



APPENDICE 4 AL CAPITOLATO TECNICO DESCRIZIONE DEI PROCESSI IN USO E STATISTICHE SULL'UTILIZZO DEI SERVIZI



INDICE

1.	PREMESSA.....	3
2.	PROCESSO DI INCIDENT MANAGENT	4
2.1.	Obiettivo	4
2.2.	Input, Output, Attività	4
2.2.1.	Input.....	4
2.2.2.	Output	4
2.2.3.	Attività.....	4
3.	PROCESSO DI PROBLEM MANAGEMENT.....	6
3.1.	Obiettivo	6
3.2.	Input, Output, Attività	6
3.2.1.	Input.....	6
3.2.2.	Output	6
3.2.3.	Attività.....	6
4.	PROCESSO DI SERVICE ASSET & CONFIGURATION MANAGEMENT	7
4.1.	Obiettivo	7
4.2.	Input, Output, Attività	7
4.2.1.	Input.....	7
4.2.2.	Output	7
4.2.3.	Attività.....	7
5.	PROCESSO DI CHANGE MANAGEMENT	9
5.1.	Obiettivo	9
5.2.	Input, Output, Attività	9
5.2.1.	Input.....	9
5.2.2.	Output	9
5.2.3.	Attività.....	10
6.	PROCESSO DI RELEASE & DEPLOYMENT MANAGEMENT.....	11
6.1.	Obiettivo	11
6.2.	Input, Output, Attività	11
6.2.1.	Input.....	11
6.2.2.	Output	11
6.2.3.	Attività.....	11
7.	INFORMAZIONI SULL'UTILIZZO DEI SERVIZI	13



1. PREMESSA

Nel seguito sono riportati “sinteticamente” i processi in essere presso l’Amministrazione, gli obiettivi che si intende raggiungere con la loro applicazione, gli input, gli output e le macro attività previste.

Si precisa che:

- alla data di predisposizione del presente documento, i processi riportati nel seguito sono in corso di revisione e/o di evoluzione, così come le relative procedure operative e ruoli
- nel corso della Fornitura, è prevista l’introduzione di ulteriori processi/tool a supporto o la sostanziale evoluzione di quelli esistenti.

Ulteriori informazioni ed eventuale documentazione a corredo sono forniti a valle dell’aggiudicazione.



2. PROCESSO DI INCIDENT MANAGENT

2.1. OBIETTIVO

ITIL definisce un Incident come “Ogni evento che non rientra nella normale operatività e di un servizio e che causa, o può causare, un’interruzione o una riduzione della qualità di quel servizio”.

L’obiettivo principale del processo di Incident Management è quello di ripristinare la normale operatività del servizio più rapidamente possibile e minimizzare l’impatto sulle business operation dell’Amministrazione, in modo tale da garantire che i migliori livelli di qualità e disponibilità di servizio siano assicurati.

ITIL definisce normale operatività di servizio l’operatività del servizio nell’ambito dei limiti stabiliti dal Service Level Agreement (SLA).

2.2. INPUT, OUTPUT, ATTIVITÀ

2.2.1. Input

Gli input di questo processo possono essere:

- Descrizione generale dell’Incident fornita dal richiedente
- Dettagli dell’Incident forniti dallo Staff IT
- Ulteriori dettagli di configurazione provenienti dal Configuration Management Database (CMDB)
- Risposte alle RfC
- Status
- Utenti coinvolti
- Impatto sul servizio
- Risposta dall’Incident Matching con Problem e Known Error
- Known Error e dettagli risolutivi
- Script di risoluzione
- Dettagli risolutivi rilevati da Incidenti verificatisi in precedenza

2.2.2. Output

Gli output di questo processo sono:

- RfC per risolvere l’Incident
- aggiornamento del ticket di Incident (compresa risoluzione e/o Workaround)
- Incident risolti e chiusi
- Comunicazioni agli utenti
- Informazioni al Management (report)

2.2.3. Attività

Le attività di questo processo sono:

- Rilevazione e registrazione Incident
- Classificazione e supporto iniziale
- Investigazione e diagnosi



- Escalation funzionale/gerarchica
- Risoluzione e ripristino del servizio
- Chiusura Incident
- Ownership, monitoring, tracking e comunicazione degli Incident



3. PROCESSO DI PROBLEM MANAGEMENT

3.1. OBIETTIVO

ITIL definisce un Problem come “La causa non nota di uno o più Incident”. L’obiettivo principale del processo di Problem Management è quello di aumentare la qualità dell’infrastruttura ICT esaminando la causa originaria degli Incident accaduti o potenziali e rimuovendo in modo permanente le anomalie.

Il processo di Problem Management può essere “reattivo” o “proattivo”. E’ reattivo nel senso che i problemi possono rendersi evidenti dal moltiplicarsi degli incidenti. E’ proattivo nel senso che e’ possibile (consigliata) l’identificazione dei problemi prima che generino incidenti. La principale differenza tra Incident e Problem Management, sta nel fatto che il processo di Incident è più orientato alla continuità dei servizi IT e produce soluzioni veloci e temporanee (workaround). Il processo di Problem Management, invece, è orientato alla soluzione definitiva del Problem prevenendone future manifestazioni.

Nel rispetto di quanto detto, la rapidità con la quale una soluzione viene trovata all’interno del processo di Problem, costituisce un aspetto comunque significativo ma di secondaria importanza.

3.2. INPUT, OUTPUT, ATTIVITÀ

3.2.1. Input

Gli input a questo processo possono essere:

- Informazioni dagli Incident (Incident Database)
- Informazioni dal Configuration Management Database (CMDB)
- Configuration details dal Configuration Management Database (CMDB)
- Informazioni su workarounds prodotti (dal processo di Incident Management)
- La base di conoscenza costruita con analisi formali ed altre referenze esterne
- Informazioni scaturite dall’analisi dei trend

3.2.2. Output

Gli output di questo processo sono:

- Workarounds (per Incident Management)
- Problemi identificati
- “Known-Errors”
- Request for Change (RfC)
- Risposte agli Incident che sono affini a Problem e Known Errors
- Contribuito di qualità per altri processi ICT

3.2.3. Attività

Le attività di questo processo sono:

- Identificazione, registrazione e prioritizzazione dei Problem
- Analisi e diagnosi
- Identificazione delle cause
- Proposizione delle soluzioni
- Chiusura dei problemi
- Ownership, monitoring, tracking e comunicazione degli Incident



4. PROCESSO DI SERVICE ASSET & CONFIGURATION MANAGEMENT

4.1. OBIETTIVO

Il principale obiettivo del processo di Service Asset and Configuration Management è consentire un'economica gestione del servizio al quale è applicato, garantendone una gestione efficiente ed efficace tramite il controllo delle infrastrutture e dei servizi.

In tale ottica il Configuration Management fornisce il modello logico dell'infrastruttura e dei servizi gestiti.

Tale modello può essere tradotto nei seguenti obiettivi:

- Identificazione di tutti gli asset e delle configurazioni nell'ambito del servizio, rappresentazione della infrastruttura tramite Configuration Item (CI).
- Fornire informazioni accurate sulle configurazioni e sulla documentazione a supporto degli altri processi.
- Assicurare che siano registrati esclusivamente gli item autorizzati e identificabili, verificando che nessun CI sia aggiunto, modificato, sostituito o rimosso senza un appropriato e documentato controllo.
- Verificare la corrispondenza tra il database e l'infrastruttura attuando le eventuali correzioni.
- Costituire il CMDB quale sistema in grado di integrare differenti fonti dati e il/i CMDB come data base ufficiale delle configurazioni dei CI (configuration Item) considerati in ambito.

4.2. INPUT, OUTPUT, ATTIVITÀ

4.2.1. Input

Gli input di questo processo possono essere:

- Esternamente al processo di Configuration Management (CM)
- Richieste provenienti dal processo di Change Management e Release Management
- Internamente al processo di CM
- Esigenze di modifica emerse a fronte di audit
- Evoluzioni pianificate
- Verifiche periodiche
- Reporting periodico

4.2.2. Output

Gli output di questo processo sono:

- SACM Plan
- SACM Policy e Procedure
- Aggiornamento CMDB
- Reporting (Periodico, On demand, di Audit, etc)

4.2.3. Attività

Le attività di questo processo sono:

- Pianificazione e definizione di finalità, ambito di applicazione, livello di dettaglio, politiche e procedure del configuration management
- Identificazione: Selezione ed individuazione delle strutture di configurazione per tutti



i CI dell'infrastruttura (Inclusi: owner, relazioni, documentazione)

- Controllo: Garantire che solo CI autorizzati ed identificabili siano accettati e registrati, dalla loro introduzione fino alla dismissione. Essa garantisce che non siano aggiunti, modificati, sostituiti o rimossi CI senza un appropriato controllo documentale, ad esempio, una RFC
- Status accounting: La segnalazione di tutti i dati attuali e storici relativi a il ciclo di vita di ogni CI
- Verification and audit: Verifica dell'aderenza tra infrastruttura fisica rispetto alle informazioni registrate nel database CMDB, e verifica della coerenza della documentazione di controllo



5. PROCESSO DI CHANGE MANAGEMENT

5.1. OBIETTIVO

Una modifica comporta dei rischi ed esorta ad un approccio rigoroso nel gestirla efficacemente.

Il primo obiettivo è garantire che siano adottati metodi e procedure standardizzate per effettuare le modifiche. In questo modo è possibile minimizzare l'impatto sulla qualità del servizio e sulla continuità del business.

Nella mission, la fase di approvazione dei Change è molto rigida, al punto da implicare inflessibilità; tuttavia per piccoli change è possibile adottare vie "preferenziali" (ad esempio la richiesta di un cambio password non passa attraverso il CAB - Change Advisory Board - per ottenerne l'approvazione).

L'adozione di appropriati processi di Change Management e di Service Asset e Configuration Management consente di ridurre in modo significativo la necessità di ricorrere con frequenza a modifiche "ad hoc", tipiche - invece - di quei contesti carenti di policies adeguate.

Un'altra responsabilità è la pianificazione delle modifiche mediante l'utilizzo della SC (Schedule of Change o Calendario dei cambiamenti). Solo le modifiche pianificate e propriamente schedate possono essere efficacemente controllate poiché ciò garantisce che ci sia tempo per supervisionare il lavoro.

5.2. INPUT, OUTPUT, ATTIVITÀ

5.2.1. Input

Gli input di questo processo possono essere:

- Le RFC dalle unità di sviluppo applicativo
- Le RFC dalle unità di gestione dell'infrastruttura
- Le RFC dai processi di Incident e Problem Management
- Informazioni a supporto dal Configuration Management System Data Base (CMDB)
- Risposte sulle RFC
- Stato RFC, collegamenti con eventi IT (ad esempio Problem o Incident) e relazioni logiche all'interno del CMDB
- Utenti coinvolti
- Impatto sul servizio

5.2.2. Output

Gli output di questo processo sono:

- Change implementati
- Informazioni in input al processo di Release Management
- Informazioni in input al processo di Configuration Management
- I dati aggiornati dell'infrastruttura ICT
- Informazioni per il Management (report)
- Informazioni per il Change Owner utili alla rivisitazione del processo



5.2.3. Attività

Le attività di questo processo sono:

- Elaborare le RFC
- Autorizzare i Change
- Schedulare i Change
- Coordinare le fasi di Build and Test dei Change
- Coordinare l'implementazione dei Change
- Registrare i Change
- Revisionare i Change



6. PROCESSO DI RELEASE & DEPLOYMENT MANAGEMENT

6.1. OBIETTIVO

Il processo di Release Management assicura che gli aspetti di una Release, sia quelli tecnici che quelli legati ai processi, siano pianificati e standardizzati:

Una Release può essere definita come:

“Un insieme di Change, relativi ad un servizio IT, autorizzati, consistenti in soluzioni a problemi noti e miglioramenti al servizio. Una Release consiste del software richiesto, nuovo o modificato, e dell’hardware necessario, nuovo o modificato, ad implementare i Change approvati.”

Il Release Management lavora a stretto contatto con i processi di Change Management e Configuration Management per assicurare che il CMDBCM sia mantenuto aggiornato dei Change implementati con le nuove Release, e che il contenuto di tali Release sia salvato nella DML e del CMDB. Anche le specifiche hardware, le istruzioni di assemblaggio e le configurazioni di rete, debbono poter essere salvate all’interno della DML e del CMDB.

6.2. INPUT, OUTPUT, ATTIVITÀ

6.2.1. Input

Gli input di questo processo possono essere:

- Informazioni dal CMDB
- RFC autorizzate dal Change Management
- Policy aziendali

6.2.2. Output

Gli output di questo processo sono:

- Hardware e software distribuito e installato
- Policies relative alle Release
- Input per il Change Management
- Input per il Configuration Management: aggiornamenti delle informazioni sulle Release
- Informazioni di gestione (report)
- Informazioni per il Management (report)
- Informazioni per il Change Owner utili alla rivisitazione del processo

6.2.3. Attività

Le attività di questo processo sono:

Pianificazione e policies di Release

- Design, build e configurazione della Release
- Accettazione della Release
- Pianificazione del Rollout
- Test secondo i criteri di accettazione predefiniti
- Chiusura della Release per l’implementazione
- Comunicazione, preparazione e training
- Audit dell’hardware e del software prima e dopo l’implementazione dei Change



- Installazione del nuovo hardware o upgrade
- Salvataggio del software controllato sia nei sistemi distribuiti che nel sistema centrale



7. INFORMAZIONI SULL'UTILIZZO DEI SERVIZI

Nel seguito sono riportate alcune informazioni quantitative sull'attuale grado di utilizzo dei servizi.

Tenuto conto che ad oggi non sono stati pienamente attuati i processi di operation, il numero di **ticket di incident** riportato si stima ampiamente inferiore al complesso delle attività di carattere operativo effettuate dagli attuali fornitori.

Totale dei ticket lavorati nel 2012	24.500	100%
di cui risolti dal Service Desk	16.400	67%
di cui assegnati al team di Conduzione	1.800	7%
di cui assegnati a II livelli terzi	6.300	26%

Come detto, alla data non è disponibile alcuna infrastruttura di Contact Center; pertanto, non sono disponibili informazioni relative al numero effettivo di chiamate e alla loro durata.

In base alle informazioni relative all'apertura dei ticket, è stata stimata la % di distribuzione media delle richieste nell'arco della giornata:

% di apertura dei ticket per fascia oraria	100%
7:30 - 9:00	8%
9:01 - 10:00	11%
10:01 - 11:00	19%
11:01 - 12:00	14%
12:01 - 13:00	13%
13:01 - 14:00	7%
14:01 - 15:00	13%
15:01 - 16:00	6%
16:01 - 17:00	6%
17:01 - 18:30	2%

Peraltro, i ticket attualmente assegnati dal Service Desk ai secondi livelli (Conduzione e/o altri gruppi di supporto di fornitori terzi) sono prevalentemente riconducibili a segnalazioni/richieste effettuate dall'utenza finale afferenti il solo processo di Incident management.

Infatti, le richieste di attività afferenti altri processi (es. change, service request, etc) nonché segnalazioni di incident effettuate da utenti diversi dall'utenza finale, quali ad esempio richieste e/o segnalazioni tra gruppi tecnici di supporto, sono effettuate attraverso l'utilizzo di canali alternativi all'apertura dei ticket, prevalentemente attraverso messaggi di posta elettronica.

In particolare, si segnala che attualmente pervengono alla Conduzione circa 30 richieste di



change al giorno. Allo stato attuale, tali richieste potrebbero essere classificate “change non standard”; si stima che a tendere, anche attraverso le attività effettuate dal Fornitore del Lotto 2, il 90-95% di tali richieste ricadranno tra i “change standard”.

Inoltre, si segnala che attualmente, in caso di eventi segnalati dal Sistema di monitoraggio dei servizi, non è resa obbligatoria l’apertura dei ticket di incident da parte della Conduzione.

Di conseguenza, con la piena attuazione dei processi, il volume delle richieste/segnalazioni pervenute al Service Desk (Lotto 1) già nel primo anno della fornitura potrebbe superare ampiamente le 30.000 mentre il numero di ticket di competenza della Conduzione (Lotto 2) potrebbe essere ampiamente superiore a 10.000.