

# Corso di Amministrazione di Sistema

## Parte I – ITIL A



Francesco Clabot

Responsabile erogazione  
servizi tecnici

[francesco.clabot@netcom-srl.it](mailto:francesco.clabot@netcom-srl.it)



# Fondamenti di ITIL per la “Gestione dei Servizi Informatici”

## *IT Service Continuity Management*

# IT Continuity Management

**E' la disciplina che si occupa della perdita di servizio non prevista**

- »» Coinvolge la pianificazione di CIs alternativi
- »» Può includere un singolo CI o una intera struttura di CIs (**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

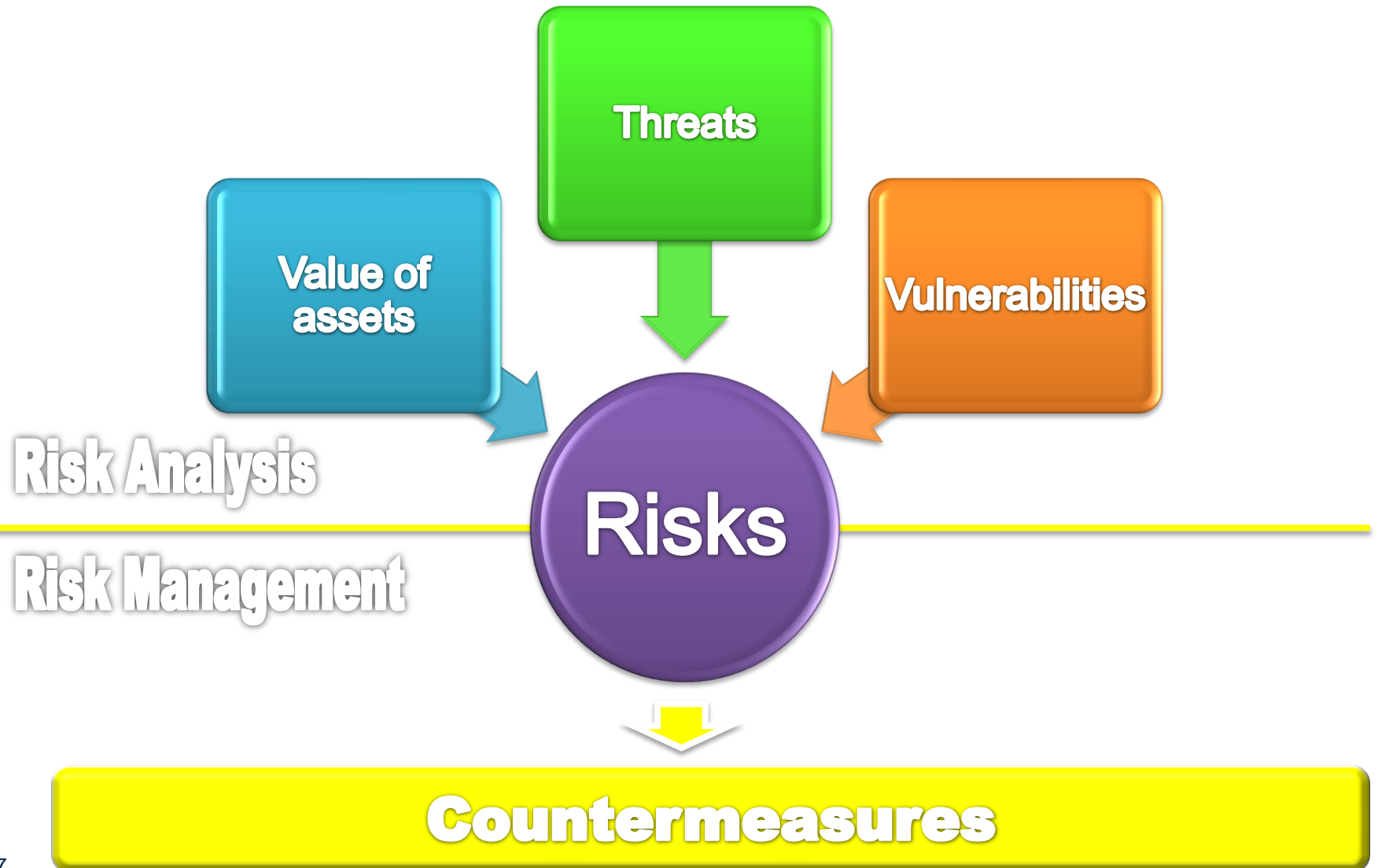
# IT Continuity Management – Perché?

- »» 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

# IT Continuity Management – Perché?

- »» 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



# Business Impact Analysis

- »» 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



# Business Impact Analysis

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**

# Business Impact Analysis

## Identificazione dei rischi. Esempi:

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

# Business Impact Analysis

## Assess Threat and Vulnerability levels

- Una minaccia dipende da vari fattori tra cui:

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

# Business Impact Analysis

## 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 – II 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

# IT Continuity Management – Il Processo

## »» 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

# IT Continuity Management – Il Processo

## »» 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

# IT Continuity Management – Il Processo

## »» 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



# IT Continuity Management – Il Processo

## »» 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

# IT Continuity Management – Il Processo

- **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 secondo quanto stabilito dai Senior Manager. Ogni modifica deve essere adeguatamente testata!



# IT Continuity Management – Il Processo

- **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



# IT Continuity Management – Le Opzioni

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



# IT Continuity Management – Le Opzioni

## »» 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

# IT Continuity Management – Le Opzioni

## »» 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)

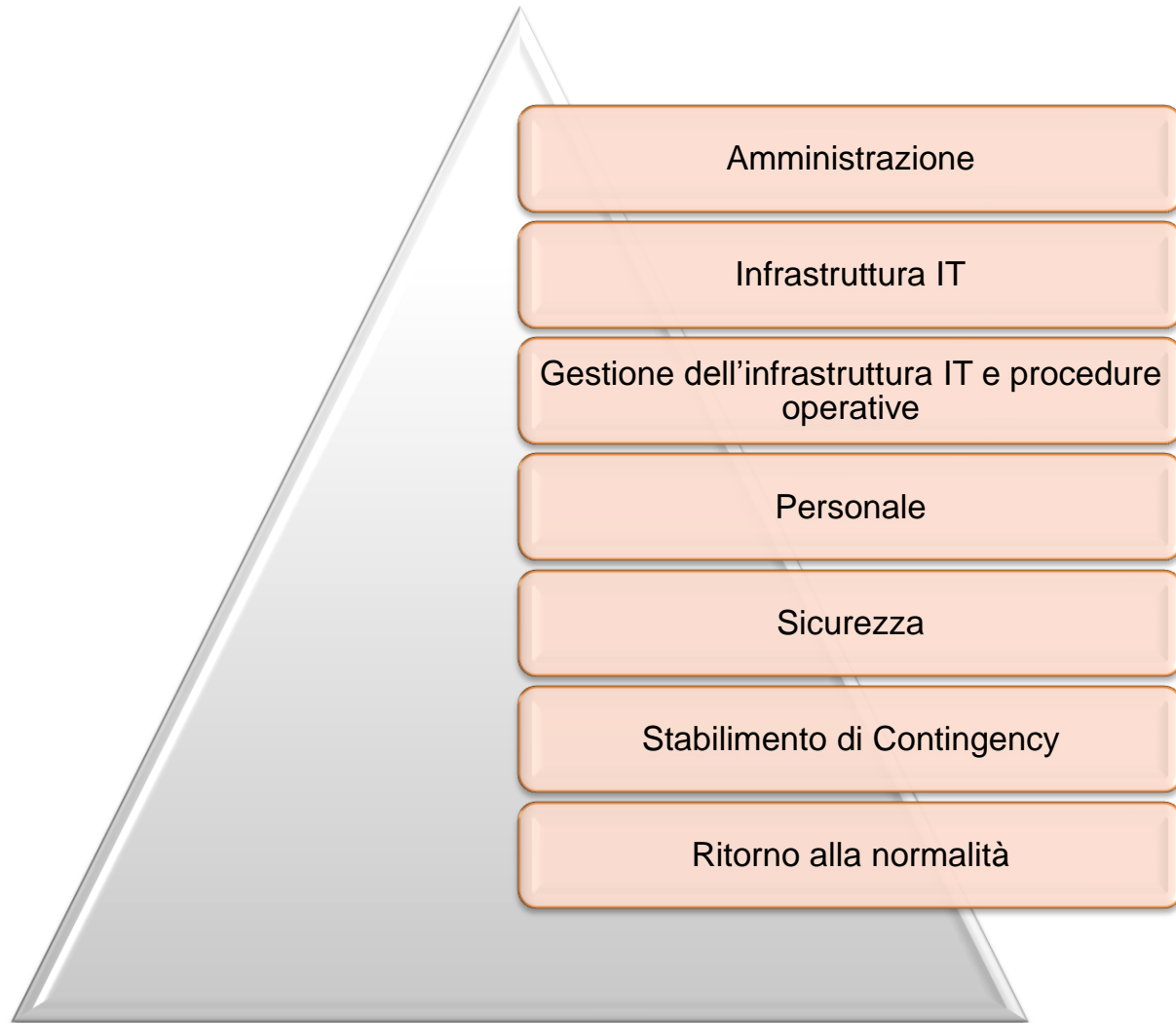
- Solitamente coinvolge il ripristino dei sistemi critici e dei servizi entro un periodo di 24 ore circa
- Può essere interna od esterna, fissa o portatile, e consiste di una struttura informativa contenente delle attrezzature di ripristino IT che possono essere configurate per supportare il business

# IT Continuity Management – Le Opzioni

## »» 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 – Le 7 sezioni del piano





# 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

# Contingency Plan – Le 7 sezioni del piano

## »» 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.

# Contingency Plan – Le 7 sezioni del piano

## »» 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

# I ruoli in situazioni normali e di crisi

<b>Normal Operation</b>	<b>In a Crisis</b>
<b>Livello Board (del Consiglio)</b>	
Avviare la Continuità dei Servizi Informatici, impostare la politica, allocare le responsabilità, indirizzare ed autorizzare	Gestione delle crisi, decisioni aziendali, affari esterni
<b>Senior Management</b>	
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
<b>Junior Management</b>	
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
<b>Supervisor e staff</b>	
Sviluppare parti da consegnare, negoziare i servizi, eseguire i test, sviluppare ed eseguire i processi e procedure	Esecuzione delle attività, partecipazione ai team, collegamenti



# I ruoli in situazioni normali e di crisi

- »» 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

# Test e revisioni esaustive

- »» 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!

# Test e revisioni esaustive

## »» 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 / CIs / Staff
- Contratti / SLAs / Contromisure / etc.

# Test e revisioni esaustive

»» 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





# Sommario

- »» Se si verifica una calamità i servizi vengono impattati
- »» Assets / Minacce / Vulnerabilità / Rischi / Contromisure
- »» Il Planning ed il design sono parte del Servizio
- »» L'IT Service Continuity Plan
  - Permette un ripristino rapido e controllato
  - Deve essere dato un accesso esteso ma controllato
  - Amministrazione, Infrastruttura, Persone, Ritorno alla Normalità
  - Opzioni (Cold, Warm and Hot StandBy)
  - Testare regolarmente – senza impattare il servizio live
- »» I vari ruoli

# Sommario

- »» L'ITSCM è uno strumento critico del business, necessario a far proseguire l'operatività nonostante i rischi esistenti
- »» Una implementazione inadeguata dell'ITSCM impatta la capacità di fronteggiare un imprevisto
- »» Le responsabilità nell'ITSCM devono essere integrate con le corrispondenti operative al fine di massimizzare le sinergie e sfruttare la conoscenza, la competenza e l'esperienza esistenti nell'ambiente operativo
- »» Il piano o i piani devono essere diffusi ma con accesso controllato ed i relativi dettagli devono essere registrati nel CMDB in quanto sono dei CIs