

Corso di Amministrazione di Sistema

Parte I – ITIL 9



Francesco Clabot

Responsabile erogazione
servizi tecnici

francesco.clabot@netcom-srl.it



Fondamenti di ITIL per la “Gestione dei Servizi Informatici”

IT Availability Management

IT Availability Management

E' una 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

Mainteinability

Resilience

IT Availability Management - Obiettivi

- »» 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

IT Availability Management - Obiettivi

- »» 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

IT Availability Management - Responsabilità

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

IT Availability Management - Responsabilità

- »» 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

IT Availability Management - Responsabilità

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

IT Availability Management - Terminologia



**Vital Business
Function**

IT Availability Management - Terminologia

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

IT Availability Management - Terminologia

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

IT Availability Management - Terminologia

Recoverability

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

IT Availability Management - Terminologia

Maintainability

- La capacità di un componente o un servizio di tornare ad uno 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

IT Availability Management - Terminologia

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

IT Availability Management - Terminologia

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

IT Availability Management - Terminologia

Security

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

IT Availability Management - Terminologia

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

Risk Analysis - CRAMM

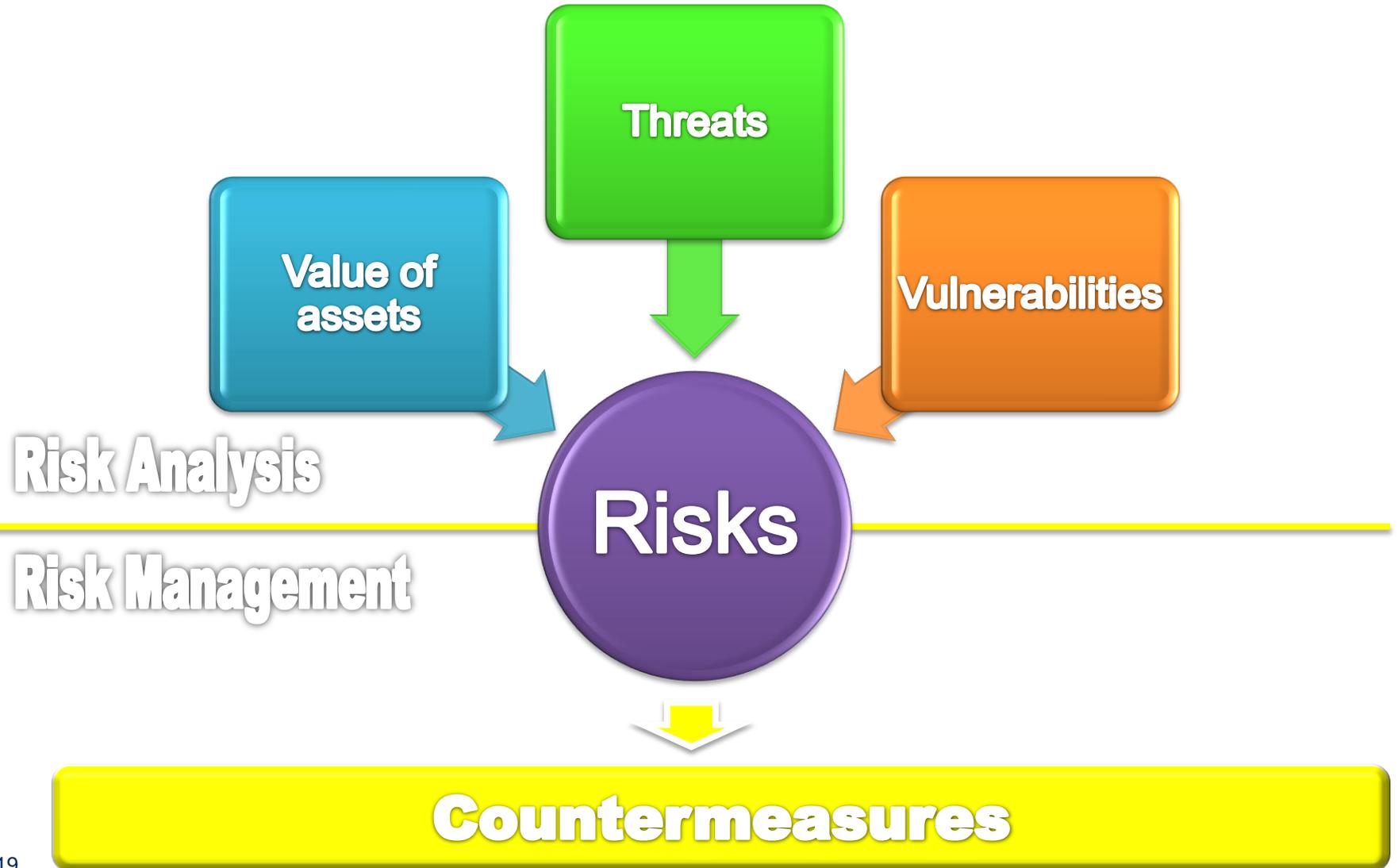
CRAMM

- **CCTA Risk Analysis and Management Method**

CCTA

- The United Kingdom's **Central Computer and Telecommunications Agency**

Risk Analysis - CRAMM



Risk Analysis - CRAMM

- »» 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

Risk Analysis - CRAMM

Almeno le seguenti attività di Risk Assessment devono essere svolte:

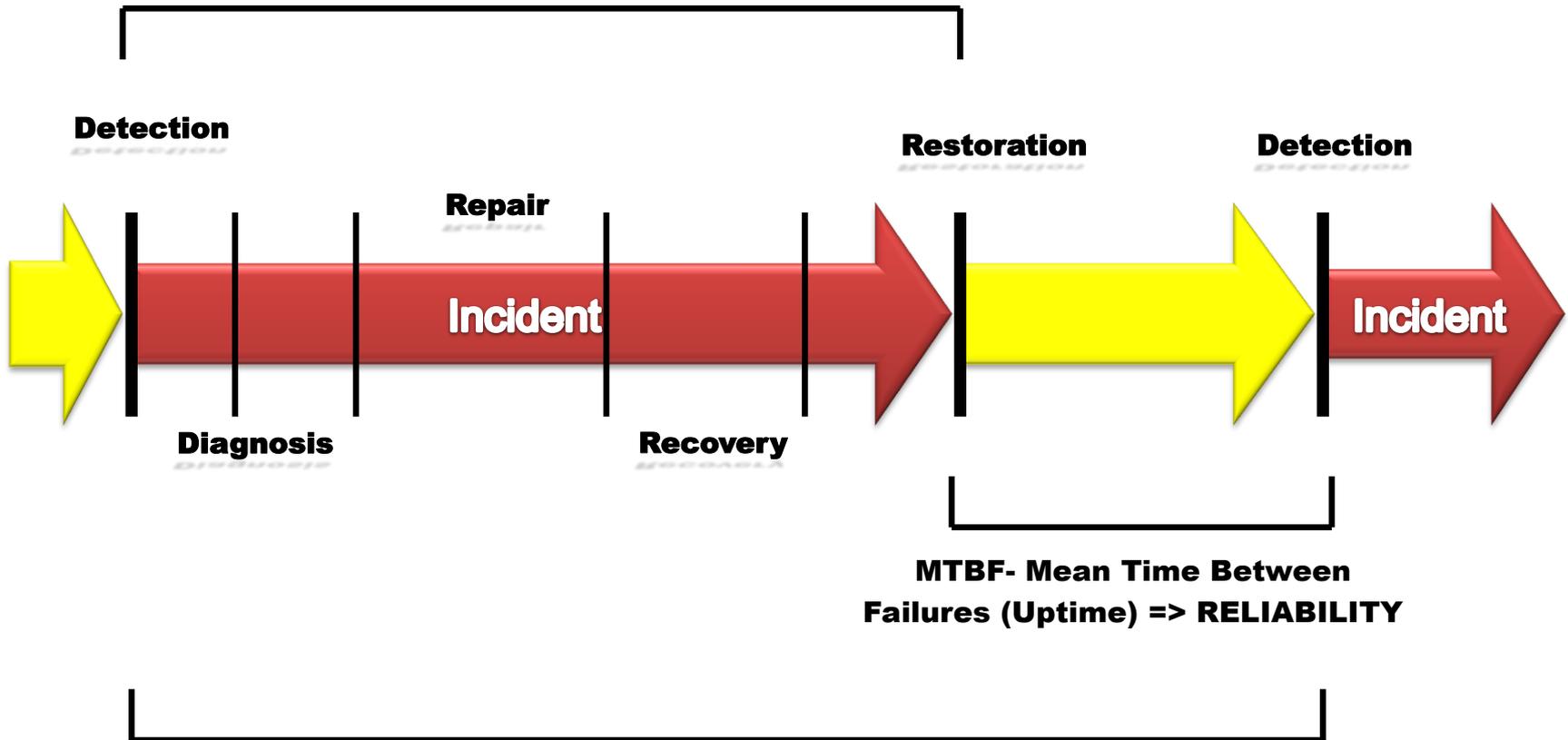
- »» Identificare i rischi, i.e. i rischi a cui è esposto un particolare componente di un servizio IT che supporta un processo di business e la cui rottura causerebbe un'interruzione del servizio
- »» Valutare le minacce e i livelli di vulnerabilità. La minaccia è la “probabilità con cui avverrà un degrado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

Risk Analysis - CRAMM

»» 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

MTTR - Mean Time to Repair (Downtime) => MAINTAINABILITY or SERVICEABILITY



Il ciclo di vita di un incidente

Durante le analisi e la pianificazione dei servizi, vengono misurati alcuni valori registrati durante le fasi che un servizio attraversa durante un problema tecnico

Si verifica un incidente

- L'utente riscontra un problema tecnico

Diagnosis

- Il servizio intraprende delle azioni per rintracciare le cause del problema tecnico

Detection

- Il servizio viene informato dell'esistenza di un problema tecnico

Reparation

- Il servizio ripara il problema

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

IT Availability Management – Le regole base

- »» 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

Quand'è che un servizio è Available?

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

Quand'è che un servizio è Available?

»» 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.

Formula dell'Availability

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

$$(A \text{ dei PC}) \times (A \text{ della rete}) \times (A \text{ dei Mainframe})$$

- »» 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

Formula dell'Availability

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

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

»» L'Availability di sistemi in parallelo si calcola

$$\begin{aligned}\text{Availability} &= 100 - (\text{A e B down}) \\ &= (100 - \text{A down}) \times (100 - \text{B down})\end{aligned}$$

IT Availability Management - Sicurezza



IT Availability Management - Sicurezza

- »» 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.

IT Availability Management - Sicurezza

- »» 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

Considerazioni sulla Sicurezza

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

Considerazioni sulla Sicurezza

- »» 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

Sommario

»» Obiettivi

- Pianificare e gestire l'Availability dei CI
- Garantire che ci siano accordi contrattuali interni e verso fornitori esterni
- Proporre Change per prevenire future perdite di servizio

»» Responsabilità

- Prevedere e definire i livelli di Availability e Sicurezza
- Availability Plan
- Raccogliere, analizzare e mantenere dati
- Monitorare i livelli di availability per garantire che siano rispettati gli SLAs e gli OLAs

Sommario

»» Valutazione del rischio – CRAMM

»» Calcolo dell'Availability

- MTBSI, MTTR, MTBF, formule varie