE (Personally Owned, Company Enabled)
- Esistono strumenti per aggredire il problema tecnologico, è molto più complesso aggredire quello organizzativo (e legale, ad esempio GPS)

## Bring your own device (BYOD)

- Definire i limiti e le modalità di utilizzo dei dispositivi mobili non aziendali (o aziendali, quando abilitati anche all'uso personale)
- Definire le responsabilità aziendali e quelle personali nell'uso dei dispositivi misti (responsabilità diverse nei casi di BYOD vs COPE)
- Definire i servizi, le applicazioni e i dati che devono essere accessibili dai dispositivi
- Fare un'analisi dei rischi dell'adozione del BYOD
- Definire l'infrastruttura tecnologica, le misure di sicurezza, le politiche di licensing, i sistemi di monitoraggio, le procedure di gestione e gli strumenti di supporto

## Il bersaglio

Il bersaglio solitamente parte dal presupposto di non essere tale. Sindrome del “perchè dovrebbero attaccare proprio me”.

Capire i meccanismi mentali e i modelli che l'utente si costruisce rispetto ai potenziali strumenti di attacco.

Perché una tecnologia funzioni bisogna che il modello della minaccia sia percepito allo stesso modo da chi sviluppa il software e da chi lo dovrà utilizzare (esempio del lucchetto per https e del “cestino” di Windows).

Attenzione all'influenza dei modelli culturali di base (occidentale/orientale, giovane/anziano ecc.).

## Il nemico

Il “nemico” non è sempre “fuori”, non è sempre cattivo e a volte non sa nemmeno di essere “il nemico”.

E allora perché diventa un “nemico” ?

E' importante capire i meccanismi perché sono più complessi di quelli dei nemici naturali esterni.

Come abbiamo visto nel primo modulo i nemici esterni solitamente sono “cattivi di professione”.

Capire i meccanismi per prevenire i comportamenti ostili, sbagliati o semplicemente dannosi.

## La consapevolezza del gesto criminale

Le persone, prima di commettere un illecito, valutano i pro e i contro e le conseguenze del loro gesto. Percepiscono, valutano, pensano; poi decidono se agire o no.

L'essere umano orienta il proprio comportamento (a maggior ragione quello criminale) in base ad una serie di informazioni che provengono dalla sua esperienza e dall'ambiente esterno.

Realtà esterna + esperienza personale/collettiva

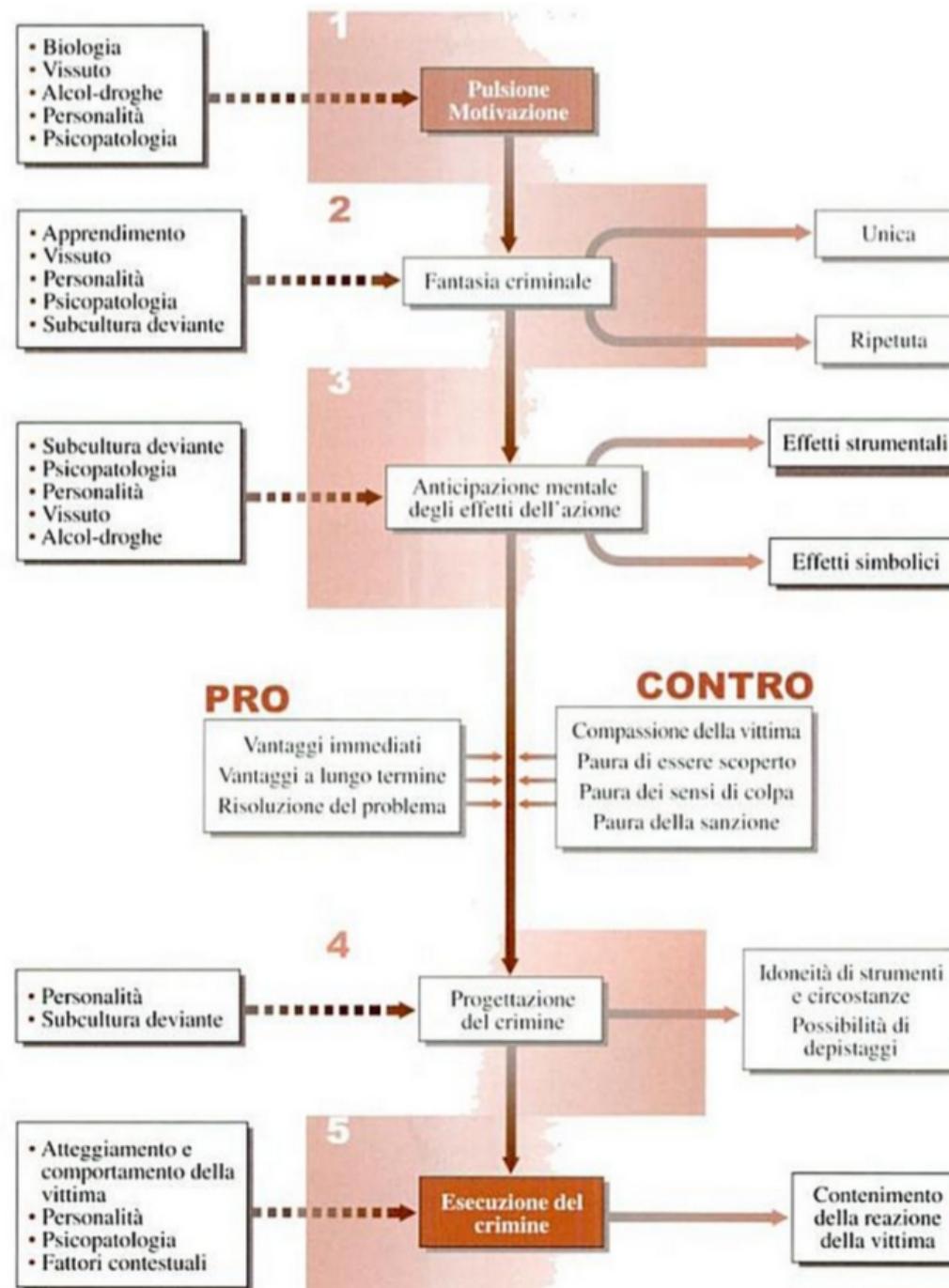
- Atteggiamenti diffusi + percezione sociale
- Elaborazione mentale + calcolo pro/contro
- Scelta del comportamento/azione

## La consapevolezza del gesto criminale

La dinamica criminale secondo il Prof. Marco Strano ([Manuale di Criminologia Clinica](#)) è articolata in cinque fasi di pensiero che inconsciamente si susseguono nella nostra mente:

- 1) Motivazione/pulsione a compiere l'azione
- 2) Fantasia criminale
- 3) Anticipazione mentale degli effetti dell'azione (empatia con la vittima, sensi di colpa, rischio di essere scoperto, possibilità di essere denunciato una volta scoperto, paura della sanzione, cosa ne pensa "il branco" ecc.)
- 4) [eventuale] Progettazione del crimine
- 5) [eventuale] Esecuzione del crimine

# Il fattore umano e organizzativo



## L'intermediazione tecnologica del gesto criminale

Nel “computer crime” scompare il contatto fisico fra l'autore del reato e la vittima.

A volte scompare anche il contatto fisico fra il reato e l'oggetto del reato.

Questo cambia completamente la fase di anticipazione mentale del crimine.

# L'intermediazione tecnologica del gesto criminale

- Attenua la percezione degli effetti del crimine sulla vittima
- Allarga la base dei possibili autori di reato rendendo adatti al crimine anche soggetti normalmente estranei al mondo della criminalità tradizionale
- Crea un fenomeno di illegalità distribuita in larghe aree sociali (vedi ad esempio il tema della violazione dei diritti d'autore o della copia illegale del software)
- Diffonde un falso senso di impunità su determinati crimini (spesso solo per mancanza di informazione)
- Disaccoppia le leggi civili e penali dall'azione criminale in corso

Per approfondimenti: <http://www.criminologia.org/>

# Il fattore umano e organizzativo

- Concetti base
- **Social engineering**
- Spam, phishing e dintorni
- Cenni di gestione dei processi IT

## Social engineering

- Sfruttare la partecipazione (inconsapevole) dell'utente per un attacco
- Si cerca di sfruttare l'ingenuità/ignoranza/fiducia dell'utente
- Meccanismi di pressione psicologica ([Nigerian Scam](#))
- A volte ci cascano anche utenti esperti
- Sfrutta molteplici canali di attacco (mail, telefono, comunicazioni cartacee, chiavette USB ecc.)
- Per riuscire bene richiede una fase di studio e di analisi molto accurati (attenzione a quello che racconta di noi il nostro sito web, i social ecc.)
- Dimostrare di conoscere bene l'azienda, le persone, le procedure porta istintivamente il target dell'attacco ad abbassare la guardia

## Social engineering

Elementi comportamentali attaccabili:

- **Reciprocità**: se mi fai un regalo o mi risolvi un problema sono predisposto a ricambiare
- **Coerenza**: stabilità dei propri comportamenti e delle proprie convinzioni
- **Validazione sociale**: “Io fanno tutti ...”
- **Liking**: si tende a dare fiducia a chi è simpatico, bello o gentile
- **Autorità**: esiste una sudditanza di base verso l'autorità vera o presunta
- **Scarsità**: si tende a sovrastimare il valore di una cosa potenzialmente scarsa
- **Altruismo**: siamo tendenzialmente portati ad aiutare una persona in difficoltà

## Social engineering

La ricostruzione di un attacco reale (sembra un film ma è basato su una storia vera):

Targeted Cyber Attack Reality - Trend Micro  
<https://www.youtube.com/watch?v=0hs8rc2u5ak>

Costruire un attacco mirato partendo da quanto ricavabile dai Social Network:

Amazing mind reader – Safe Internet Banking - Belgio  
<https://www.youtube.com/watch?v=F7pYHN9iC9I>

## Social engineering

Un esempio personale:



## Lettura istruttiva

L'arte dell'inganno - Kevin David Mitnick

# Il fattore umano e organizzativo

- Concetti base
- Social engineering
- **Spam, phishing e dintorni**
- Cenni di gestione dei processi IT

## Spam

Lo spam, o “Unsolicited Commercial Bulk Email”, è un fenomeno largamente diffuso.

Da solo occupa buona parte della banda internet.

Consiste nel pubblicizzare prodotti e servizi a scopo commerciale o di phishing, o nell'indurre il destinatario della mail a visitare siti o pagine compromessi al fine di catturare dati o credenziali.

Produce danni sia come perdita di tempo che, a volte anche direttamente economici.

Non vi sono rimedi particolarmente efficaci o applicabili con elevato successo; tenendo alta l'attenzione all'evolversi del fenomeno si mettono in atto diverse pratiche, non ultima la **“semplice”** educazione degli utenti.

## Antispam

Vengono utilizzate varie metodologie per **mitigare** gli effetti dello spam (il punto finale dell'attacco rimane sempre l'utente finale):

- Filtri sui contenuti (probabilistici e comunque sempre un passo indietro rispetto all'attaccante)
- Black&white-listing dei mittenti (aggiornamento delle liste, rischio DOS per mittenti inconsapevoli)
- **Sender Policy Framework** (controllo incrociato con MX record del DNS)
- Graylisting (rifiuto la prima mail con un “temporary error”)

Siti per verificare se sono finito nelle liste degli spammer (ad esempio <http://mxtoolbox.com/blacklists.aspx> )

# Phishing

Neologismo, assonanza con “fishing” → “Andare a pesca di ingenui”. Via mail ma anche via IM.

Social Engineering di massa, spesso poco mirato, si lanciano milioni di esce sperando che qualcuno abbocchi. Utilizzo di “shadow server”.

Metodologie di difesa simili a quelle contro lo spam.

Ancora più importante però la consapevolezza dell'utente. A differenza dello SPAM la minaccia è nascosta e richiede un'azione da parte dell'utente.

Insegnare all'utente di cercare sempre il “lucchetto verde”.

## Phishing

**Whaling:** phishing mirato a CIO/CEO, molto sofisticato.

**Spear Phishing:** attacchi molto mirati a singole persone o gruppi, non necessariamente in alto nella catena gerarchica, ma potenzialmente canali di intrusione in azienda. Spesso l'anello debole della catena, alta percentuale di successo. Non esiste una risposta tecnologica → Awareness !

MESTRE

## Sventata frode informatica ai danni di un noto calzaturificio veneziano

*Con la tecnica delle “fake mail”, ovvero le mail fasulle, l'imprenditore rischiava di perdere 58 mila euro di una commessa. I soldi sono stati restituiti alla vittima della truffa  
di Mitia Chiarin*

 FAKE MAIL  TRUFFE  POLIZIA  POLIZIA POSTALE

17 luglio 2015



## Il fattore umano e organizzativo

- Concetti base
- Social engineering
- Spam, phishing e dintorni
- **Cenni di gestione dei processi IT**

## Gestione e sicurezza

Senza gestione non può esserci sicurezza.

Come faccio a definire delle policy di sicurezza aziendali se non conosco ruoli, funzioni, necessità ecc. degli utenti ?

Il perimetro aziendale a volte è complesso (partecipate, consociate, consulenti, insourcing, outsourcing ecc.).

Nessuna tecnologia può aiutarmi a sapere “chi fa che cosa” in azienda.

Serve organizzazione, metodo, policy e profonda conoscenza del proprio “environment”.

A volte bisogna comunque arrivare a soluzioni di compromesso.

# Il fattore umano e organizzativo



**Le aree in cui è suddiviso ITIL (core books) nella nuova versione V3 comprendono:**

- Service Strategy: allineamento fra il business ed i servizi IT
- Service Design: progettazione dei servizi di Service Management
- Service Transition: gestione del cambiamento e avvio in produzione
- Service Operations: gestione dei processi operativi
- Continual Service Improvement: miglioramento continuo dei servizi

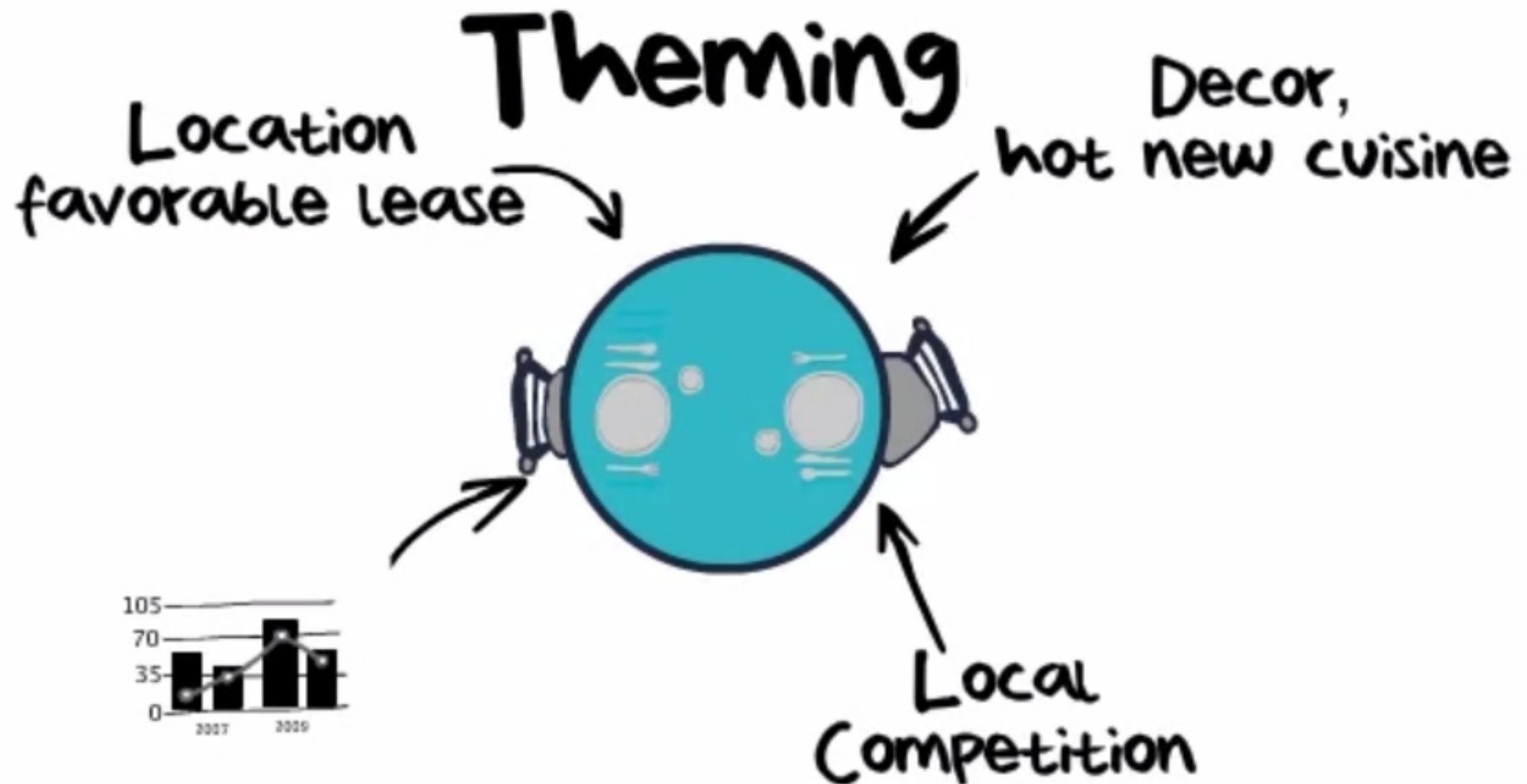
[http://en.wikipedia.org/wiki/Information\\_Technology\\_Infrastructure\\_Library](http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library)

## E se i servizi IT fossero un ristorante ?

<https://www.youtube.com/watch?v=vBguassbAzo>

# Il fattore umano e organizzativo



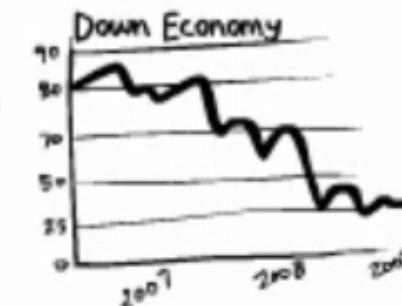
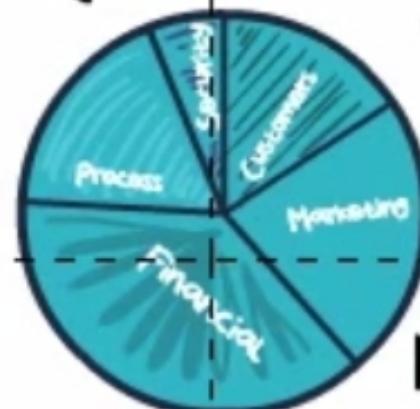


## Service Strategy

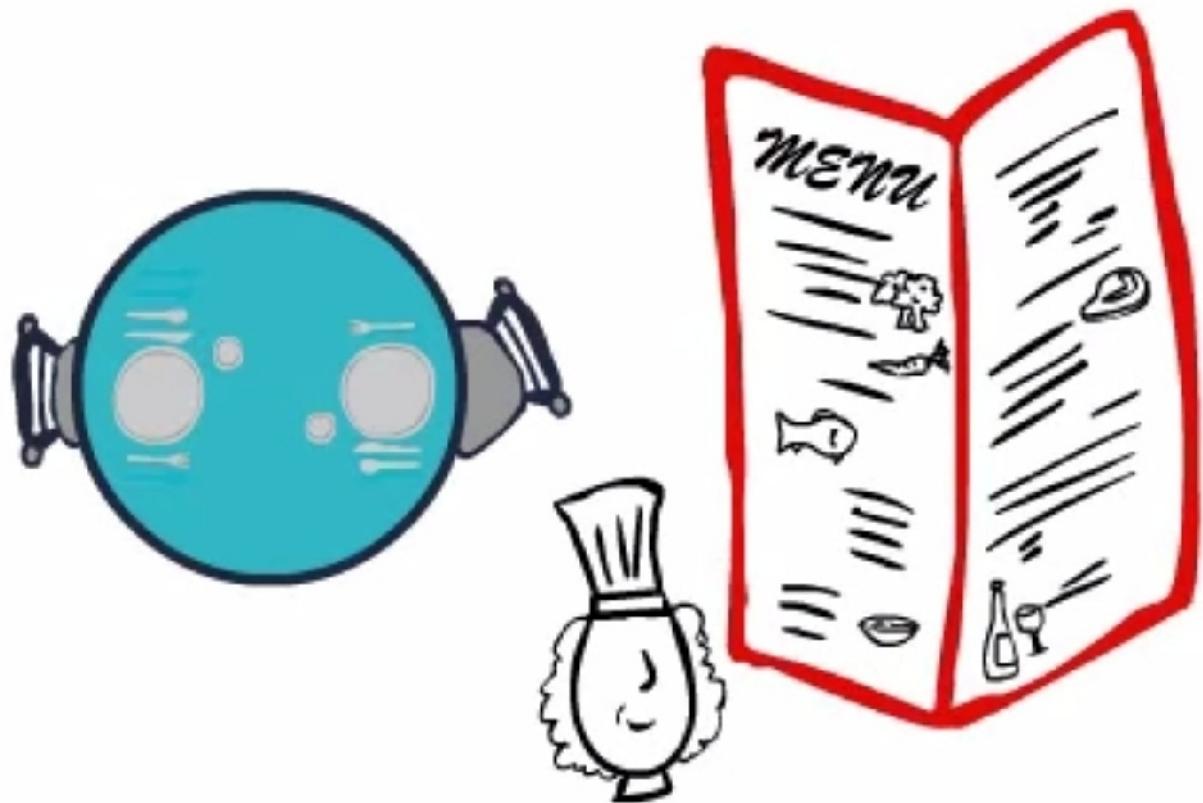
Strategic Needs

Competitive Needs & Emerging Markets

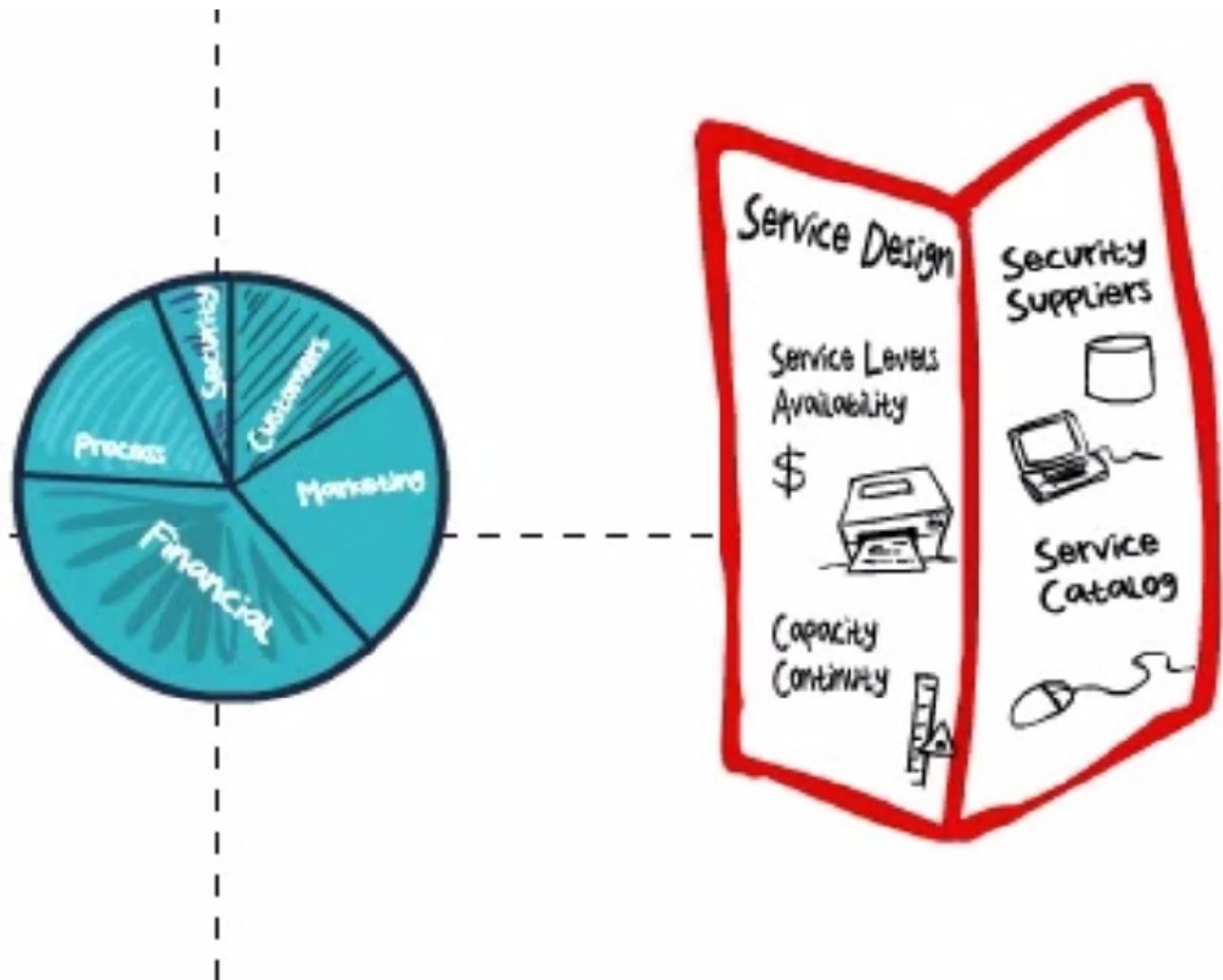
Budget Constraints



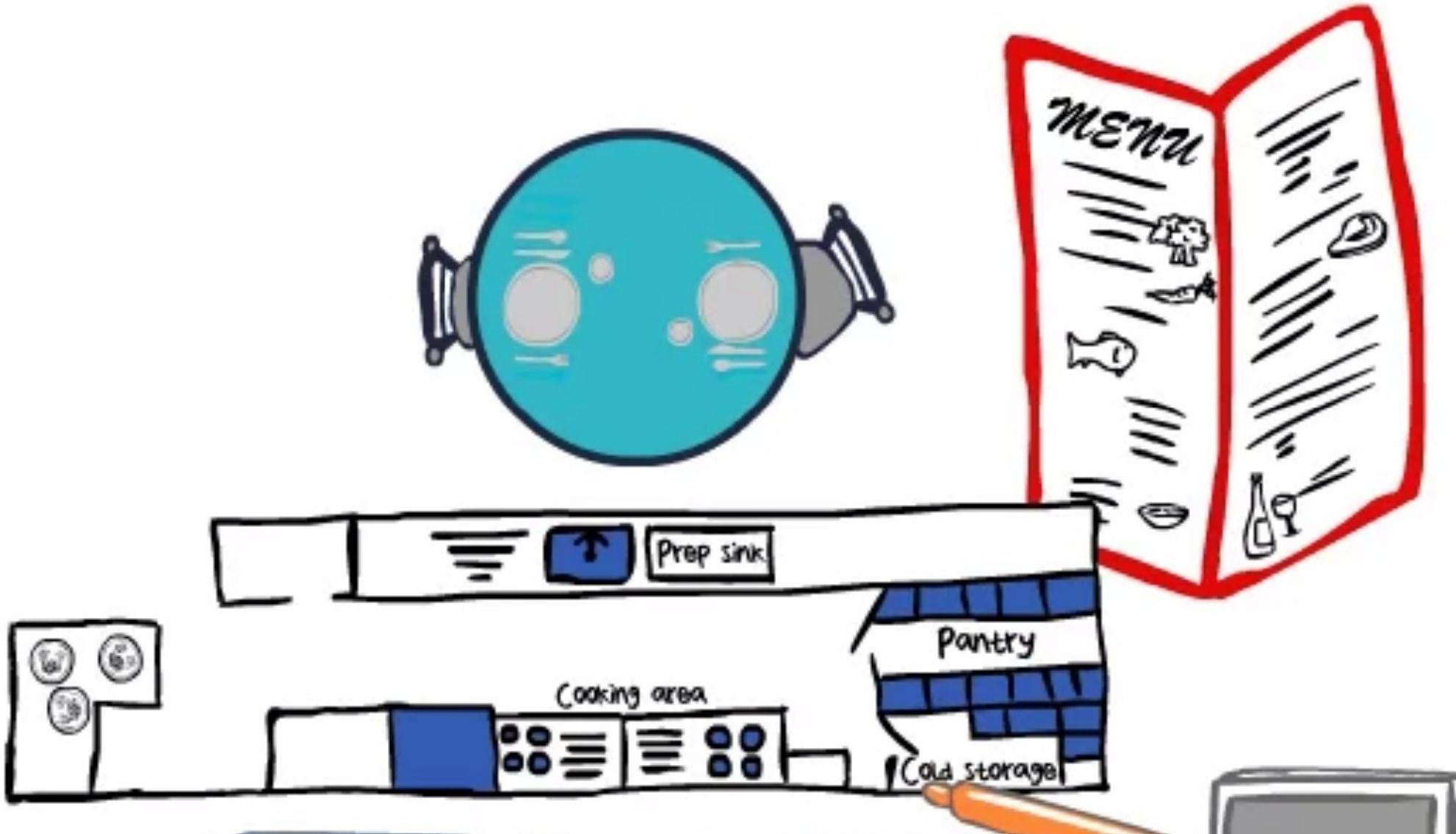
# Il fattore umano e organizzativo



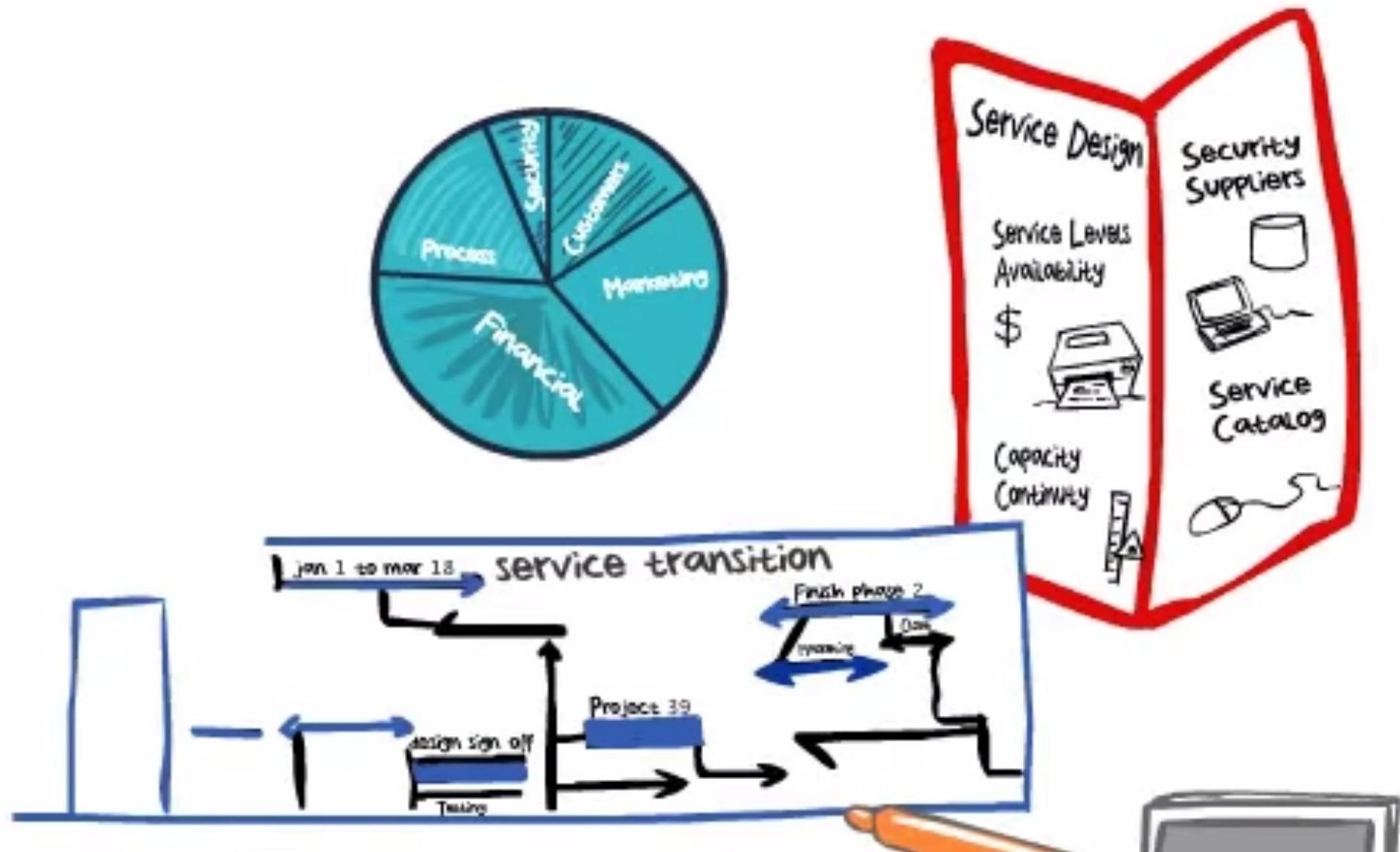
# Il fattore umano e organizzativo



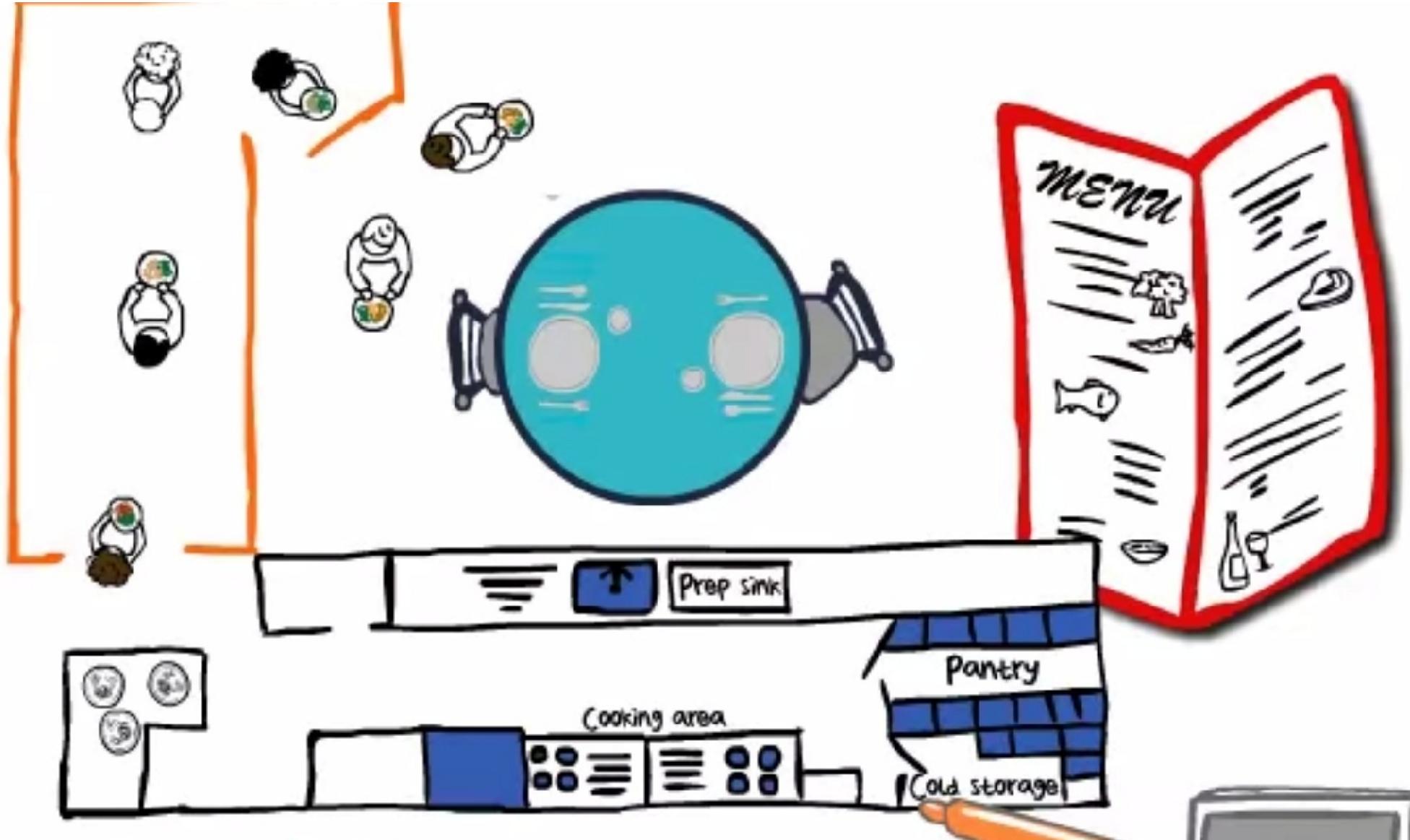
# Il fattore umano e organizzativo



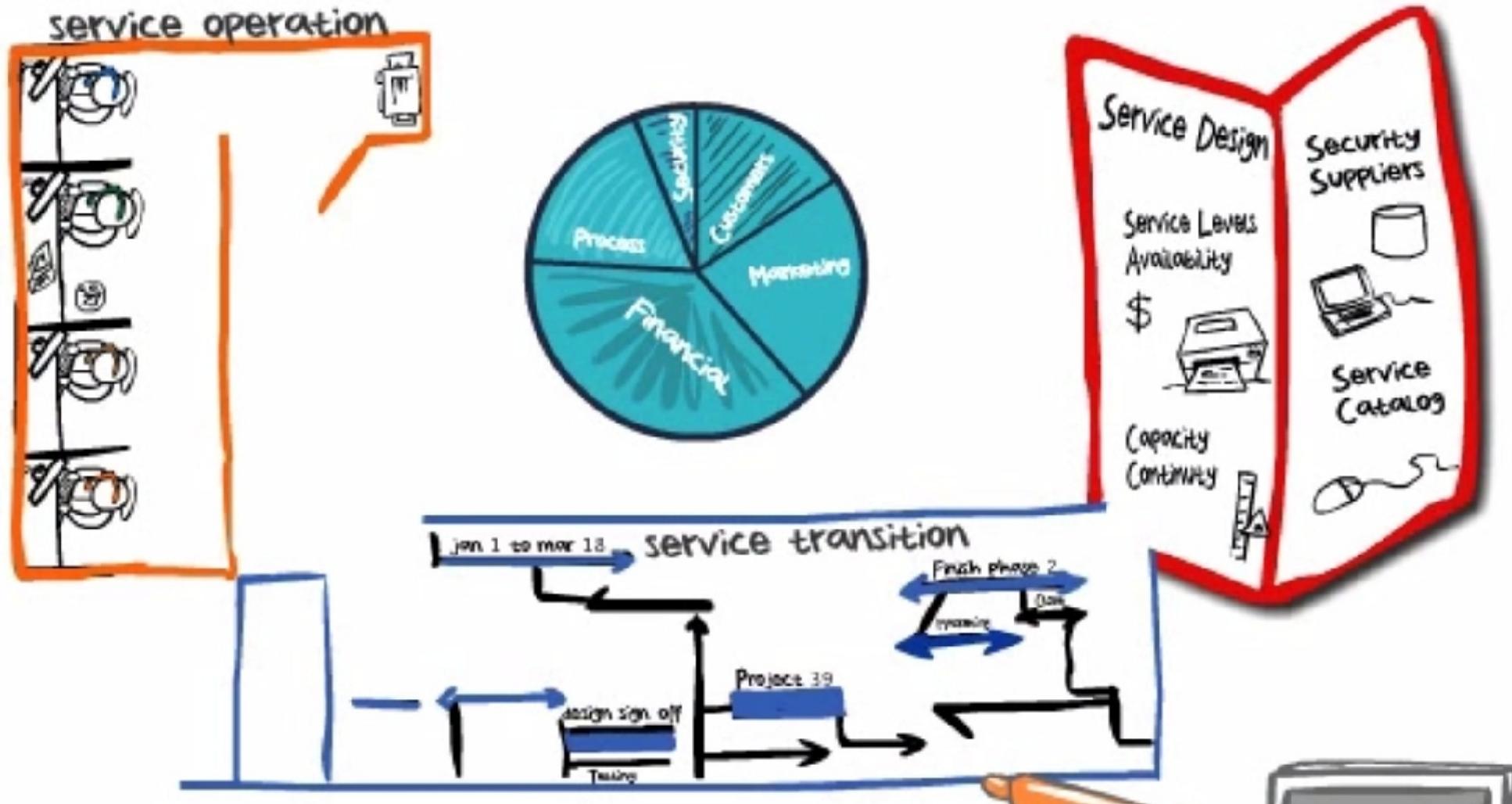
# Il fattore umano e organizzativo



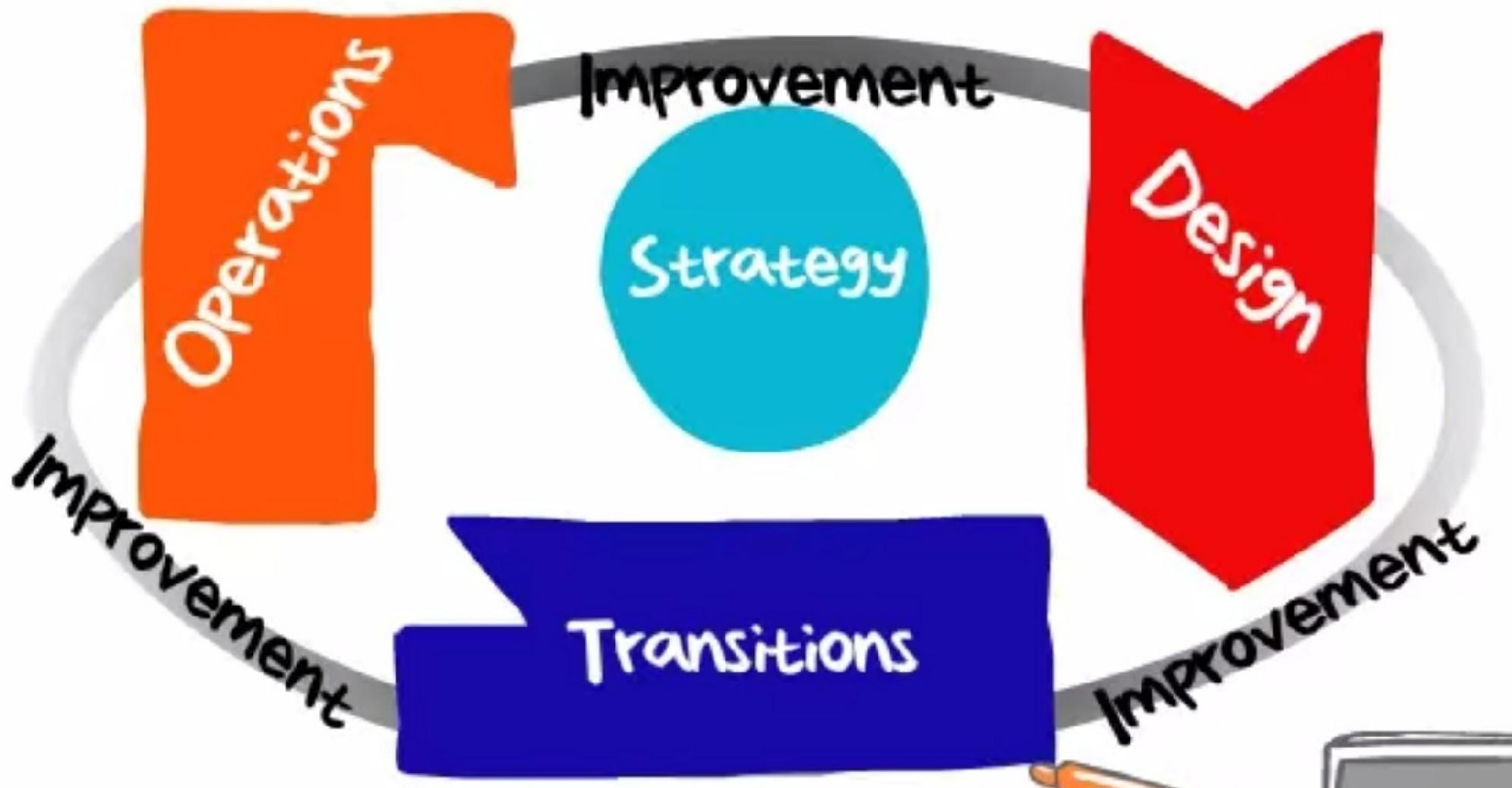
# Il fattore umano e organizzativo



# Il fattore umano e organizzativo



# Il fattore umano e organizzativo



ITIL richiede l'utilizzo di un sistema informatico di supporto alla gestione e controllo dei processi: il Data Base della Configurazione (CMDB) nel quale confluiscono le informazioni sugli elementi del sistema, sulle reciproche relazioni e sui flussi operativi.

# Il fattore umano e organizzativo



# Il fattore umano e organizzativo

