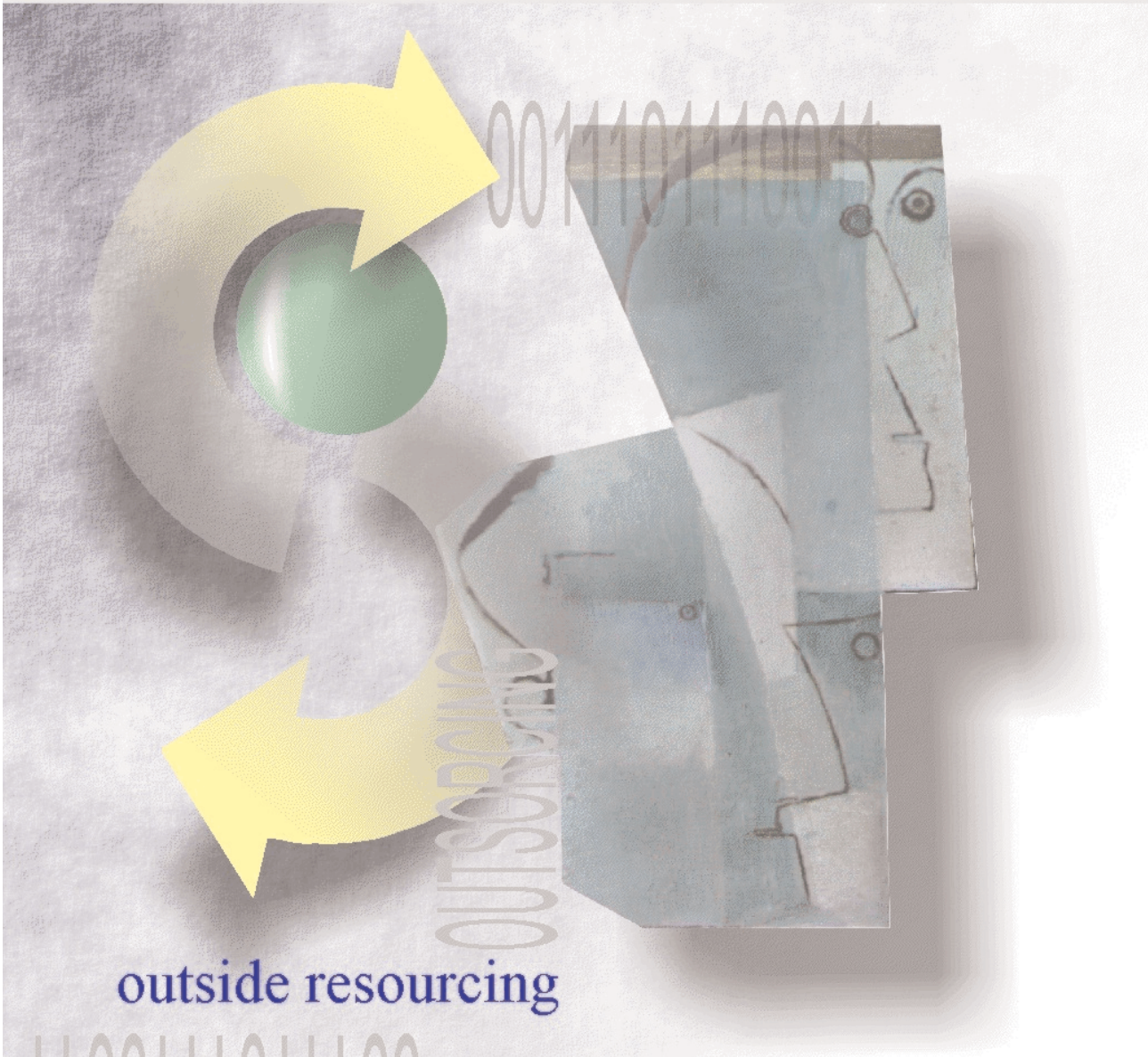
Ministero delle Comunicazioni

ISCOM
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

OUTSOURCING E SICUREZZA



Linee Guida ISCOM

Istituto Superiore delle Comunicazioni
e delle Tecnologie dell'Informazione
Ministero delle Comunicazioni

Outsourcing e sicurezza

Il presente documento è stato realizzato da:

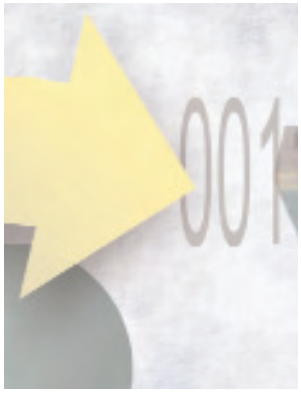
Elena Agresti	INNOVIA
Giovanni D'Amato	INNOVIA
Marcella Di Domenico	SIEMENS
Alessandro Di Nepi	ISCOM (Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione)
Vincenzo Di Turi	SIEMENS
Luisa Franchina	ISCOM (Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione)
Ivan Gaudenzi	ENEL
Clara Isola	RAI
Matteo La Speme	SIEMENS
Paolino Madotto	PROGESOFTWARE
Maurizio Mayer	AICT
Andrea Mercurio	FINSIEL
Walter Narisoni	SOPHOS
Fabio Pacchiarotti	GETRONICS
Daniele Perucchini	FONDAZIONE UGO BORDONI
Massimo Piccirilli	MINISTERO DELLE COMUNICAZIONI
Gianluigi Pugni	ENEL
Andrea Rigoni	SYMANTEC
Stefano Spagnoli	GRTN/AIEA
Enzo Tieghi	VISION AUTOMATION

Copertina e Progetto Grafico: Roberto Piraino
(Graphics Lab - Istituto Superiore
delle Comunicazioni e delle Tecnologie dell'Informazione)

Le opinioni e le considerazioni espresse in questo volume, nonchè le proposte avanzate, sono da considerarsi come personali dei singoli partecipanti e non riflettono necessariamente la posizione dei rispettivi Enti e Società d'appartenenza.
Il contenuto del presente volume è da considerarsi unicamente come studio tecnico/scientifico orientativo delle problematiche inerenti la sicurezza delle reti e la tutela delle comunicazioni.
Pertanto nessuna responsabilità potrà essere attribuita agli autori o all'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione, che cura questa pubblicazione, per ogni eventuale conseguenza derivante da qualsivoglia utilizzo dei contenuti del presente testo.

Le citazioni di specifici marchi o nomi di prodotti presenti nel documento sono riportati a mero scopo esemplificativo, non esauriscono il novero di prodotti esistenti sul mercato e in nessun caso costituiscono elemento di valutazione o di raccomandazione per l'utilizzo dei prodotti stessi.

Indice



Indice delle figure e delle tabelle

INDICE DELLE FIGURE

INDICE DELLE TABELLE

1 - Introduzione

La presente pubblicazione si inquadra in una serie di attività svolte da un gruppo di esperti volontari appartenenti al settore pubblico e privato nel 2005 e relative alla realizzazione di linee guida su:

Gestione delle emergenze locali

Risk analysis approfondimenti

Qualità del servizio su UMTS

Qualità dei servizi per le PMI su reti fisse a larga banda

Outsourcing e sicurezza

Certificazione della sicurezza ICT

Si coglie volentieri l'occasione per ringraziare quanti hanno, con entusiasmo e professionalità, collaborato alla redazione del presente documento:

Elena Agresti (INNOVIA), Giovanni D'Amato (INNOVIA), Marcella Di Domenico (SIEMENS), Alessandro Di Nepi (ISCOM), Vincenzo Di Turi (SIEMENS), Ivan Gaudenzi (ENEL), Clara Isola (RAI Way), Matteo La Speme (SIEMENS), Paolino Madotto (PROGESOFTWARE), Maurizio Mayer (AICT), Andrea Mercurio (FINSIEL), Walter Narisoni (SOPHOS), Fabio Pacchiarotti (GETRONICS), Daniele Perucchini (FUB), Massimo Piccirilli (Ministero delle Comunicazioni), Gianluigi Pugni (ENEL), Andrea Rigoni (SYMANTEC), Stefano Spagnoli (GRTN AIEA), Enzo Tieghi (VISION AUTOMATION).

Si ringraziano ancora, per il loro apporto e i loro suggerimenti:

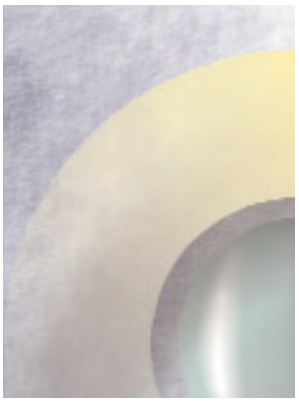
Alfredo Albano (RESI ASSOTEL), Fabio Battelli (SYMANTEC), Davide Braccini (ABI), Stefano Bruschini (EDS), Roberta Bruzzone (ICAA), Roberto D'Alicandro (CAPGEMINI), Sebastiano D'Amore (PWC), Maria Dattoli (TERNA), Tobia Del Vecchio (BANKSIEL), Anna Di Benedetto (BANKSIEL), Silvio Fantin (GRTN), Giovanni Fassina (POSTE ITALIANE), Franca Fico (Ministero dell'Interno), Massimo Giacomini (Ministero del Tesoro), Federico Grimaldi (SIEMENS), Alberto Gusella (PWC), Simona Napoli (KPMG), Massimo Panichelli (ANCITEL), Mauro Parmagnani (IMQ), Nicola Pergola (IBM), Rodolfo Perugino (POSTE ITALIANE), Sergio Petronzi (INPROTEC), Claudia Piccolo (IMQ), Alfredo Polizzi (SUN), Stefano Quintarelli (iNET),

Giuseppe Russo (SUN), Alberto Sarti (FINMECCANICA), Giuliano Serafini (FINSIEL), Guido Tripaldi (iNET), Alfredo Valenza (ORACLE), Carlo Veneri (RESI), Marco Vernetti (RAI).

Roma, luglio 2006

Il Direttore
dell'Istituto Superiore delle Comunicazioni
e delle Tecnologie dell'Informazione

Ing. Luisa Franchina



2 - Guida alla lettura

Il fenomeno dell'outsourcing, come viene in gergo indicato l'affidamento di servizi di un'azienda ad un'entità esterna, ha acquisito negli ultimi anni una notevole importanza per due principali fattori:

- da una parte alcune tipologie di servizi, tipicamente quelli ICT, costituiscono un bene primario anche per quelle aziende il cui core business non è propriamente legato a quel mondo;

- d'altra parte, per aziende il cui core business non sia quello dei servizi in oggetto è sconveniente, nonché inefficiente, tenere personale ed infrastrutture per la messa in opera, la gestione e la manutenzione di tali servizi.

Si pensi ad esempio ad un'azienda tessile che vuole comunque avere e gestire un'infrastruttura informatica per fornire servizi di messaggistica email verso i propri clienti ed i propri fornitori. Piuttosto che investire in personale ed infrastrutture per la gestione del servizio email, che non costituisce il bene primario dell'azienda, conviene affidare quel servizio ad una terza parte il cui core business è proprio la gestione della messaggistica online. Il costo per l'affidamento a terzi di tale servizio sarà minore di quello di messa in opera e mantenimento del servizio in-house con risultati sicuramente migliori.

L'outsourcing apre però delle problematiche che non sono presenti quando la gestione dei servizi avviene internamente: sempre

riferendosi all'esempio dell'azienda tessile che vuole dotarsi di una piattaforma di messaggistica, chi assicura tale azienda che il provider del sistema di email rispetti, ad esempio, la privacy dei dati trattati?

Lo scopo del presente documento è quindi quello di evidenziare e fornire delle linee guida di carattere generale per gestire le problematiche di sicurezza nell'affidamento a terzi di alcuni dei servizi di un'azienda.

Piuttosto che elencare pedissequamente tutte le possibili classi di servizi evidenziando per ognuna di esse le problematiche relative all'outsourcing di tali servizi, abbiamo deciso di raggruppare in macroclassi alcuni tra i servizi oggi di maggior interesse, mettendo insieme quelli che presentano modalità simili nella gestione degli aspetti di sicurezza.

Ciò risulta sicuramente non esaustivo, ovvero non offre un'indicazione su ogni tipo di servizio possibile, ma offre comunque un'ampia panoramica su come improntare un rapporto di outsourcing per molte classi di servizi. Vista comunque la continua evoluzione del panorama dei servizi disponibili, tale elenco "completo" sarebbe comunque limitativo nel giro di breve tempo. D'altra parte un elenco esaustivo dei servizi oggi presenti è riportato nel catalogo CNIPA [CNIPA01] a cui rimandiamo per eventuali approfondimenti.

La linea guida apre offrendo un'ampia panoramica, nel paragrafo 3.2, delle principali "best practice" oggi presenti in letteratura per la gestione esterna di servizi:

- ISO27001 e ISO17799
- ITIL
- COBIT

Le diverse metodologie vengono poi messe a confronto per evidenziare similitudini e differenti approcci proposti nell'affrontare l'outsourcing.

Nell'ottica illustrata precedentemente, partendo dalla lista dei servizi individuati dal CNIPA, nel paragrafo 3.3, proponiamo la

macro-classificazione dei servizi di maggiore interesse, rispetto agli aspetti di sicurezza che tali servizi pongono.

Nel capitolo 4, viene introdotto un modello di controllo generale per l'affidamento a terzi dei servizi appartenenti a tali macro-classi, fornendo una panoramica delle modalità di selezione, valutazione e contrattualizzazione dell'outsourcer.

Successivamente, nel capitolo 5, si analizzano i requisiti generali in termini contrattuali e di SLA che hanno una valenza trasversale rispetto alla macro-classificazione effettuata.

Il capitolo termina con esempio di reale applicazione delle metodologie illustrate, prendendo in considerazione l'outsourcing dei servizi di telecomunicazioni. Tale esempio, sebbene riferito al campo TLC (area a cui appartengono gli autori della presente linea guida), mostra la metodologia generale che andrebbe seguita nel definire il rapporto di outsourcing. Partendo da uno SLA generale (come quello mostrato nel capitolo 5) bisogna identificare ed associare le clausole di proprio interesse sulla base del prototipo di una o più macroclassi di servizio (paragrafo 3.3) a cui appartiene l'oggetto della fornitura.

3 - Generalità

3.1 Introduzione

La politica di "gestione esterna", (attraverso contratti di outsourcing) dei servizi di vario tipo, che ha caratterizzato negli anni passati la filosofia di gestione stessa delle imprese, sta vedendo un momento di riflessione e di ripensamento sulle valutazioni in merito alle opportunità di "esternalizzare" alcune delle attività funzionali dell'azienda.

Si deve rilevare che anche il mercato americano, che era stato il primo a ricorrere alle strategie di outsourcing ed aveva fatto scuola in merito all'argomento, sta attraversando un momento di riflessione sull'opportunità e la convenienza di ricorrere a tali strumenti di gestione ed in particolare modo sulla politica dell'outsourcing.

Le considerazioni generiche che si possono fare sull'opportunità di "esportare" conoscenze e valori che, in quasi tutti i casi, rappresentano parte del patrimonio dell'azienda presso altri soggetti, inducono quanto meno, ad una più attenta riflessione e valutazione di tutti i vantaggi contrapposti agli eventuali svantaggi che ne potrebbero derivare.

Le precedenti linea guida ISCOM, [ISCOM01] e [ISCOM02], invitavano a compiere un attento esame dei "valori" dell'azienda da proteggere, pertanto è probabile che molti lettori possano essere stati già indotti e indirizzati ad una più corretta politica di gestione della sicurezza.

3.1.1 Valutazione ed analisi del rischio

L'esito di quest'analisi del rischio è da condurre a delle scelte (Gestione del rischio): censiti i beni, viste le minacce e le vulnerabilità, analizzate le ragioni che potrebbero muovere degli attaccanti, esaminati costi e benefici delle possibili contromisure, si scelgono quelle contromisure che si reputano idonee ad evitare e/o ridurre il rischio. Quindi non tutte le contromisure identificate devono essere adottate.

Esse possono essere meno rigorose per ragioni di costo o di fattibilità. Il rischio aumenterà ma nell'ottica costo/beneficio sarà un rischio accettabile. Il punto fondamentale è quello di prevedere almeno una contromisura per ogni attacco sferrato su un bene considerato "di valore" per il sistema.

Vale la pena ricordare il principio secondo cui non esiste la sicurezza totale. Saranno sempre possibili attacchi che superano le contromisure adottate, ma anche quegli attacchi hanno un costo. Per disincentivarli è normalmente sufficiente che costino di più del beneficio che si ottiene perpetrandoli con successo.

Ancora più importante e determinante, quindi, è il caso in cui si debba riflettere, su servizi che sono collegati alla gestione della sicurezza.

Non si può cedere alla tentazione di delegare tutte le attività che in apparenza possono apparire poco rilevanti, all'esterno.

Il primo impatto, se il progetto di valutazione ha seguito un iter corretto, è che qualsiasi contratto di gestione di servizi (anche se si sono seguite tutte le indicazioni per ottenere un adeguato

"SLA" (Service Level Agreement) o "OLA" (Operation Level Agreement) richiede una risorsa di gestione e controllo (altamente specialistica) interna.

Tale prerogativa non può essere "esternalizzata" per ovvi motivi, che assumono aspetti rilevanti e inderogabili nel caso della gestione dei servizi riconducibili alla sicurezza.

Non può sfuggire che, alcuni aspetti dei servizi che in una prima superficiale analisi possono apparire come un peso per l'azienda, sono in realtà delle opportunità di arricchimento del patrimonio aziendale.

Quanto detto non va interpretato nel senso che non si deve usufruire dei servizi esterni, ma solo che l'utilizzo di tale strumento deve essere in ogni caso vagliato e valutato in tutti i suoi aspetti.

3.2 Best Practice

3.2.1 ISO27001 e ISO17799

Nella direttiva ISO27001 si fa riferimento ai servizi esterni mediante i controlli riportati in Tabella 1

Obbiettivo: fornire una gestione nella direzione e nel supporto per la sicurezza informatica in accordo con i requisiti aziendali e con le leggi in vigore e le regolamentazioni piu' rilevanti	
Politica di sicurezza informatica	Controllo Un documento di politica di sicurezza informatica deve essere approvato dalla direzione, pubblicato e comunicato a tutti gli impiegati ed alle parti esterne più rilevanti.

Tabella 1: Politiche di sicurezza informatica

A tal riguardo si possono fare i seguenti commenti:

- l'Organizzazione che si avvale di servizi esterni deve aver elaborato una politica di sicurezza interna e deve comunicarla alle parti esterne (nel nostro caso agli outsourcer) affinché essi possano rispettarla;

- questo controllo impone, di fatto, l'individuazione di tutti i controlli che devono essere realizzati dall'outsourcer. Occorrerà, quindi, ripercorrere tutti i controlli previsti nella ISO27001 e specializzarli per l'outsourcer;

- nel caso l'Organizzazione non abbia una politica di sicurezza formalizzata, è sempre necessario esplicitare anche in modo non formale (cioè, anche senza rispettare pienamente le best practice tipo la ISO27001 e la ISO17799) una politica di sicurezza parziale e relativa almeno alle parti di interesse nel rapporto di outsourcing;

- la totale assenza di una politica di sicurezza, espressa in modo formale o informale, rende impossibile imporre all'outsourcer il rispetto di regole che non esistono.

La normativa ISO17799 riporta le seguenti guide all'implementazione.

Il documento contenente le politiche di gestione della sicurezza deve specificare gli obblighi del management e fissare l'approccio dell'organizzazione nella gestione della sicurezza informatica.

Tale documento dovrebbe contenere delle dichiarazioni riguardo:

- Una definizione di sicurezza informatica, i suoi obbiettivi ed ambiti di utilizzo e l'importanza della sicurezza come meccanismo abilitante per la condivisione delle informazioni;

- Uno statuto di gestione delle intenzioni che supporti gli obbiettivi ed i principi di sicurezza informatica in linea con le strategie e gli obbiettivi aziendali;

- Un quadro di lavoro per la pianificazione degli obbiettivi e controlli che includa la struttura di valutazione e gestione dei rischi;

- Una breve spiegazione delle politiche, dei principi, degli standard e requisiti di conformità in ambito sicurezza di particolare importanza per l'organizzazione che includa:

- Conformità ai requisiti legislativi, alla regolamentazione e al contratto;

- Educazione e tutoraggio in materia di sicurezza e consapevolezza dei requisiti;

- Gestione della business continuity;

- Conseguenza delle violazioni alle politiche di sicurezza informatica;

- Una definizione delle responsabilità generali e specifiche per la gestione della sicurezza informatica che includano i resoconti degli incidenti di sicurezza informatica;

- Riferimenti alla documentazione di supporto, come ad esempio dettagliate politiche di supporto e procedure di sicurezza per specifici sistemi informativi o regole di sicurezza a cui l'utente dovrebbe conformarsi.

Questa politica di sicurezza informatica dovrebbe essere comunicata attraverso l'organizzazione a tutti gli utenti in una forma che è rilevante, accessibile e di facile comprensione per l'interlocutore a cui è destinata.

La politica di sicurezza informatica può essere parte di un documento più generale di politiche aziendali. Maggiori informazioni possono essere trovate nella normativa ISO/IEC TR 13335.

Riguardo alla Tabella 2, punto 2.1 possiamo commentare quanto segue:

Il ricorso a un outsourcer può esporre l'Organizzazione a nuovi rischi che non sarebbero stati presenti altrimenti. Questa circostanza richiede che venga effettuata un'analisi dei rischi supplementare e l'individuazione di contromisure, tecniche e non tecniche, aggiuntive.

Obbiettivo: Mantenere la sicurezza delle informazioni dell'organizzazione e delle sedi di elaborazione delle informazioni che sono accedute, processate, comunicate o gestite da parti esterne.		
2.1	Identificazione dei rischi legati alle parti esterne.	Controllo I rischi ai dati dell'organizzazione ed alle sedi di elaborazione degli stessi derivati dal processamento che coinvolge parti esterne devono essere identificat i ed appropriati controlli devono essere messi in atto prima di garantire l'accesso a tal i dati e/o sedi.
2.2	Gestione della sicurezza nel rapporto col cliente.	Controllo Tutti i requisiti di sicurezza identificati devono essere gestiti prima di dare accesso al cliente alle sedi o alle informazioni dell'organizzazione.
2.3	Gestione della sicurezza negli accordi con terze parti.	Controllo Accordi con terze parti sull'accesso, l'elaborazione, la comunicazione, la gestione delle informazioni dell'organizzazione o delle relative sedi di elaborazione o l'aggiunta di prodotti o servizi al processo informativo devono coprire tutti i rilevanti requisiti di sicurezza.

Tabella 2: Fornitori esterni

Nella normativa ISO17799 si trova:

Guida all'implementazione

Quando c'è una necessità di permettere ad una organizzazione esterna l'accesso alle informazioni o procedure di una organizzazione, deve essere fatta una valutazione dei rischi in modo da identificare ogni requisito per controlli specifici. L'identificazione dei rischi legati all'accesso di organizzazioni esterne deve tenere in conto le seguenti questioni:

1) Le risorse a cui l'organizzazione esterna ha bisogno di accedere
2) Il tipo di accesso che avrà l'organizzazione esterna, ad esempio:
    a) Accesso fisico: uffici, stanze dei computer, schedari, etc.;

b) Accesso logico: database dell'organizzazione, sistemi informativi;

c) Se l'accesso avverrà localmente o in remoto.

3) Il valore e la sensibilità delle informazioni coinvolte, nonché il grado di criticità per le operazioni dell'organizzazione;

4) I controlli necessari alla protezione delle informazioni che non sono destinate ad essere accessibili da parti esterne;

5) Il personale delle organizzazioni esterne coinvolte nel tratta mento delle informazioni dell'organizzazione;

6) Come identificare il personale autorizzato all'accesso e la relativa verifica di autorizzazione nonché quanto spesso tale autorizzazione debba essere riconfermata;

7) I differenti mezzi e controlli effettuati dall'organizzazione esterna nell'immagazzinamento, elaborazione, comunicazio ne, condivisione e scambio di informazioni;

8) L'impatto di una indisponibilità per l'organizzazione esterna e della fornitura/ricezione di informazioni fallaci;

9) Pratiche e procedure da trattare per incidenti di sicurezza informatica e potenziali danni; termini e condizioni per la continuità dell'accesso dell'organizzazione esterna in caso di tali incidenti;

10) Requisiti legali e regolamentazioni ed altri obblighi contrat tuali rilevanti per l'organizzazione esterna che devono essere tenuti in conto;

11) Come gli interessi di qualsiasi altro stakeholder possono essere affetti dall'accordo.

L'accesso dell'organizzazione esterna alle informazioni interne non deve essere fornito fino a che appropriati controlli siano stati effettuati e, ove possibile, è stato firmato un contratto che definisca termini e condizioni per la connessione o l'accesso e le disposizioni di lavoro.

Generalmente, tutti i requisiti di sicurezza risultanti dal lavoro

con organizzazione esterne o controlli interni devono essere contenuti nell'accordo con l'organizzazione esterna (si veda anche i commenti alle parti 2.2 e 2.3).

Deve essere assicurato che l'organizzazione esterna è consapevole dei suoi obblighi e accetta le responsabilità legate all'accesso, all'elaborazione, alla comunicazione o gestione delle informazioni dell'organizzazione.

Le informazioni possono essere messe a rischio dall'organizzazione esterna con una gestione inadeguata della sicurezza. Adeguati controlli devono essere identificati ed applicati nell'amministrazione degli accessi alle sedi di elaborazione delle informazioni da parte dell'organizzazione esterna. Per esempio, se c'è una speciale necessità per la confidenzialità delle informazioni, può essere usato efficacemente un accordo di non divulgazione.

Laddove si abbia un elevato livello di outsourcing o siano coinvolti diversi fornitori esterni, le organizzazioni possono trovarsi di fronte a rischi associati ai processi, alla gestione ed alle comunicazioni fra organizzazioni diverse.

Sempre facendo riferimento alla Tabella 3, passando al punto 2.2 possiamo commentare quanto segue:

Il controllo si riferisce agli utenti che accedono alle informazioni o ai beni dell'Organizzazione e prescrive che l'Organizzazione deve affrontare e risolvere tutti i problemi di sicurezza prima di concedere il suddetto accesso. Questa prescrizione, oltre che agli utenti finali propriamente intesi di un servizio fornito dall'Organizzazione, si applica anche a quei servizi di outsourcing (ad esempio, i servizi di data entry) che prevedono l'utilizzo da parte dell'outsourcer di servizi realizzati da altri.

Nella normativa ISO17799 si trova:

I controlli 2.2 e 2.3 coprono differenti intese con organizzazioni esterne, tra cui:

1) Service provider come ISP (Internet Service Provider), Operatori di rete, servizi di fonia, servizi di supporto e manutenzione;

2) Servizi di gestione della sicurezza;
3) Clienti;
4) Outsourcing di sedi e/o operazioni, come sistemi IT, servizi di data collection, operazioni di call center;
5) Consulenti e revisori di gestione e amministrazione;
6) Sviluppatori e fornitori, di prodotti software e sistemi IT;
7) Pulizia, catering e altri servizi di supporto dati in outsourcing;
8) Personale temporaneo, studenti ed altri appuntamenti a breve termine;

Tali accordi possono aiutare nel ridurre i rischi associati con le parti esterne all'organizzazione.

Guida all'implementazione.

I seguenti termini dovrebbero essere considerati per assicurare la sicurezza prima di dare accesso ai clienti ad ogni tipo di bene dell'organizzazione (alcune clausole potrebbero non applicarsi a seconda del tipo e dell'estensione dell'accesso):

1) Protezione dei beni, includendo:

a) Procedure di protezione dei beni dell'organizzazione, informazioni e software, nonché gestione delle vulnerabilità note;

b) Procedure per la determinazione di eventuali compromis sioni dei beni dell'organizzazione, come ad es. perdita o modifica dei dati;

c) Integrità;

d) Restrizioni sulla copia o divulgazione delle informazioni.

2) Descrizione del prodotto o del servizio da fornire;
3) Motivi, requisiti e benefici per l'accesso del cliente;

4) Politiche di controllo dell'accesso, che trattino:

   a) Metodi di accesso permesso e controllo ed uso di identifi catori univoci quali user ID e password;

   b) Un processo di autorizzazione per l'accesso dell'utente e la gestione dei suoi privilegi;

   c) Uno statuto che vieti ogni accesso non esplicitamente autorizzato;

   d) Un processo di revoca dei diritti d'accesso o di interruzione della connessione tra sistemi

5) Disposizioni per la rendicontazione, la notifica e l'investigazione di informazioni non accurate (ad es. dettagli personali), incidenti di sicurezza informatica e breccia nei sistemi di sicurezza;

6) Una descrizione di ciascun servizio che deve essere reso disponibile;

7) Il livello ottimale e la soglia di non accettabilità di un servizio;

8) Il diritto a monitorare, revocare ed a tutte le attività relative ai beni dell'organizzazione;

9) I rispettivi diritti dell'organizzazione e del cliente;

10) Le responsabilità rispetto alla materia legale e come assicura re che i requisiti legali sono rispettati; ad es. legislazione sulla protezione dei dati, specialmente tenendo conto dei differenti sistemi legislativi nazionali se gli accordi coinvolgono cooperazioni tra organizzazioni in paesi diversi;

11) Diritti di proprietà intellettuale e assegnazione del copyright e protezione di ogni lavoro collaborativo.

I requisiti di sicurezza legati all'accesso di clienti ai beni dell'organizzazione possono variare considerevolmente a seconda dell'informazione e della sua sede di elaborazione. Questi requisiti di sicurezza possono essere regolati con accordi con l'utente che contengano tutti i rischi identificati ed i requisiti di sicurezza

(vedi commenti fatti a 2.1).

Accordi con organizzazioni esterne possono anche prevedere altre parti coinvolte.

Accordi che garantiscono l'accesso ad organizzazioni esterne dovrebbero includere la possibilità di designazione di altre organizzazioni idonee e le condizioni per il loro accesso e coinvolgimento.

Da ultimo riguardo il punto 2.3 della Tabella 3, possiamo commentare quanto segue:

Questo controllo stabilisce, di fatto, le modalità di stesura dei contratti di outsourcing che devono contemplare il rispetto di tutti i requisiti di sicurezza individuati mediante l'analisi dei rischi.

Nella normativa ISO17799 si trova:

Guida all'implementazione.

L'accordo deve assicurare l'assenza di incomprensioni tra l'organizzazione e terze parti. Le organizzazioni coinvolte devono adempiere ai loro obblighi ed eventuali indennizzi verso terze parti.

I seguenti termini devono essere considerati nell'accordo allo scopo di soddisfare i requisisti di sicurezza identifica ti (vedi 2.1):

1) Le politiche di sicurezza informatica;
2) I controlli necessari ad assicurare la protezione dei beni, includendo:
3) Le procedure per la protezione dei beni dell'organizzazione, includendo informazioni, software e hardware;
4) Le procedure per determinare una eventuale compromis sione dei beni, come ad esempio il verificarsi di perdita o modifica di informazioni, software e hardware;
5) Il controllo per assicurare la restituzione o la distruzione

delle informazioni e dei beni alla fine dell'accordo, o ad un punto concordato nel tempo;

6) Confidenzialità, integrità, disponibilità e ogni altra proprietà rilevante dei beni;

7) Restrizioni sulla copia e divulgazione di informazioni e uso di accordi di confidenzialità;

8) Descrizione del prodotto o del servizio da proteggere;

9) Istruzione di utenti ed amministratori nei metodi, procedure e sicurezza;

10) Assicurare la consapevolezza dell'utente nelle responsabilità e problematiche connesse alla sicurezza informatica;

11) Provvedere al trasferimento del personale, dove appropriato;

12) Responsabilità circa installazione e manutenzione di hardware e software;

13) Una struttura chiara di reporting con formati concordati;

14) Una chiara e specificata struttura di gestione delle modifiche;

15) Ogni controllo e meccanismo richiesto per assicurare la protezione fisica;

16) Controlli per assicurare la protezione contro software malevolo

17) Una politica di controllo degli accessi che copra:

    a) Le differenti ragioni, requisiti e benefici che rendono necessario l'accesso alle terze parti;

    b) I metodi di accesso permessi ed il controllo e l'uso di identificatori univoci come username e password;

    c) Un processo di autorizzazione per l'accesso degli utenti e la gestione dei privilegi;

    d) Il requisito a mantenere una lista di individui autorizzati all'uso dei servizi e ai relativi diritti e privilegi

rispetto al loro uso;

e) Una dichiarazione che vieti tutti gli accessi non esplicitamente autorizzati

f) Un processo di revoca dei diritti di accesso o interruzione della connessione tra sistemi

18) Disposizioni per la rendicontazione, la notifica e l'investigazione di informazioni non accurate (ad es. dettagli personali), incidenti di sicurezza informatica e breccia nei sistemi di sicurezza;

19) Una descrizione di ciascun servizio che deve essere reso disponibile insieme alla sua classificazione rispetto alla sicurezza;

20) Il livello ottimale e la soglia di non accettabilità di un servizio;

21) Il diritto a monitorare, revocare ed a tutte le attività relative ai beni dell'organizzazione;

22) Il diritto a revisionare le responsabilità definite nell'accordo, ad avere queste revisioni compiute da terze parti e ad enumerare i diritti legali degli auditori;

23) L'istituzione di un processo di escalation per la risoluzione dei problemi;

24) Requisiti per la continuità del servizio, includendo misure per la disponibilità ed affidabilità in accordo con le priorità commerciali dell'organizzazione;

25) I rispettivi obblighi delle parti coinvolte nell'accordo;

26) Le responsabilità in materia legale e come viene assicurato che tali requisiti legali vengano rispettati; ad es. legislazione sulla protezione dei dati, specialmente tenendo conto dei differenti sistemi legislativi nazionali se gli accordi coinvolgono cooperazioni tra organizzazioni in paesi diversi;

27) Diritti di proprietà intellettuale e assegnazione del copy-

right e protezione di ogni lavoro collaborativo;

28) Coinvolgimento di terze parti con sub-fornitori ed i con trolli di sicurezza che tali sub-fornitori devono mettere in pratica;

29) Le condizioni per la rinegoziazione/terminazione del l'accordo:

a) Un piano di contingency che deve essere messo in pratica in caso una delle parti desideri terminare la relazione prima della fine dell'accordo;

b) La rinegoziazione degli accordi nel caso di modifiche ai requisiti di sicurezza dell'organizzazione

c) Documentazione corrente della lista dei beni, licenze, accordi o diritti legati ad essi

L'accordo può variare considerevolmente per differenti organizzazioni e tra differenti tipi di terze parti coinvolte. Conseguentemente, una speciale cura deve essere presa per includere tutti i rischi identificati ed i requisiti di sicurezza nell'accordo. Quando necessario, i controlli e le procedure richieste possono essere estese ad un piano di gestione della sicurezza.

Se la gestione della sicurezza informatica viene data in outsourcing, gli accordi devono mirare ad esplicitare come l'organizzazione esterna garantirà che un adeguata sicurezza, come definita nell'analisi dei rischi, sarà mantenuta e come tale sicurezza sarà adattata ad identificare e trattare cambiamenti nei rischi.

Alcune delle differenze tra l'outsourcing e le altre forme di forniture di servizi da parte di terze parti include aspetti di obblighi legali, pianificazione del periodo di transizione e potenziali interruzioni delle operazioni durante questo periodo, accordi di pianificazione della contingency e revisioni della normale diligenza, raccolta e gestione delle informazioni sugli incidenti di sicurezza.

In quest'ottica è molto importante che un'organizzazione pianifichi e gestisca le transizioni ad una situazione di outsourcing e abbia appropriati processi per maneggiare cambiamenti e la rinegoziazione/terminazione degli accordi.

Le procedure per la continuità del processo nel momento in cui il fornitore esterno non è più in grado di erogare il suo servizio devono essere concordate a priori in modo da evitare ritardi nel disporre servizi di sostituzione.

Accordi con terze parti possono anche prevedere altre organizzazioni.

Accordi che garantiscono l'accesso ad organizzazioni esterne dovrebbero includere la possibilità di designazione di altre organizzazioni idonee e le condizioni per il loro accesso e coinvolgimento.

Generalmente gli accordi sono principalmente sviluppati da organizzazioni. Ci possono essere occasioni in alcune circostanze dove un accordo può essere sviluppato ed imposto su un'organizzazione da una terza parte.

L'organizzazione ha bisogno di garantire che la sua sicurezza non sia impattata da requisiti di terze parti stipulati in accordi imposti.

3.2.2 ITIL

L'economia della conoscenza presuppone che l'informazione venga considerata come la risorsa strategica più importante che ogni organizzazione si trova a dover gestire. La chiave per la raccolta, l'analisi, la produzione e l'utilizzo delle informazioni all'interno di un'organizzazione è la qualità (intesa come la capacità di disporre in ogni momento delle risorse alla massima efficienza ed efficacia) dei sistemi ICT e dei servizi IT forniti al business. I sistemi ICT sono dunque un patrimonio cruciale e strategico dell'organizzazione e pertanto le organizzazioni investono elevate risorse nel supporto, nell'erogazione e nella gestione dei servizi IT. Tuttavia, molto spesso questi aspetti dell'IT sono trascurati o

trattati superficialmente. Una scarsa cultura manageriale di molti CIO li porta ad investire tempo e risorse su soluzioni tecnologiche (sul "cosa") e sui progetti senza tenere con la dovuta attenzione processi, persone e culture in grado di perseguire gli obbiettivi in modo efficace ed efficiente (il "come").

L'ITIL (IT Infrastructure Library) fornisce un quadro di lavoro composto da linee guida che raccolgono le "best practice" per l'IT Service Management ed è l'approccio più utilizzato ed accettato al mondo per l'IT Service Management.

La qualità dei servizi IT può essere raggiunta perseguendo il rispetto dei requisiti e delle aspettative del Cliente in ogni momento. In particolare ITIL adotta un modello fondato sulla figura del Cliente (interno o esterno) e del fornitore (anch'esso interno o esterno). L'ITIL fa di questo il pilastro principale della gestione dei servizi, definendo un numero di processi chiave che sono vitali per il successo dei processi ITIL all'interno di questa area, quali:

1) Documentare, negoziare e concordare gli obiettivi di qualità e le responsabilità del Cliente e dei Fornitori nei Service Level Agreements (SLA);

2) Indagini regolari dell'opinione del Cliente attraverso ricerche di Customer Satisfaction;

3) Far propria da parte del Fornitore IT la visione del business del Cliente;

4) Perseguire costantemente la costruzione di un rapporto aperto e cordiale con il Cliente;

5) Avere una forte attenzione sia sugli aspetti tecnici ma soprattutto al governo dell'organizzazione dei servizi e alla cultura aziendale.

L'ITIL riconosce che non c'è nessuna soluzione universale per la progettazione e l'implementazione di un processo per la gestione e l'erogazione di servizi IT di qualità. L'ITIL nasce dal contributo di molte esperienze e best practice nate all'interno

delle aziende ed il risultato che ne è scaturito è un modello che fornisce un approccio strutturato e basato sul "buon senso" verso i principali processi coinvolti. ITIL è stato pensato per essere guidato dai processi, in un modo scalabile e sufficientemente flessibile da potersi adattare ad ogni organizzazione dalle PMI alle organizzazioni multinazionali. Ogni Fornitore di un servizio IT (interno o di terze parti) dovrebbe adottare le linee guida, i principi, e i concetti di ITIL ed adattarli al proprio ambiente secondo un principio guida "adotta ed adatta".

Pertanto, i processi IT devono essere sviluppati basandosi sulla loro capacità di erogare veri benefici al business. La sola maniera di raggiungere questo è quella di progettare, pianificare ed implementare i servizi IT utilizzando tecnologie e processi di gestione in grado di mettere a disposizione le informazioni e le soluzioni richieste dal business. Secondo un approccio top-down si parte innanzitutto progettando i ruoli delle persone, i ruoli dei partner ed i processi e poi configurano la tecnologia per supportare ed automatizzarli.

L'ITIL fornisce delle linee guida per le "best practice" ed per le architetture al fine di assicurare che i processi IT siano strettamente allineati ai processi di business e che l'IT eroghi le corrette ed appropriate soluzioni di business. ITIL non è uno standard, né una regola o una norma e pertanto nessuno strumento, processo o persona può essere definita "conforme ad ITIL (o ITIL compliant)". I processi e le organizzazioni possono essere confrontate con il BS 15000(ISO20000), lo standard di IT Service Management. Comunque, nessuno strumento o individuo può essere certificato BS 15000.

Uno dei principali obiettivi di ITIL è quello di assistere le organizzazioni fornitrici di servizi IT "nel migliorare l'efficacia e l'efficienza IT contemporaneamente al miglioramento della qualità del servizio per il business all'interno di determinati vincoli di costo", come recitano le descrizioni di ITIL presenti nelle linee guida. Gli specifici obiettivi dell'IT sono quelli di realizzare e mantenere i servizi che:

- Sviluppino e mantengano delle relazioni buone e sappiano rispondere efficacemente alle richieste del business;

- Soddisfino le richieste IT esistenti da parte del business;

- Siano all'interno di un ciclo di miglioramento continuo che consenta di far fronte alle future necessità, con una attenzione ai costi e ai tempi;

- Rendano efficace ed efficiente l'utilizzo di tutte le risorse (persone, processi e tecnologie);

- Contribuiscano al miglioramento della qualità totale dell'organizzazione al fine di proteggere la conoscenza aziendale e la sua competitività.

I benefici raggiunti da molte organizzazioni IT attraverso l'implementazione di ITIL e dei processi basati sulle linee guida delle sue "best practice" sono:

- Miglioramento continuo nell'erogazione di servizi IT di qualità;

- Un notevole incremento della sicurezza dei servizi IT;

- Riduzione dei costi di lungo termine attraverso un miglioramento del ROI o la riduzione del TCO per mezzo dell'ottimizzazione dei processi;

- Una migliore rappresentazione del valore aggiunto derivato dall'investimento economico in IT;

- Riduzione del rischi di non raggiungere gli obiettivi di business, attraverso l'erogazione di servizi di livello costante e di alta affidabilità;

- Un miglioramento delle comunicazioni e migliori relazioni di lavoro fra l'IT ed il business;

- Capacità di adattamento maggiore ai cambiamenti imposti dal business con un tasso di successo migliorato e misurabile;

- Benchmarking di processi e procedure che possono essere valutate per la loro conformità alle linee guida "best practice";

- Migliorata capacità di reagire e adattarsi alle acquisizioni, alle fusioni e all'outsourcing.

Esempi di alcuni risparmi fatti dalle organizzazioni includono:

- Riduzione di oltre il 70% nel fermo dei servizi;

- ROI aumentato sino ad oltre il 1000%;

- Riduzione del 50% sul ciclo di sviluppo e messa in produzione di nuovi prodotti/servizi.

Quando si sviluppa l'IT Service Management all'interno di una organizzazione è facile fraintendere percependo ed interpretando ITIL come voluminoso, burocratico. E' importante invece che ITIL venga implementato con un approccio "adotta ed adatta", in modo che siano realizzati processi appropriati ed efficaci. Ciò può essere raggiunto da una parte definendo metriche, Critical Success Factors (CSF) e Key Performance Indicator (KPI) ispirati dal business, dall'altra attraverso una forte attenzione alle risorse umane a disposizione, alla cultura aziendale, alla gestione del cambiamento organizzativo. L'approccio "adotta e adatta" consente anche di affrontare meglio lo scoglio di introdurre nuovi processi organizzativi in una cultura aziendale consolidata, di permettere alle organizzazioni di mantenere il sufficiente grado di diversità necessario per competere tra loro.

La qualità e la misura della qualità, in termini di business, è un altro principio fondamentale di ITIL.

L'ITIL fornisce delle linee guida di "best practice" complete per tutti gli aspetti della gestione dei servizi "a 360 gradi" e si occupa dell'intero spettro delle persone, dei processi, dei prodotti e dell'utilizzo dei partner. ITIL è stato inizialmente progettato e sviluppato negli anni '80 dall'ente governativo inglese che si occupava di tecnologie informatiche e delle telecomunicazioni, oggi è stato recentemente rivisto ed aggiornato per essere allineato con le moderne pratiche, architetture distribuite ed internet fino a diventare l'approccio più diffuso al mondo, per la gestione dell'erogazione e del supporto dei servizi e dell'infrastruttura IT. La

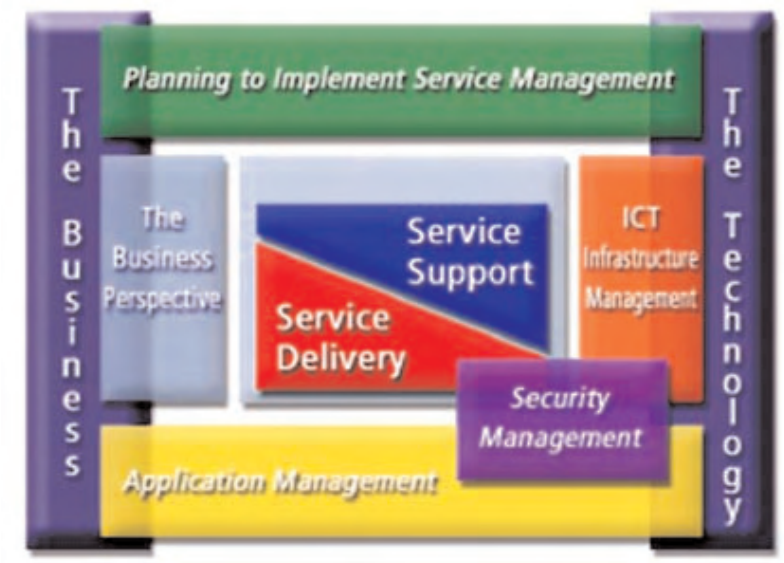


Figura 1: La struttura di ITIL

struttura di ITIL si compone di vari moduli così come rappresentato in Figura 1.

- Erogazione Servizi (Service Delivery): comprende i processi richiesti per la pianificazione e l'erogazione di servizi IT, si occupa degli aspetti di pianificazione e governo dell'erogazione del servizio.

- Supporto Servizi (Service Support): descrive i processi associati con il supporto e le attività di manutenzione quotidiane associate con la fornitura dei servizi IT.

- Gestione Infrastruttura ICT (ICT Infrastructure Management): comprende tutti gli aspetti della gestione dell'infrastruttura tecnologica, dall'architettura, ai processi di acquisto, al test di accettazione, all'installazione, alla messa in funzione, all'operatività e all'ottimizzazione dei componenti ICT.

- Pianificazione dello Sviluppo della Gestione Servizi (Planning to Implement Service Management): esamina i problemi e le attività coinvolte nella pianificazione, implementazione e miglioramento

dei processi di Service Management all'interno di una organizzazione. Esso indirizza anche i problemi associati con i cambiamenti culturali ed organizzativi (Cultural and Organizational Change), lo sviluppo di una visione, la strategia ed il più appropriato metodo di approccio.

- Gestione delle Applicazioni (Application Management): descrive come sviluppare le applicazioni partendo dalla gestione della domanda di business, attraverso tutte le fasi nel ciclo di vita di una applicazione, fino alla sua dismissione. Pone enfasi sull'assicurare che i progetti e le strategie IT siano fortemente allineate.

- La Prospettiva Aziendale (The Business Perspective): supporta la funzione IT a comprendere come possa contribuire al raggiungimento degli obiettivi di business e come il suo ruolo possa essere utilizzato per massimizzare i risultati aziendali.

- Gestione della Sicurezza (Security Management): dettaglia il processo di pianificazione e gestione del livello di sicurezza per le informazioni ed i servizi IT, inclusi tutti gli aspetti relativi alla reazione agli incidenti di sicurezza. Include anche la valutazione e la gestione dei rischi e delle vulnerabilità, e l'implementazione delle contromisure a costi giustificabili. Sotto l'aspetto della sicurezza, ITIL rappresenta un valido strumento per adeguare l'organizzazione alle specifiche della BS7799/ISO27001.

ITIL è un tassello fondamentale per un'organizzazione IT che voglia uscire dall'ambito artigianale di processi ad hoc e non ripetibili per andare verso un governo manageriale dei servizi di business basati sulle tecnologie IT. ITIL si inquadra facilmente in un quadro di lavoro più ampio che vede COBIT dal punto di vista della governance e BS7799/ISO27001 dal punto di vista della gestione integrata del sistema delle informazioni aziendali.

3.2.3 COBIT

Il COBIT (Control Objectives for Information and related Technology), è un quadro di lavoro sviluppato da ISACA, e da IT Governance Institute per dare un aiuto alle organizzazioni nel

gestire i rischi dell'IT e assicurare che i processi IT siano coerenti con gli obiettivi di Business dell'azienda.

La prima definizione del framework COBIT si è avuta nel 1994; in seguito l'applicazione degli standard internazionali, delle linee guida e delle ricerche nell'ambito delle "best practice" ha portato allo sviluppo degli "obiettivi di controllo". Infine sono state sviluppate le "Audit Guideline" per valutare se l'implementazione degli obiettivi di controllo è effettuata in maniera appropriata. Grazie alle ricerche ed agli studi effettuati per la prima e la seconda edizione (1998), sono state possibili la collezione e l'analisi delle fonti internazionali; tali ricerche sono state condotte in Europa (la libera università di Amsterdam in Olanda), in USA (il politecnico della California) e in Australia (università del New South Wales). Tali gruppi hanno effettuato, per ciascun obiettivo di controllo così come previsto dal framework, una ricerca, un'analisi, ed una valutazione dei principali standard internazionali tecnici, dei codici di condotta, degli standard di qualità, degli standard professionali relativi all'auditing ed alle practice ed ai requisiti delle varie "industry". Ciascun dominio e processo è stato analizzato in profondità e sono stati suggeriti nuovi obiettivi di controllo (o modificati quelli esistenti) per ciascun particolare processo IT. Infine il COBIT Steering Committee ha effettuato il consolidamento finale dei risultati.

La 3° edizione di COBIT (rilasciato nel 2000) ha introdotto le "management guideline" ed aggiornato, sulla base di nuove referenze internazionali, i contenuti della precedente edizione; il framework è stato rivisto e migliorato per supportare l'aumento del "management control", per introdurre il "performance management" e per sviluppare ulteriormente la "IT governance".

Quanto riportato nel presente paragrafo fa riferimento a tale edizione. Recentemente è stata emessa la 4° edizione del framework le cui principali differenze con la precedente edizione sono sinteticamente riportate alla fine del presente paragrafo.

L'aggiornamento di COBIT si è reso necessario a causa di numerosi cambiamenti nel mondo del business. Recentemente è stata ammessa la 4° versione. Nella versione più recente sono stati

leggermente modificati gli obiettivi di controllo per ottenere i seguenti risultati:

- Un'analisi su come gli obiettivi di controllo di dettaglio possono essere mappati sui cinque domini dell'IT Governance per identificare potenziali gap;

- Una ricerca sulle più importanti "IT Governance practice" che non sono ancora (completamente) previste in COBIT 3.0 per colmare i potenziali gap;

- Armonizzazione di COBIT con altri standard - un mapping dettagliato tra COBIT ed ITIL, CMM, COSO, PMBOK, ISF e ISO/IEC 17799 per rendere agevole l'armonizzazione con tali standard dal punto di vista del linguaggio, delle definizioni e dei concetti.

E' opportuno sottolineare che la recente versione COBIT 4.0 è un'estensione di COBIT 3° edizione ed in nessun modo invalida una implementazione od una attività basata su COBIT 3° edizione.

Per le Amministrazioni Pubbliche come per le aziende, il patrimonio informativo e la tecnologia che si utilizza per gestirlo rappresentano sempre di più un bene di fondamentale importanza. La continua crescita della dipendenza delle organizzazioni dalle informazioni e dai relativi sistemi che le gestiscono porta ad avere:

- Aumento delle vulnerabilità,

- Aumento del volume degli investimenti,

- Continua trasformazione delle organizzazioni e di conseguenza, necessità di ridurre i Costi.

Il principale obiettivo del COBIT è quello di pubblicare promuovere e autorizzare le prassi da utilizzare per il governo del IT generalmente accettate (best practice) rendendo pubblico un set di obiettivi di controllo accettati a livello internazionale per il controllo e governo l'IT.

Il COBIT è progettato principalmente per i responsabili dei processi di gestione del patrimonio informativo nell'ambito delle organizzazioni per i quali essere una guida al governo dell'IT. Il quadro di lavoro è basato su Standard, Practice e metodologie : OECD, ISACA, ITSEC, TCSEC, ISO900, TickIT, Common Criteria, COSO, IFAC, AICPA, GAO, ISO 17799.

La metodologia (la cui versione ufficiale è in lingua inglese), orientata oltre che ai responsabili dei processi anche agli utenti ed ai revisori, è articolata in una serie di documenti:

- Executive Summary: descrizione generale della metodologia;

- Framework: descrizione del metodo e degli obiettivi di controllo di alto livello;

- Control Objective: descrizione dei controlli minimi da adottare e degli obiettivi di controllo di dettaglio;

- Audit Guideline: descrizione degli obiettivi di controllo di audit;

- Implementation Tool Set: come si utilizza la metodologia COBIT;

- Cobit Security Baseline: si focalizza sui passi essenziali dell'organizzazione per assicurare la sicurezza delle informazioni.

Nell'ambito del COBIT sono adottate le seguenti definizioni:

- Controllo – si ottiene mediante politiche, procedure, prassi e strutture organizzative che forniscono la garanzia del raggiungimento degli obiettivi dell'organizzazione.

- Obiettivo di controllo nell'IT – definizione del risultato o dell'obiettivo atteso mediante l'implementazione di una procedura di controllo in una particolare attività IT.

- Governo dell'IT – una struttura di relazioni e processi per dirigere e controllare la struttura (azienda o Pubblica Amministrazione) al fine di raggiungere gli scopi (missione istituzionale) della stessa apportando valore e benefici al IT ed ai suoi processi.

Il framework COBIT identifica 34 principali processi di

Information Technology, raggruppati in 4 domini:

1) Pianificazione ed organizzazione,
2) Acquisizione e Realizzazione,
3) Erogazione ed Assistenza,
4) Monitoraggio.

I 34 processi sono supportati da 318 obiettivi di controllo di dettaglio. Ciascuno dei 34 processi individua le risorse IT coinvolte ed i requisiti di qualità, fiducia e di sicurezza richiesti.

I principi su cui si basa la metodologia sono:

- efficacia – le informazioni devono essere rilevanti e pertinenti ai processi dell'organizzazione;

- efficienza – riguarda l'uso ottimale delle risorse;

- riservatezza – le informazioni devono essere protette da accessi non autorizzati;

- integrità – riguarda la accuratezza e completezza delle informazioni;

- disponibilità – l'informazione deve essere disponibile quando richiesto dai processi;

- conformità – per il rispetto di leggi, regolamenti, accordi contrattuali cui è soggetta la struttura;

- affidabilità – riguarda la fornitura di appropriate informazioni alla Direzione, per far fronte alle proprie responsabilità ed obblighi.

Le linee guida di COBIT sono generiche ed orientate ai processi allo scopo di indirizzare le seguenti necessità del management che si occupa di controlli:

- Misurazione delle performance – quali sono i migliori indicatori di performance?

- IT control profiling – cosa è veramente importante? Quali sono i fattori critici per il successo dei controlli?

- Consapevolezza – quali sono i rischi che potrebbero impedirci di raggiungere i nostri obiettivi?

- Benchmarking – cosa fanno gli altri? Come possiamo misurare e confrontare i nostri risultati?

- Gestione delle emergenze IT e continuità dell'erogazione dei servizi.

Di seguito sono riepilogati 4 Domini ed i relativi 34 Obiettivi di controllo di alto livello di COBIT.

Organizzazione e pianificazione:

Il dominio copre la Strategia e la Tattica, riguarda come l'IT può meglio identificare il modo con cui contribuire al raggiungimento degli obiettivi di alto livello della organizzazione (azienda o Pubblica Amministrazione), realizzare quindi una visione strategica con la pianificazione da parte dei responsabili dei processi (management) che si deve occupare anche di comunicare e gestire tali obiettivi:

- PO1: Definizione di un piano IT strategico (Define a strategic IT plan)

- PO2: Definizione delle architetture informatiche (Define the information architecture)

- PO3: Individuazione degli indirizzi tecnologici (Determine technological direction)

- PO4: Definizione dell'organizzazione IT (Define the IT organization and relationships)

- PO5: Gestione degli investimenti IT (Manage the IT investment)

- PO6: Comunicazione al management degli obiettivi strategici (Communicate management aims and direction)

- PO7: Gestione delle risorse umane (Manage human resources)

- PO8: Assicurare il rispetto dei requisiti esterni (Ensure compliance with external requirements)

- PO9: Valutazione dei rischi (Assess risks)

- PO10: Gestione e Pianificazione dei progetti (Manage projects)

- PO11: Gestione della qualità (Manage quality)

Acquisizione e realizzazione delle soluzioni IT:

- AI1: Identificazione delle soluzioni automatizzate (Identify automated solutions)

- AI2: Acquisizione e manutenzione del software applicativo (Acquire and maintain application software)

- AI3: Acquisizione e manutenzione della infrastruttura tecnologica (Acquire and maintain technology infrastructure)

- AI4: Sviluppo e manutenzione delle procedure (Develop and maintain procedures)

- AI5: Installazione e certificazione dei sistemi (Install and accredit systems)

- AI6: Gestione delle Modifiche (Manage changes)

Erogazione del servizio e assistenza:

- DS1: Definizione e gestione degli Accordi di Servizio (Define and manage service levels)

- DS2: Gestione dei servizi affidati a terze parti (Manage third-party services)

- DS3: Gestione delle prestazioni e delle capacità (Manage performance and capacity)

- DS4: Garanzia della continuità del servizio (Ensure continuous service)

- DS5: Garanzia della sicurezza dei sistemi (Ensure systems security)

- DS6: Identificazione ed attribuzione dei costi (Identify and allocate costs)

- DS7: Formazione degli utenti (Educate and train users)

- DS8: Assistenza e informazione dei clienti (Assist and advise

customers)

- DS9: Gestione della configurazione (Manage the configuration)

- DS10: Gestione dei problemi e degli incidenti (Manage problems and incidents)

- DS11: Gestione dei dati (Manage data)

- DS12: Gestione dei servizi di comodità (Manage facilities)

- DS13: Gestione delle operazioni (Manage operations)

Monitoraggio:

- M1: Monitoraggio dei processi (Monitor the processes)

- M2: Verifica dell'adeguatezza dei controlli interni (Assess internal control adequacy)

- M3: Ottenimento di una verifica di conformità indipendente (Obtain independent assurance)

- M4: Fornitura di una revisione indipendente (Provide for independent audit)

Nell'ambito della metodologia è previsto inoltre una documentazione di Linee guida per il Management rivolto ai più alti responsabili dell'organizzazione al fine di fornire un quadro di riferimento per poter controllare e misurare l'Information Technology.

La documentazione è costituita da:

3.2.3.1 Modelli di maturità

Per ciascuno dei 34 processi COBIT, è previsto di adottare una scala di misurazione basata su un punteggio che varia fra "0" e "5"; la scala è associata con un modello di maturità che varia dal "Non Esistente" a "Ottimizzato", modello mutuato dal "Capability Maturity Models" del Software Engineering Institute - SEI. La scala di valutazione è volutamente non troppo granulare al fine di rendere il sistema semplice da usare; viceversa è opportuno concentrasi sui livelli qualitativi di maturità del processo analizzato utilizzando una serie di condizioni non ambigue. Per

ciascuno dei 34 processi COBIT è così possibile effettuare dei confronti sulla base del livello qualitativo indicato:

- lo stato corrente dell'organizzazione – dove è oggi l'organizzazione;

- lo stato corrente (best-in-class in) dell'industry di riferimento – il confronto;

- lo stato corrente come indicato dagli standard internazionali – il benchmarking;

- la strategia dell'organizzazione per operare il miglioramento – dove l'organizzazione vuole posizionarsi nel futuro.

3.2.3.2 Fattori critici di successo

Definiscono gli elementi o le azioni più importanti per i responsabili per controllare i processi IT, sia essi dall'esterno che dall'interno, mediante Linee Guida orientate alla gestione del processo che devono indicare le azioni da eseguire (Procedure). Le linee guida sono le attività che perseguono la strategia Tecnica/Organizzativa della struttura con riferimento alla risorse. Nell'ambito dei Fattori Critici di Successo si devono definire e documentare:

- Processi,

- Politiche,

- Chiare competenze,

- Forte supporto "Impegno" dei responsabili,

- Idonea comunicazione,

- Coerenti pratiche di misurazione.

3.2.3.3 Indicatori chiave di obiettivo

Definiscono le misure per indicare ai responsabili se un processo IT ha soddisfatto i requisiti aziendali, espressi in termini di criteri informatici:

- Disponibilità,
- Integrità e Riservatezza, (abbattimento dei rischi),
- Efficienza economica dei processi e delle operazioni,
- Conferma dei criteri di affidabilità, efficacia, e conformità.

Un indicatore Chiave di Obiettivo rappresenta l'obiettivo del processo e deve essere misurabile per consentire la valutazione del raggiungimento dell'obiettivo. Gli Indicatori Chiave di Obiettivo sono indicatori "a posteriori", e danno indicazione che l'informatica e la tecnologia stanno o meno contribuendo alla strategia dell'organizzazione.

3.2.3.4 Indicatori chiave di prestazione

Sono misure che indicano ai responsabili che il processo IT sta raggiungendo i suoi obiettivi aziendali. E' un controllo "a priori" che misura le prestazioni dei fattori abilitanti dei processi IT e indica quanto bene il processo contribuisce al raggiungimento dello scopo. Gli Indicatori Chiave di Prestazione spesso sono una misura per i Fattori Critici di Successo.

Nel contesto delle presenti linee guida, è opportuno sottolineare come uno dei domini del quadro di lavoro sia specificatamente indirizzato alla erogazione del servizio ed assistenza, che riguarda le operazioni volte alla sicurezza e continuità del servizio IT in questione, comprese le attività di assistenza sistemistica, elaborazione dei dati, controllo delle applicazioni informatiche.

A titolo di esempio si riporta di seguito una descrizione di maggiore dettaglio di quanto previsto nell'ambito dell'obiettivo di controllo di alto livello DS2 – Gestione dei servizi affidati a terze parti del dominio in questione con i relativi obiettivi di controllo di dettaglio.

3.2.3.5 Dominio: Erogazione del servizio ed assistenza

Obiettivo di controllo di alto livello

DS2 – Gestione dei servizi affidati a terze parti: La necessità di assicurare che i servizi forniti da terze parti siano coerenti con i requisiti aziendali richiede un efficace gestione del relativo processo. Questo processo viene portato a termine definendo, nell'ambito di specifici accordi con terze parti, in maniera chiara i ruoli, le responsabilità e le aspettative così come rivedendo e controllando tali accordi per assicurarne la efficacia e rispetto.

Una efficace gestione dei servizi affidati a terze parti minimizza il rischio associato a fornitori che non assicurino le prestazioni richieste.

Obiettivi di controllo di dettaglio

DS2-1 Interfaccia con i fornitori : i responsabili (management) dovrebbero assicurarsi che tutti i fornitori terzi di servizi siano identificati in maniera appropriata e che le interfacce sia tecniche che organizzative con tali fornitori siano opportunamente documentate.

DS2-2 Proprietario (owner) delle relazioni : i responsabili della organizzazione dell'utente dovrebbero nominare un proprietario (owner) delle relazioni che è responsabile di assicurare la qualità delle relazioni con le terze parti.

DS2-3 Contratti con fornitori terzi : i responsabili (management) dovrebbero definire delle procedure specifiche per assicurarsi che, per ciascuna delle relazioni con i fornitori terzi di servizi, sia definito e concordato un contratto formale prima che i lavori siano avviati.

DS2-4 Qualifica dei fornitori terzi : i responsabili (management) dovrebbero assicurarsi che, prima della selezione, i potenziali fornitori terzi siano stati qualificati appropriatamente attraverso una valutazione della loro capacità di erogare il servizio richiesto (due diligence).

DS2-5 Contratti di Outsourcing : dovrebbero essere definite delle specifiche procedure organizzative per assicurare che il con-

tratto tra il fornitore dei servizi di gestione della infrastruttura e l'organizzazione sia basato sui livelli richiesti di capacità elaborativa, sicurezza, monitoraggio, ed altri requisiti appropriatamente concordati.

DS2-6 Continuità del servizio : rispetto alla continuità del servizio, i responsabili (management) dovrebbero tenere conto del "rischio di business" connesso all'affidamento a terzi in termini di incertezza e preoccupazioni legali, e, ove necessario, negoziare accordi di impegno (escrow contracts).

DS2-7 Relazioni inerenti la sicurezza : riguardo alle relazioni con fornitori di servizi terzi, i responsabili (management) dovrebbero assicurarsi che gli accordi che riguardano la sicurezza (es. accordi sulla riservatezza – 'non disclosure agreements') siano ben identificati ed esplicitamente dichiarati, conformi agli standard universalmente accettati di mercato ed in accordo con i requisiti normativi e con i regolamenti, ed includa la responsabilità connessa.

DS2-8 Monitoraggio : i responsabili (management) dovrebbero mettere a punto un processo di monitoraggio del servizio erogato da terzi per assicurare la continua aderenza con gli accordi contrattuali.

3.2.4 Confronto tra ISO17799, ITIL e COBIT

L'utilizzo di politiche e procedure di gestione standard e di prassi comunemente accettate consente di rendere più efficienti ed efficaci le normali attività di erogazione dei servizi IT evitando ogni volta di dover ri-progettare gli stessi servizi e rivedere le metodologia per la risoluzione dei problemi.

D'altra parte le prassi individuate devono avere un loro riscontro con un quadro di lavoro di controllo e di gestione dei rischi che sia appropriato e calato nella particolare situazione concreta, che sia adatto per la specifica organizzazione e che sia armonizzato con gli altri metodi e prassi adottate nell'ambito della struttura. In altre parole, risulta opportuno che le 'best practice' individuate a supporto della gestione e del management ICT

siano opportunamente personalizzate per aderire al meglio alla specifica realtà in cui devono essere applicate.

Nei paragrafi precedenti è stata riportata una breve panoramica delle principali 'best practice' indicate a supporto del management ICT per il governo e controllo dei processi di gestione in sicurezza dell'affidamento a terzi dei servizi ICT : ISO 270001/ISO17799, ITIL e COBIT.

Risulta opportuno a questo punto individuare, anche se in maniera estremamente sintetica, come queste tre metodologie possano integrarsi e completarsi per concorrere in maniera efficiente ed efficace ad assicurare gli obiettivi delineati nel presente documento.

Nel seguito sono suggeriti alcuni criteri di base di confronto indicati al fine di assicurare, utilizzando un linguaggio comune per le tre metodologie, l'ottenimento dei medesimi obiettivi.

Adattare

Ogni organizzazione ha bisogno di adattare l'utilizzo di standard e metodologie per il raggiungimento dei propri specifici requisiti. A questo riguardo le tre metodologie possono giocare un ruolo molto utile: COBIT ed ISO17799 possono aiutare nel definire cosa deve essere fatto, mentre ITIL aiuta nel definire il come nel definire gli aspetti di gestione dei servizi.

Dare la priorità

Per evitare implementazioni delle metodologie che risultino non focalizzate sugli obiettivi e eccessivamente costose, l'organizzazione ha bisogno di avere delle priorità per decidere in che ambiti e come utilizzare le diverse metodologie. A questo riguardo è importante che l'alta direzione prenda pienamente la ownership del governo ICT e stabilisca chiaramente la direzione che il management ICT deve seguire. Nel far questo si può tenere conto che COBIT è un quadro di lavoro per il management del governo IT, mentre ITIL è un framework per la gestione dei servizi IT.

Pianificare

Avendo chiaro il mandato e le priorità, il management può mettere in atto un piano di implementazione dei servizi ICT. Nello stabilire il piano il management dovrebbe tenere conto che:

- il framework COBIT, che aiuta a definire gli obiettivi IT, usato in congiunzione con ITIL aiuta a definire sia i servizi che gli SLA nell'ottica dell'utente finale;

- il processo di gestione del rischio ed il framework del COBIT aiuta ad assicurare che i rischi siano identificati e presi in carico. Dall'altra parte i rischi operativi sono resi più chiari nell'adozione di ITIL mentre ISO 17799 rende più chiari i rischi di sicurezza;

- il framework dei processi COBIT, con il supporto delle definizioni ITIL dei processi chiave per l'erogazione dei servizi e degli obiettivi di sicurezza ISO17799, può aiutare nella definizione degli obiettivi e dei processi IT e nella gestione dei relativi rischi associati;

- le linee guida COBIT , supportate con maggiori dettagli dalle guide specifiche ITIL ed ISO17799, danno la possibilità di analizzare le capacità attuali del sistema ed individuare eventuali falle da colmare, così come aiutano nel definire delle strategie e delle prassi di miglioramento continuo.

A titolo di esempio si riporta nella tabella seguente (Tabella 3) la corrispondenza, nel caso del dominio erogazione del servizio ed assistenza/obiettivo gestione del servizio affidato a terze parti, per ciascuno dei relativi obiettivi di controllo di dettaglio. Il riferimento a ITIL e ISO è riportato nella versione in lingua inglese

3.3 Macro-Categorie di Servizio

Di seguito si propone una nuova catalogazione dei servizi ICT definiti dal CNIPA secondo il criterio della sicurezza.

Tale catalogazione si rivolge simmetricamente sia alle amministrazioni che acquisiscono beni e servizi ICT, sia ai fornitori di

COBIT	ITIL	ISO 17799
DS2-1 Interfaccia con il fornitore	Gestione della relazione col fornitore: 7.1 tipo di relazione col fornitore	4.1 Infrastruttura di sicurezza Informatica 4.2 Sicurezza dell'accesso delle terze parti 11.1 Gestione degli aspetti di business continuity
DS2-2 Proprietario della relazione	Gestione della relazione col fornitore: 7.2 caratterizzazione della relazione	4.2 Sicurezza dell'accesso delle terze parti
DS2-3 Contratti con fornitori terzi	Gestione della relazione col fornitore: 7.4 Gestione del contratto	4.2 Sicurezza dell'accesso delle terze parti
DS2-4 Qualifica dei fornitori terzi		6.1 Sicurezza nella definizione dei ruoli e delle risorse
DS2-5 Contratti di Outsourcing	Gestione della relazione col fornitore: 7.4 Outsourcing	4.3 Outsourcing 8.1 Procedure operative e responsabilità 10.5 Sicurezza nello sviluppo e supporto dei processi
DS2-6 Continuità dei servizi	Sviluppo della relazione col fornitore: 7.6.4 Fine della relazione	4.3 Outsourcing 10.5 Sicurezza nello sviluppo e supporto dei processi
DS2-7 Relazioni inerenti la sicurezza		4.2 Sicurezza dell'accesso delle terze parti 6.1 Sicurezza nella definizione dei ruoli e delle risorse 6.3 Reazione ad incidenti e malfunzionamenti di sicurezza 8.1 Procedure operative e responsabilità 8.7 Scambio di informazioni e software 10.3 Controlli crittografici 10.5 Sicurezza nello sviluppo e supporto dei processi
DS2-8 Monitoraggio	Gestione della relazione col fornitore: 7.4 Gestione del contratto Erogazione del servizio, Gestione del livello del servizio: 4.4.7 Capacità di monitoring	4.3 Outsourcing 6.1 Sicurezza nella definizione dei ruoli e delle risorse 10.5 Sicurezza nello sviluppo e supporto dei processi

Tabella 3: Confronto fra le tre metodologie

quest'ultimi, in quanto la biunivocità di una relazione contrattuale porta inevitabilmente al risultato che una cosa suggerita a chi

appalta si rifletta su chi offre e viceversa. Peraltro, la necessità di garantire un elevato livello di sicurezza anche nella esternalizzazione dei servizi ICT (outsourcing), trasforma la relazione asimmetrica cliente/fornitore in una relazione paritetica tra partner con ruoli e responsabilità complementari.

La catalogazione proposta raccoglie i contratti della Pubblica Amministrazione che definiscono l'erogazione di servizi ICT in base agli aspetti di scurezza che devono essere tenuti in considerazione. In particolare, tiene conto che, in fase di stipula di tali servizi, siano definiti:

- i ruoli tra amministrazione e fornitore, al fine di evitare ambiguità per quanto riguarda le responsabilità reciproche relative alla sicurezza;

- i livelli di sicurezza tra l'amministrazione utente dei servizi, ed il fornitore erogatore dei servizi. In questo caso il contratto è l'unico mezzo utile per definire a priori il livello di sicurezza atteso ed eliminare possibili ambiguità nel rapporto tra le parti prima che queste effettivamente si presentino;

- gli strumenti per impostare ed attuare un'efficace azione di governo della fornitura e di verifica del livello di sicurezza atteso. Le modalità di misurazione del livello di sicurezza garantito dal fornitore sono infatti l'unica efficace assicurazione per garantire un livello di sicurezza dei servizi e dei prodotti realizzati dal fornitore in linea con le attese dell'Amministrazione.

In particolare, la seguente catalogazione si pone l'obiettivo di individuare quei requisiti che consentano di realizzare forme di esternalizzazione che garantiscano un elevato livello di sicurezza dei servizi ICT acquisiti.

Gli aspetti di sicurezza individuati nella presente catalogazio
ne si applicano a tutte le possibili forme di acquisizione delle forniture ICT (outsourcing totale o parziale di servizi, insourcing e co-sourcing, joint venture, consorzi, etc.), tenendo conto che un livello elevato di sicurezza può essere raggiunto soltanto se, sia il fornitore del servizio che l'acquirente, si organizzino per:

- identificare i processi, le attività e gli strumenti di supporto e di

riscontro, sia nella fase di acquisizione che nell'attuazione della fornitura;

- rappresentare una reale controparte presidiando le funzioni essenziali alla gestione della relazione cliente/fornitore, con una struttura organizzativa adeguata nella quale siano chiaramente definiti ruoli e responsabilità;

Nella Tabella 4 viene riportato lo schema di classificazione dei servizi ICT individuato dal CNIPA con l'elenco delle Classi di fornitura e dei processi trasversali, ovvero dei lemmi contenuti nel Dizionario delle forniture ICT, ordinati per codice in base alla suddetta classificazione.

Nella Tabella 5 viene proposta una nuova classificazione di tali classi di servizi, al fine di individuare quelle tipologie di servizio che richiedono un livello di attenzione omogeneo dal punto di vista della sicurezza.

L'approccio che viene seguito è quello di creare una macro categorizzazione dei servizi per livello omogeneo di sicurezza. Le macro categorie individuate presentano infatti una serie di tematiche comuni relative alla sicurezza che devono essere affrontate in modo comune:

3.3.1 Servizi di gestione

Rientrano in questa categoria le seguenti classi di servizio (tra parentesi quadre il riferimento alla classificazione CNIPA di Tabella 5):

3.3.1.1 Gestione applicativi e Basi Dati [1.2.1 GSW]

La classe dei servizi di gestione applicativi e basi dati comprende le attività per la presa in carico, la gestione, l'evoluzione e la terminazione di applicativi e delle loro relative basi-dati. In questo contesto viene definita "applicazione" un qualsiasi software (ad-hoc o prodotto di mercato) composto da uno o più moduli e da un database a cui l'applicazione fa riferimento.

Cod	*Sigla*	*Denominazione, Classi di fornitura ICT*
1.	**Servizi per l'utente**	
1.1	Sviluppo e Manutenzione Evolutiva applicazioni	
1.1.1	SSW	Sviluppo e MEV di software ad hoc
1.1.2	PSW	Personalizzazione e MEV di prodotti esistenti
1.1.3	SSC	Sviluppo e MEV mediante soluzioni commerciali
1.2	Gestione e manutenzione applicazioni	
1.2.1	GSW	Gestione applicativi e Basi Dati
1.2.2	MAC	Manutenzione correttiva ed adeguativa (MAC)
1.2.3	MSW	Migrazione e conversioni applicazioni
1.3	Assistenza all'utente e formazione	
1.3.1	ASS	Assistenza in remoto e in locale
1.3.2	FOR	Formazione e addestramento
2.	**Servizi per l'interoperabilità e la cooperazione**	
2.1	Servizi di integrazione	
2.1.1	ISW	Integrazione di prodotti software e basi dati
2.1.2	ISI	Integrazione di sistemi e infrastrutture
2.2	Servizi applicativi	
2.2.1	ASP	Servizi applicativi in modalità ASP
2.2.2	PEL	Posta elettronica
2.2.3	PEC	Posta elettronica certificata
2.2.4	INT	Servizi Internet
2.2.5	WEB	Gestione contenuti WEB
2.3	Riconoscimento digitale	
2.3.1	CFD	Certificazione delle firma digitale
3.	**Servizi infrastrutturali**	
3.1	Servizi per le Reti	
3.1.1	SRT	Sviluppo Reti
3.1.2	GMR	Gestione e manutenzione reti
3.2	Servizi per i Sistemi	
3.2.1	SSI	Sviluppo sistemi
3.2.2	GSI	Gestione sistemi
3.2.3	MSI	Manutenzione sistemi
3.3	Servizi di sicurezza	
3.3.1	SIL	Gestione della sicurezza logica
3.3.2	SIF	Gestione della sicurezza fisica
3.4	Servizi di Gestione Documentale	
3.4.1	TDO	Trattamento documentale e acquisizione dati
3.4.2	WFM	Gestione elettronica dei documenti
3.5	Servizi di monitoraggio della qualità dei servizi	
3.5.1	MLS	Controllo dei livelli di servizio
3.6	Servizi di Desktop	
3.6.1	GPL	Gestione e manutenzione delle postazioni di lavoro
4.	**Servizi di consulenza e body rental**	
4.1	Servizi professionali	
4.1.1	CON	Consulenza
4.1.2	DLA	Direzione lavori
4.1.3	MCS	Misura della Customer Satisfaction
4.2	Servizi di body rental	
4.2.1	IMD	Ingegneria e Mano d'opera
5.	**Fornitura di beni**	
5.1	Fornitura di prodotti Hardware e Software	
5.1.1	FPD	Prodotti Hardware e Software
6.	**Processi trasversali alle classi di servizio**	
6.1	Processi di supporto	
6.1.1	PGD	Documentazione
6.1.2	PGC	Gestione della Configurazione
6.1.3	PAQ	Assicurazione Qualità
6.2	Processi organizzativi	
6.2.1	PGE	Gestione

Tabella 4: Catalogo dei servizi ICT (CNIPA)

Codice	*Acronimo*	*Denominazione*
Servizi di gestione		
1.2.1	GSW	Gestione applicativi e basi dati
2.2.1	ASP	Servizi applicativi in modalità ASP
2.2.2	PEL	Posta elettronica
2.2.4	INT	Servizi Internet
2.2.5	WEB	Gestione contenuti WEB
3.4.1	TDO	Trattamento documentale e acquisizione dati
3.4.2	WFM	Gestione elettronica dei documenti
Servizi di integrazione		
2.1.1	ISW	Integrazione di prodotti software e basi dati
2.1.2	ISI	Integrazione di sistemi e infrastrutture
3.1.1	SRT	Sviluppo Reti
3.2.1	SSI	Sviluppo sistemi
Servizi di gestione e manutenzione delle infrastrutture		
1.3.1	ASS	Assistenza in remoto e in locale
3.1.2	GMR	Gestione e manutenzione reti
3.2.2	GSI	Gestione sistemi
3.2.3	MSI	Manutenzione sistemi
3.3.1	SIL	Gestione della sicurezza logica
3.3.2	SIF	Gestione della sicurezza fisica
3.6.1	GPL	Gestione e manutenzione delle postazioni di lavoro
4.2.1	IMD	Ingegneria e mano d'opera
5.1.1	FPD	Prodotti hardware e software
6.1.2	PGC	Gestione della configurazione
Servizi di sviluppo software		
1.1.1	SSW	Sviluppo e MEV di software ad hoc
1.1.2	PSW	Personalizzazione e MEV di prodotti esistenti
1.1.3	SSC	Sviluppo e MEV mediante soluzioni commerciali
1.2.2	MAC	Manutenzione correttiva ed adeguativa (MAC)
1.2.3	MSW	Migrazione e conversioni applicazion i
Servizi per la certificazione dei dati		
2.2.3	PEC	Posta elettronica certificata
2.3.1	CFD	Certificazione delle firma digitale
Servizi di consulenza formazione e documentazione		
1.3.2	FOR	Formazione e addestramento
4.1.1	CON	Consulenza
4.1.2	DLA	Direzione lavori
6.1.1	PGD	Documentazione
6.2.1	PGE	Gestione
Servizi di controllo qualità		
3.5.1	MLS	Controllo dei livelli di servizio
4.1.3	MCS	Misura della Customer Satisfaction
6.1.3	PAQ	Assicurazione Qualità

Tabella 5: Macro categorizzazione dei servizi ICT per livello di sicurezza

Il ciclo di vita di questa classe si articola nelle seguenti fasi:

- definizione dei requisiti di gestione;
- progetto di gestione delle applicazioni e delle basi-dati;
- presa in carico dell'applicazione;
- gestione dell'applicazione e livelli di servizio richiesti;
- gestione dell'evoluzione dell'applicazione e della base-dati in relazione al solo contesto operativo;
- amministrazione degli application server e dei data-base server;
- gestione della terminazione dell'applicazione.

3.3.1.2 Servizi applicativi in modalità ASP [2.2.1 ASP]

La classe dei servizi applicativi in modalità ASP (Application Service Provider) prevede l'utilizzo di una o più applicazioni remote di diversa natura proposte attraverso modelli di pricing a canone e/o a tariffa, determinando costi basati sugli effettivi consumi, senza investimenti iniziali e senza costi di gestione e manutenzione.

Il servizio offerto in modalità ASP è erogato attraverso infrastrutture remote e condivise, ubicate presso Centri Servizi di aziende specializzate operanti nel settore ICT. Tali infrastrutture consentono la fruizione dei servizi contemporaneamente a più utenti, garantendo tuttavia a ciascuno di essi la sicurezza dei propri dati.

3.3.1.3 Posta elettronica [2.2.2 PEL]

Il servizio di Posta Elettronica (PEL) fornisce il servizio di posta elettronica al personale dell'Amministrazione. Può essere un servizio dell'amministrazione gestito da un outsourcer, oppure un servizio erogato in modalità ASP. Tipicamente è integrato con elementi di sicurezza, quali antivirus, antispamming, ecc.

3.3.1.4 Servizi internet [2.2.4 INT]

I Servizi Internet possono essere definiti come la gamma di prodotti/servizi che vengono erogati sulla rete, rendendo difficile qualsiasi tentativo di classificazione, anche in virtù della continua evoluzione tecnologica e della crescente richiesta di funzioni relative alla sicurezza, alla disponibilità ed all'affidabilità a garanzia degli utenti a cui è destinata la fornitura.

I servizi Internet possono essere visti in due modalità: la prima fornisce le facilities ed i servizi dei quali l'utente deve poter fruire; la seconda fornisce le infrastrutture, le tecnologie e le competenze per garantire lo sviluppo, la realizzazione e l'erogazione dei servizi agli utenti.

3.3.1.5 Gestione contenuti web [2.2.5 WEB]

Obiettivo del servizio di gestione dei contenuti web è la creazione, classificazione e archiviazione dei contenuti del sito, la pubblicazione dinamica dei contenuti su Internet e/o sulla Intranet, aggiornamento e fine-tuning del sito, mediante strumenti di analisi dei contenuti, degli accessi e del traffico.

Il servizio può essere fornito in varie modalità:

- servizio in modalità ASP: tutto il servizio è gestito dal Service Provider;

- soluzione in hosting ovvero la soluzione applicativa è sviluppata e posseduta dall'Amministrazione, mentre il Provider fornisce hardware e connettività ed esercisce il servizio;

- soluzione in housing: l'Amministrazione possiede non solo la soluzione applicativa ma anche l'hardware

3.3.1.6 Trattamento documentale e acquisizione dati [3.4.1 TDO]

Nell'ambito dei servizi di Acquisizione Documentale rientra un'ampia gamma di servizi rivolti al trattamento dei documenti

con la finalità di pervenire all'acquisizione dei dati e delle informazioni in essi contenute, ivi compresa la trasposizione integrale di una "immagine" del documento su altro supporto e/o in altro formato.

3.3.1.7 Gestione elettronica dei documenti [3.4.2 WFM]

I servizi di Gestione Elettronica dei Documenti riguardano le soluzioni legate all'acquisizione, archiviazione, classificazione e ritrovamento/consultazione di informazioni non strutturate.

La classe comprende le attività di:

- gestione dei documenti cartacei, ovvero memorizzazione, classificazione, archiviazione e recupero dei documenti cartacei collocati in appositi archivi;

- cattura dei documenti cartacei, loro trasposizione in formato elettronico e gestione dei documenti così ottenuti;

- creazione, pubblicazione e distribuzione dei documenti e contenuti elettronici;

- realizzazione dell'infrastruttura della gestione documentale, ovvero i sistemi necessari per la condivisione, l'accesso e l'automazione dei processi di business;

- distribuzione dei documenti, ovvero stampa, pubblicazione e distribuzione verso determinati destinatari.

3.3.1.8 Aspetti di sicurezza

I servizi dovranno essere svolti nel rispetto delle leggi vigenti in materia di trattamento dei dati personali (D. Lgs 196/2003). I processi di supporto definiti per tali servizi dovranno tenere conto anche degli aspetti di sicurezza, come ad esempio le politiche di sicurezza e le istruzioni operative per gestire situazioni di emergenza, oppure per il monitoraggio dei sistemi, le politiche di backup e le funzionalità di integrazione, ecc.

Dovrà essere stilato un documento atto ad identificare in modalità chiara ed univoca i ruoli con le relative responsabilità, gli aspetti tecnici, tecnologici e procedurali della fornitura del servizio.

Il fornitore dovrà inoltre definire un documento con le specifiche dei requisiti minimi di sicurezza per garantire: integrità, confidenzialità dei dati sia nella comunicazione sia nella custodia ed accesso, con espressa aderenza alle normative vigenti.

Per quanto riguarda i servizi erogati in modalità ASP deve essere inoltre garantita a ciascun utente la sicurezza dei propri dati, intesa come riservatezza, disponibilità ed integrità delle informazioni gestite. Deve essere in ogni caso garantita l'aderenza alle normative vigenti in termini di riservatezza dei dati e trattamento dei dati personali. Deve essere infine definito un piano della sicurezza, che descriva i criteri tecnici ed organizzativi relativi alla protezione delle aree e dei dati gestiti dal fornitore.

Per quanto riguarda il servizio di posta elettronica il fornitore dovrà garantire adeguate misure di sicurezza al fine di evitare usi impropri dei server di posta elettronica, dovrà disporre di una configurazione delle mailbox che ne garantisca la protezione consentendo un'identificazione univoca dell'utilizzatore (ad esempio attraverso identificativo utente e password) e dovrà predisporre opportune misure di controllo di sicurezza (antivirus, anitspam, antiphishing, ecc.)

Per quanto riguarda i servizi di trattamento documentale e acquisizione dati e di gestione elettronica dei documenti, attraverso procedure e strumenti adeguati, il fornitore, attraverso procedure e strumenti adeguati, dovrà garantire:

- la conservazione dei documenti, escludendo i rischi di manipolazione e dispersione, con la garanzia che l'integrità degli stessi sia assicurata a livello di supporto fisico (ad esempio: supporti certificati legalmente a 25 anni)

- la trasmissione dei documenti in modalità sicura utilizzando appositi protocolli ed eventualmente linee di comunicazione fisicamente sicure.

- la tutela dei dati personali in conformità al Testo Unico (D. Lgs. 196/2003)

Per quanto concerne infine i servizi di gestione dei contenuti web, la fornitura del servizio deve garantire l' accessibilità da parte dei soggetti disabili in base alla legge n. 4 del 9 gennaio 2004 "Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici". La pubblicazione di siti e pagine web, accessibili al pubblico su Internet, dovranno essere fornite rispettando sia gli standard di gestione dei contenuti sia quelli relativi ai formati di descrizione dei contenuti.

3.3.2 Servizi di integrazione

Rientrano in questa categoria le seguenti classi di servizio:

3.3.2.1 Integrazione di prodotti software e basi dati [2.1.1 ISW]

Obiettivo della classe è quello di realizzare l'integrazione o la cooperazione tra applicazioni. Appartengono a questa categoria i servizi di integrazione di componenti e sistemi software tra sottosistemi di una stessa organizzazione o tra organizzazioni diverse, l'integrazione tra banche dati oppure l'esposizione di servizi legacy con interfaccia web.

L'obiettivo è quello di offrire servizi che consentano di mettere insieme le informazioni frutto di specifiche elaborazioni di diverse applicazioni attraverso prodotti di EAI (Enterprise Application Integration), al fine di rendere omogeneo il sistema informativo e consolidarlo, per poi estendere le sue funzionalità anche alla cooperazione con sistemi appartenenti ad organizzazioni diverse.

Relativamente ai servizi di integrazione tra banche dati, questa classe si riferisce all'utilizzo di prodotti di ETL (Extract, Transform and Load) oppure OLAP (On-line Analytical Processing).

3.3.2.2 Integrazione di sistemi e infrastrutture [2.1.2 ISI]

La classe di servizi si riferisce all'integrazione dei sistemi e delle infrastrutture, affinché i sistemi ed ambienti tecnologici diversi divengano interoperabili. I servizi di questa classe si pongono l'obiettivo di migliorare e fornire nuovi servizi agli utenti, oppure di valorizzare, senza dover abbandonare le scelte tecnologiche gia fatte, i servizi isolati/obsoleti presenti nell'esistente architettura, integrandoli con altre tecnologie avanzate.

3.3.2.3 Sviluppo reti [3.1.1 SRT]

La classe di fornitura Sviluppo Reti comprende le attività di progettazione e realizzazione finalizzate alla attivazione dei sistemi di rete necessari per la erogazione di servizi di telecomunicazioni (TLC).

La classe di fornitura Sviluppo Reti, partendo dall'analisi delle necessità di base dei servizi di rete, dal supporto di telecomunicazioni necessario alle applicazioni e dai documenti contrattuali, si sviluppa allo scopo di:

- definire ed identificare le specifiche della fornitura, integrando i documenti contrattuali con le ulteriori informazioni necessarie;

- sviluppare la documentazione progettuale esecutiva necessaria per le successive attività realizzative e di prova.

3.3.2.4 Sviluppo sistemi [3.2.1 SSI]

La classe di fornitura Sviluppo Sistemi definisce le attività ed i prodotti necessari alla progettazione e realizzazione di un'infrastruttura informatica a supporto dell'erogazione di un servizio. L'infrastruttura può comprendere i server, i client, il software di base ed il software d'ambiente (middleware: DBMS, application server, driver di comunicazione, ecc.). La classe di fornitura Sviluppo Sistemi, partendo dall'analisi delle necessità di base di un

servizio o di un'applicazione, comprende tutte le attività necessarie per la realizzazione dell'infrastruttura informatica.

3.3.2.5 Aspetti di sicurezza

La fornitura dei servizi di integrazione dovrà comprendere:

- un piano di progetto;

- una serie di rapporti tecnici atti a dimostrare la rispondenza delle tecnologie e delle scelte sistemistiche adottate nei confronti dei Requisiti di Base della fornitura e delle scelte adottate durante la progettazione tecnica;

- proposte migliorative rispetto ai requisiti minimi;

- un piano di gestione delle comunicazioni, soprattutto nel caso in cui l'introduzione del nuovo sistema implichi significative modifiche all'ambiente organizzativo o ai processi dell'Amministrazione o del gestore dei sistemi.

Per tutti i casi di integrazione, si possono verificare due situazioni: sistemi appartenenti alla stessa organizzazione o sistemi appartenenti ad organizzazioni diverse. La situazione nella quale i sistemi appartengano ad Amministrazioni differenti pone maggiori vincoli di sicurezza che riguardano la confidenzialità delle informazioni scambiate, la disponibilità e la loro integrità. Per esempio sarà necessario configurare od inserire apparati che garantiscano la sicurezza dei collegamenti con strutture di reti esterne.

Per quanto riguarda l'utilizzo di prodotti EAI, la modalità di accesso alle applicazioni esistenti può imporre dei vincoli relativamente all'integrità dei dati e alla loro sicurezza. In particolare devono essere garantiti livelli di sicurezza e di protezione dei dati di origine. Per questo motivo tali servizi devono essere accompagnati da un'analisi che individui i protocolli di comunicazione che implementino le misure di sicurezza più opportune.

Devono essere tenuti in considerazione anche gli aspetti di sicurezza per garantire:

- l'integrità e la confidenzialità dei dati, sia a livello applicativo che a livello di reti di e protocolli di comunicazione;

- la disponibilità dei dati, sia per quanto riguarda il salvataggio e la conservazione (eventuali politiche di ritenzione, frequenza del backup, ecc.), sia per la garanzia della continuità del servizio (ridondanza dei sistemi, cluster, ecc.);

Per quanto riguarda la sicurezza fisica, i luoghi dove saranno ospitati i sistemi di erogazione del servizio dovranno essere aderenti alle norme specifiche riguardanti la sicurezza degli edifici e dei luoghi di lavoro e dovranno garantire i livelli di sicurezza ed affidabilità secondo le normative vigenti.

3.3.3 Servizi di gestione e manutenzione delle infrastrutture

Rientrano in questa categoria le seguenti classi di servizio:

3.3.3.1 Assistenza in remoto e in locale [1.3.1 ASS]

La classe comprende i servizi che forniscono agli utenti interni o esterni di un'Amministrazione un punto di accesso unificato ad un insieme di funzioni di assistenza.

Si tratta di soluzioni basate sul canale telefonico (Call Center) o su strategie multicanali (Contact Center) di accesso alle informazioni e ai servizi (Help Desk tecnico/amministrativo, CRM – Customer Relationship Management).

3.3.3.2 Gestione e manutenzione reti [3.1.2 GMR]

La classe di fornitura Gestione e Manutenzione Reti (GMR) comprende le attività di gestione della rete di telecomunicazioni necessaria per l'erogazione di servizi di telecomunicazioni. Obiettivo della fornitura è la gestione di tutti gli elementi che costituiscono l'infrastruttura di rete, coordinando ed assicurando gli interventi volti al ripristino delle funzionalità del servizio di rete e/o apparati.

3.3.3.3 Gestione sistemi [3.2.2 GSI]

La classe di fornitura Gestione sistemi include tutte quelle attività, necessarie per prendere in carico, condurre e mantenere sempre aggiornata e funzionante una infrastruttura hardware e software utilizzata per l'erogazione di uno o più servizi informatici. Questa classe quindi si identifica come la gestione dell'esercizio dei sistemi e comprende le installazioni dell'hardware e del software di base, la loro configurazione, personalizzazione ed eventuale distribuzione presso sistemi periferici in relazione ad aggiornamenti di configurazioni esistenti. Le attività previste dalla fornitura includono anche la conduzione operativa dei sistemi, il monitoraggio dei sistemi per la rilevazione e la risoluzione di malfunzionamenti e la definizione delle modalità di utilizzo dello storage e del backup.

3.3.3.4 Manutenzione sistemi [3.2.3 MSI]

La classe di fornitura Manutenzione Sistemi comprende le attività necessarie per mantenere continuamente allineati i Sistemi HW e SW alle più recenti innovazioni tecnologiche rilasciate dai fornitori e necessarie per la corretta erogazione del servizio, nonché tutte le attività necessarie per ripristinare il funzionamento dei Sistemi a fronte di errori.

Le attività previste dalla fornitura possono quindi essere di due tipi:

- Manutenzione Preventiva (attività di manutenzione atta a prevenire l'occorrenza di errori, malfunzionamenti e guasti);

- Manutenzione Correttiva (attività di manutenzione a seguito di malfunzionamenti o guasti).

3.3.3.5 Gestione sicurezza logica [3.3.1 SIL]

Un servizio di Gestione della Sicurezza Logica (SIL) realizza e gestisce le contromisure di tipo tecnologico volte alla difesa

perimetrale e di contenuto del sistema informativo.

Un sistema SIL è un insieme di servizi aventi lo scopo di:

- attuare la politica per la sicurezza ai flussi di rete in termini di tipo e/o contenuto del traffico;

- monitorare e verificare l'efficacia delle misure di sicurezza adottate per i flussi di rete;

- valutare e gestire il rischio associato alle minacce di tipo informatico;

- acquisire strumenti tecnologici e competenze in grado di affrontare e risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza.

Le principali attività che caratterizzano il servizio posso essere riassunte in:

- Monitoraggio

- Gestione delle emergenze

- Aggiornamento

3.3.3.6 Gestione sicurezza fisica [3.3.2 SIF]

La Gestione della sicurezza fisica (SIF) tratta le misure necessarie per proteggere le aree, i sistemi e le persone che operano sul sistema informativo.

Generalmente un sistema SIF si articola nelle seguenti due categorie di servizi:

- sicurezza di area: ha il compito di proteggere le aree, impedendo accessi non autorizzati, danni e interferenze agli ambienti, danneggiamento delle informazioni;

- sicurezza delle apparecchiature: ovvero protezione degli ambienti, delle risorse ICT e dei supporti, da danneggiamenti accidentali o intenzionali, da furti o manomissioni di informazioni e strumenti di elaborazione.

3.3.3.7 Gestione e manutenzione delle postazioni di lavoro [3.6.1 GPL]

La classe comprende i servizi di gestione e manutenzione delle postazioni di lavoro (PdL) finalizzati a garantire costantemente l'efficienza e l'operatività dell'utente, indipendentemente dalla locazione.

Il servizio oggetto della fornitura opera a prescindere dal fatto che la postazione di lavoro sia di proprietà del Committente o meno (concessa in noleggio, locazione operativa, in leasing, ecc..).

La gestione e la manutenzione delle postazioni di lavoro è scomponibile per elementi: installazione, movimentazione, aggiunte e cambiamenti e manutenzione preventiva e correttiva del posto di lavoro. Il servizio include, logicamente, anche attività connesse alla fornitura di beni (installazione di nuove postazioni di lavoro, installazioni di aggiornamenti hardware e/o software, ecc.).

Le attività necessarie all'espletamento del servizio di gestione e manutenzione delle postazioni di lavoro sono eseguite da personale tecnico, con competenze specialistiche, presso l'utente con operatività diretta sulla postazione di lavoro.

3.3.3.8 Ingegneria e mano d opera [4.2.1 IMD]

La classe di fornitura di servizi di Ingegneria e Mano d'Opera è relativa ai servizi di fornitura di risorse umane, in modalità a consumo, detta "man power" o "body rental", che corrispondano a determinati requisiti di competenza e conoscenza professionale (ad es. professionisti di elevato livello, risorse per data entry, operatori telefonici, analisti-programmatori, etc.).

La responsabilità del fornitore per i servizi di Ingegneria e Mano d'Opera e' relativa alle risorse fornite e non alle attività svolte od ai prodotti realizzati dalle risorse stesse.

3.3.3.9 Fornitura prodotti hardware e software [5.1.1 FPD]

La classe di Fornitura Prodotti Hardware e Software (FPD) e' relativa alla fornitura di prodotti hardware (che possono essere di varie tipologie, come personal computer o sistemi server o periferiche e accessori) e di prodotti software delle tipologie software di base, software di ambiente e software di rete. La classe comprende anche i servizi a "corredo" della fornitura (Consegna, Installazione, Configurazione, Collaudo, ecc.).

3.3.3.10 Gestione della configurazione [6.1.2 PGC]

La classe comprende le attività di Gestione della Configurazione, a supporto dei processi di sviluppo e manutenzione del software e dei processi di evoluzione e manutenzione dell'hardware, con lo scopo di assicurare la conoscenza, la completezza, l'integrità, la consistenza e la correttezza delle componenti di un sistema, in particolare in relazione alle dipendenze esistenti tra le stesse, attraverso la documentazione e l'aggiornamento della configurazione e la conoscenza dello stato delle modifiche proposte, della loro motivazione, della loro approvazione, della loro attuazione e della loro evoluzione.

3.3.3.11 Aspetti di sicurezza

I servizi dovranno essere svolti nel rispetto delle leggi vigenti in materia di sicurezza sul lavoro (D. Lgs 626/1994) e al trattamento dei dati personali (D. Lgs 196/2003).

Le parti interessate dovranno adottare un approccio globale della gestione della sicurezza. Le misure di protezione e le soluzioni devono essere allo stesso tempo, tecniche e non tecniche e commisurate al valore dell'informazione nei sistemi e reti d'informazione dell'organizzazione.

Nel documento di specifiche tecniche dovranno essere defini-

te, con descrizione completa, le tecnologie adottate, gli aspetti applicativi, i processi relativi al servizio e le modalità di test, collaudo e monitoraggio del servizio stesso.

Periodicamente dovrà essere compilato un rapporto che elenchi e descriva gli eventi anomali (comprendendo ogni singolo allarme) che si sono verificati nel corso del periodo di riferimento e le azioni che sono state intraprese, di conseguenza, per affrontare gli eventi anomali.

Nel caso di incidente dovrà essere dettagliato un rapporto sulle cause e sulle attività svolte per affrontare l'emergenza. Il rapporto sull'incidente riepiloga ed analizza gli eventi al fine di individuare le cause imputabili all'emergenza.

Dovranno inoltre essere programmati degli interventi periodici per garantire il buon funzionamento dei sistemi garantendo una elevata qualità dei servizi forniti.

Dovranno essere esplicitamente definiti i requisiti delle risorse (hardware, software ed umane; in questo ultimo caso le quantità e i profili professionali) utilizzate per svolgere il servizio.

Nel caso di fornitura del servizio di assistenza tecnica in modalità ASP, dovrà essere richiesta la descrizione della struttura organizzativa adottata dal fornitore con l'indicazione dei ruoli, competenze, profili professionali e delle risorse assegnate alla gestione ed al controllo del servizio e la descrizione dei documenti che verranno prodotti ed aggiornati nello svolgimento del servizio.

Per quanto concerne la sicurezza fisica gli amministratori di sistema IT dovranno applicare politiche di accesso restrittive, tramite strumenti tecnologici e procedurali, occupandosi inoltre delle attività di gestione e controllo delle utenze, dei relativi diritti e del monitoraggio degli accessi.

E' necessario inoltre gestire con particolare attenzione l'accesso alla rete aziendale di utenti appartenenti ad Aziende terze, i quali, solo nel caso di esigenze straordinarie, dovranno essere autorizzati a tale accesso, ma in via temporanea e limitatamente alle applicazioni riguardanti informazioni attinenti al particolare

compito assegnato.

Nel caso di servizi di gestione della sicurezza logica particolare attenzione dovrà essere rivolta alla scelta dei protocolli di comunicazione. E' inoltre indispensabile programmare, realizzare, gestire soluzioni che consentano di attuare il salvataggio e il riavvio immediato delle funzionalità informatiche e delle reti in caso di malfunzionamenti, calamità o attacchi dolosi che incidono sui sistemi primari, assicurando tempestività operativa e massimi livelli di sicurezza e di affidabilità.

Nel caso di servizi di fornitura di prodotti hardware e software particolare attenzione dovrà essere rivolta ai rischi legati alla fase di transizione tra i prodotti vecchi e nuovi.

Per la perfetta riuscita dei progetti relativi alla presente classe di fornitura, è fondamentale formare sui temi della sicurezza i sistemisti e l'utente finale. I servizi dovranno essere affidati a personale specializzato che segua procedure consolidate e adeguatamente monitorate.

3.3.4 Servizi di sviluppo software

Rientrano in questa categoria le seguenti classi di servizi:

3.3.4.1 Sviluppo e MEV di software ad hoc [1.1.1 SSW]

La classe include i servizi di sviluppo di applicazioni e di manutenzione evolutiva (MEV) di software esistente attraverso l'introduzione di nuove funzioni.

Lo sviluppo di software ad hoc comprende sia la possibilità di realizzare interi nuovi sistemi applicativi, sia la possibilità di realizzare parti autonome degli stessi che risolvano esigenze specifiche dell'Amministrazione.

La manutenzione evolutiva di software ad hoc comprende gli interventi volti ad arricchire un prodotto di nuove funzionalità o di altre caratteristiche non funzionali (quali l'usabilità, le presta-

zioni, ecc.) o comunque a modificare o integrare le funzionalità del prodotto.

3.3.4.2 Personalizzazione e MEV di prodotti esistenti [1.1.2 PSW]

La classe include i servizi di personalizzazione e manutenzione evolutiva di software esistente.

Questa classe tratta le attività volte al riuso di software già disponibile ed alla eventuale personalizzazione. Sono inclusi servizi di personalizzazione di applicazioni sviluppate secondo vari metodi e gli interventi per riusare (ed eventualmente arricchire) applicazioni software in uso presso altre Amministrazioni.

3.3.4.3 Sviluppo e MEV mediante soluzioni commerciali [1.1.3 SSC]

La classe comprende le attività relative alla parametrizzazione e alla personalizzazione di applicazioni software esistenti sul mercato in base ai requisiti richiesti dal cliente. Sono comprese attività di integrazione e personalizzazione di componenti e piattaforme di mercato (ERP; CRM; SRM; PLM; SCM, Business Intelligence, etc.).

La Manutenzione Evolutiva di software commerciale riguarda quelle attività relative all'introduzione di nuove funzioni, o l'evoluzione di funzioni preesistenti, oppure lo sviluppo di nuove funzionalità richieste dall'Amministrazione.

3.3.4.4 Manutenzione correttiva ed adeguativa [1.2.2 MAC]

La classe include tutte le attività che trattano la manutenzione correttiva (diagnosi e rimozione delle cause di malfunzionamenti di procedure e programmi) e la manutenzione adeguativa (volta invece ad assicurare la costante aderenza delle procedure e dei programmi all'evoluzione dell'ambiente tecnologico

dell'Amministrazione).

I servizi di questa classe si applicano sia a soluzioni software sviluppate ad hoc che a soluzioni che impiegano software commerciale, al quale si applicano significative parametrizzazioni e/o personalizzazioni.

3.3.4.5 Migrazione e conversioni applicazioni [1.2.3 MSW]

La classe di servizi di migrazione e conversione delle applicazioni consiste nella trasformazione di prodotti software da una piattaforma tecnologica ad un'altra, basata su una diversa architettura, lasciando inalterate tutte le funzionalità dell'applicazione di partenza.

3.3.4.6 Aspetti di sicurezza

Nel caso di servizi di sviluppo software sono da tenere presenti i seguenti aspetti.

Nel documento di specifiche funzionali devono essere definiti tutti gli aspetti dell'applicazione, in modo da ottenere una descrizione completa e non ambigua, che tenga conto anche delle funzionalità di sicurezza richieste.

Tale documento deve analizzare gli aspetti relativi alla sicurezza sia relativamente ai processi ed alle modalità con cui tali processi risulteranno visibili agli utenti finali, sia al disegno logico dei dati e alle relative modalità di accesso.

Devono inoltre essere definiti e documentati i requisiti di riservatezza e sicurezza legati sia ai dati che devono essere gestiti dall'applicazione, sia ai profili degli utenti.

In particolare, se lo sviluppo dell'applicazione prevede anche l'utilizzo di basi di dati, si deve tenere conto degli aspetti di sicurezza logica tipici della gestione delle basi di dati e dei sistemi.

Per quanto riguarda la manutenzione correttiva ed adeguativa

i criteri di valutazione della sicurezza devono essere presi in considerazione relativamente all'impatto che hanno sul livello di sicurezza complessivo del sistema, che possono essere alterati considerevolmente in attività di questo tipo.

3.3.5 Servizi di certificazione dei dati

Rientrano in questa categoria le seguenti classi di servizi:

3.3.5.1 Certificazione della firma digitale [2.3.1 CFD]

La certificazione della firma digitale è l'operazione con la quale si garantisce la corrispondenza biunivoca tra la chiave pubblica e il soggetto titolare cui essa appartiene, si identifica quest'ultimo e si attesta il periodo di validità di detta chiave. La certificazione viene compiuta dal certificatore, che la esercita firmando il certificato. La firma digitale certificata consente quindi al sottoscrittore di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici con assoluta certezza.

Al Titolare del Certificato viene rilasciato il dispositivo sicuro di firma contenente il Certificato di Firma Digitale, unitamente a tutti i prodotti e servizi accessori, descritti di seguito:

- Emissione e gestione del certificato di Firma Digitale, come definito dalla vigente normativa sulla documentazione amministrativa (TUDA dpr 445/2000 e successive modifiche) e gestito secondo le norme di qualità (UNI EN ISO 9002);

- Generazione di una coppia di chiavi almeno a 1024 bit, secondo procedimento di crittografia asimmetrica;

- Fornitura del dispositivo sicuro di firma;

- Fornitura del lettore di smart card (ove necessario);

- Fornitura del client software per la firma, la verifica delle firme

ed eventualmente per la cifratura dei documenti (dispositivo di verifica della firma);

- Fornitura della manualistica di supporto;

- Servizio locale di Registrazione dei Titolari.

Il servizio di certificazione digitale può anche essere ero gato in modalità ASP in soluzione "hosting" o "housing".

3.3.5.2 Posta elettronica certificata [2.2.3 PEC]

La posta elettronica certificata (PEC) è un sistema di e-mail che prevede, a fronte dell'invio da parte di un mittente, una serie di e-mail firmate dal sistema PEC che servono a certificare l'avvenuto invio e l'avvenuta consegna del messaggio originale non modificato.

Il servizio può essere oggetto di fornitura in modalità ASP, in soluzione "hosting" (dove il fornitore, utilizzando proprie infrastrutture e proprie piattaforme di erogazione, eroga servizi personalizzati per conto del cliente, ma non necessariamente fornisce anche i prodotti per la fruizione dei servizi) oppure in soluzione "housing" (dove il fornitore ospita e gestisce presso proprie infrastrutture gli apparati di proprietà dell'Amministrazione, necessari all'erogazione del servizio PEC). Infine può essere prevista una soluzione "on site" presso l'Amministrazione, gestita dal Provider, che assicura all'Amministrazione la fornitura della soluzione così come disegnata da un'apposita progettazione e provvede alla sua gestione locale e/o in remoto. Non sono previste attività di erogazione, mentre si possono prevedere attività di consulenza in fase di progettazione e le usuali attività di manutenzione. Si tratta di forniture destinate a bacini di utenza molto numerosi oppure con specifiche e stringenti esigenze di controllo di processo, tali da non poter essere soddisfatte dalle precedenti modalità.

3.3.5.3 Aspetti di sicurezza

La presente classe di servizi deve necessariamente soddisfare i seguenti requisiti:

- la firma deve essere basata su di un certificato qualificato ovvero emesso da un Certificatore Accreditato

- il Certificatore deve assicurare che un insieme di informazioni e di operazioni riguardanti il certificato risultino sempre disponibili in linea.

- i certificatori devono pubblicare nel Manuale Operativo tutte le informazioni relative alle modalità con cui il servizio viene erogato.

- la firma deve essere generata mediante un dispositivo sicuro per la creazione di una firma.

- deve essere garantita la conservazione della documentazione relativa all'identificazione per almeno dieci anni dalla scadenza dei certificati.

3.3.6 Servizi di consulenza, formazione e documentazione

Rientrano in questa categoria le seguenti classi di servizio:

3.3.6.1 Formazione e addestramento [1.3.2 FOR]

La classe include i servizi finalizzati all'aggiornamento e allo sviluppo delle competenze e delle capacità professionali delle risorse umane.

I servizi di formazione si caratterizzano per i contenuti, per le metodologie didattiche e per le modalità di realizzazione, che possono prevedere attività formative sia in aula sia in modalità di e-learning fruibili tramite supporto multimediale; oppure formazione on the job, tramite attività di addestramento, finalizzate allo sviluppo di abilità/conoscenze con particolare riferimento all'utilizzo di sistemi specifici, alla gestione di apparati ed applicazioni, ecc.

3.3.6.2 Consulenza [4.1.1 CON]

Nella classe di fornitura è trattato il servizio di consulenza inteso come un insieme integrato di attività di supporto come ad esempio:

- la pianificazione delle attività e supporto organizzativo;

- gli studi, analisi e ricerche per approfondire temi particolari e approntare modelli previsionali;

- supporto alle decisioni;

- supporto all'utente nella re-ingegnerizzazione dei processi supportati dal sistema informativo e nella definizione dei requisiti dei nuovi sistemi;

- valutazione dell'impatto dei cambiamenti normativi sul sistema informativo;

- analisi e valutazioni dell'impatto dovuto all'introduzione di una nuova tecnologia sulla organizzazione, sui processi amministrativi, sul sistema informativo preesistente.

3.3.6.3 Direzione lavori [4.1.2 DLA]

La classe comprende i servizi di consulenza professionale finalizzati ad assicurare una corretta azione di governo di un progetto o di un servizio e dei relativi contratti di fornitura.

Il servizio di Direzione Lavori si inserisce nella fase di realizzazione di prodotti e/o servizi informatici e comprende le attività di verifica e controllo in corso d'opera del corretto andamento delle attività di realizzazione, sia in relazione al rispetto dei requisiti progettuali, che al raggiungimento degli obiettivi previsti, in ottica di efficacia e di efficienza.

3.3.6.4 Gestione della documentazione [6.1.1 PGD]

La classe comprende le attività di gestione sistematica, secondo la norma ISO 9001, della documentazione, che comprende sia documenti veri e propri sia qualunque altra forma di rappresenta-

zione di informazioni prodotte nel ciclo di vita di una fornitura (tabelle, grafici, diagrammi di flusso, banche dati, prospetti).

Il processo si esplica attraverso un insieme di attività finalizzate a pianificare, progettare, produrre e distribuire i documenti necessari a tutte le entità organizzative interessate sulla base di regole, strumenti, standard definiti nel processo di Progettazione.

3.3.6.5 Gestione e processi organizzativi [6.1.2 PGE]

La classe include tutte le attività di conduzione di progetto per gli aspetti organizzativi e di coordinamento: la definizione della struttura di progetto e delle infrastrutture a supporto, la pianificazione delle attività e delle risorse, il coordinamento delle risorse assegnate al progetto, le attività di controllo dell'avanzamento, la gestione della documentazione e la valutazione e gestione dei rischi. Comprende anche la gestione dei processi di produzione, la pianificazione dello sviluppo e della formazione delle risorse assegnate al progetto.

3.3.6.6 Aspetti di sicurezza

I servizi dovranno essere svolti nel rispetto delle leggi vigenti relative al trattamento dei dati personali (D. Lgs 196/2003). Particolare attenzione dovrà essere rivolta alla riservatezza dei dati trattati e al riserbo delle conoscenze acquisite inerenti le attività svolte e l'organizzazione interna.

Dovranno essere esplicitamente definiti ruoli e responsabilità. La problematica progettuale dovrà essere necessariamente supportata da tutte la componenti aziendali attraverso un approccio unitario, definito e completo.

3.3.7 Servizi di controllo qualità

Rientrano in questa categoria le seguenti classi di servizi:

3.3.7.1 Controllo dei livelli di servizio [3.5.1 MLS]

La classe include tutte quelle attività finalizzate alla misura e rendicontazione degli indicatori individuati per il controllo della qualità dei servizi, sia nel caso di servizi erogati da un fornitore esterno, sia da una struttura interna,.

L'obiettivo primario è il controllo in corso di erogazione della qualità dei servizi, nell'ottica di:

- esercizio del controllo sulla conduzione dei contratti, monitoraggio di livelli di servizio relativi a specifici contratti di fornitura, dove viene necessariamente indicata anche la modalità di controllo e misurazione;

- monitoraggio del servizio offerto nel suo insieme all'utente, al fine di disporre di uno strumento decisionale sulla conduzione del servizio;

- supporto decisionale per futuri investimenti e interventi correttivi o migliorativi, siano essi in corso d'opera, in corso di erogazione o a scadenza del contratto.

3.3.7.2 Misura della customer satisfaction [4.1.3 MCS]

La classe comprende i servizi finalizzati a misurare la qualità percepita dall'utente di prodotti o servizi. Le attività prevalenti del servizio sono:

- pianificazione della misura;

- progettazione della misura;

- realizzazione della misura;

- produzione dei risultati della misura.

3.3.7.3 Assicurazione qualità [6.1.3 PAQ]

Questa classe comprende l'insieme delle attività sistematiche e pianificate messe in campo dal fornitore per dare adeguata con-

fidenza che i servizi e i prodotti contrattualmente forniti siano conformi ai requisiti di qualità attesi.

Mentre le caratteristiche e i requisiti di qualità sono riferiti al prodotto finito o al servizio erogato, il PAQ definisce le modalità e i momenti in cui è possibile intervenire durante il processo produttivo al fine di stimare la qualità del prodotto finale.

L'assicurazione della qualità è una delle strategie fondamentali per la gestione del rischio (Risk Management).

3.3.7.4 Aspetti di sicurezza

I servizi dovranno essere svolti nel rispetto delle leggi vigenti relative alla sicurezza sul lavoro (D. Lgs 626/1994) e al trattamento dei dati personali (D. Lgs 196/2003). E' requisito fondamentale per lo svolgimento delle attività la garanzia di imparzialità. "Per assicurare l'imparzialità, è necessario che le funzioni che si occupano di assicurare la qualità abbiamo autonomia ed autorità rispetto alle persone direttamente responsabili o dello sviluppo del software o della esecuzione delle attività previste a progetto (norma UNI CEI ISO/IEC 12207)".

Il processo di assicurazione qualità e i controlli di qualità devono essere chiari nelle specifiche e nelle modalità. I casi e le procedure di test dovranno essere completi ed accurati. I risultati delle attività di test e collaudo dovranno essere registrati e se necessario aggiornati.

La misura di customer satisfaction dovrà inoltre essere ripetuta periodicamente in modo da poter controllare la qualità percepita sui servizi misurati.

4 - La sicurezza nell'acquisto dei Servizi

In questo capitolo verranno affrontati i rischi e le contromisure comuni a tutti i servizi, descrivendo in particolare il ciclo di vita di un servizio.

Alcuni dei concetti fondamentali che verranno sviluppati sono:

- l'affidamento dei servizi in outsourcing che hanno un qualche impatto sulla sicurezza ICT (e non ICT) di fatto modifica l'analisi dei rischi, introducendo nuovi rischi (e nuove minacce) per l'Organizzazione che non sarebbero stati presenti se il servizio non fosse stato dato in outsourcing. Questa circostanza impone da una parte l'individuazione dei nuovi rischi (variabili al variare del servizio dato in outsourcing) e l'individuazione di nuove contromisure, sia tecniche sia procedurali/organizzative.

- Oltre all'individuazione dei nuovi rischi (e minacce), occorre considerare che il ricorso all'outsourcing può, in generale, trasferire la responsabilità della gestione di alcuni rischi dall'Organizzazione all'outsourcer. Questi trasferimenti devono essere effettuati in modo oculato e consapevole (non è opportuno che tutti i rischi siano "trasferiti") e che vengano regolati da contratti (SLA e OLA).

In questo senso, la presente Linea Guida "integra" le considerazioni svolte nelle altre Linee Guida dedicate alle analisi dei

rischi, che affrontano il problema dell'outsourcing solo marginalmente.

4.1 Modello di controllo degli outsourcer ed insourcer

Il ricorso all'outsourcing non può essere esteso a tutte le funzioni necessarie per gestire il rischio (ICT e non); occorre quindi individuare almeno alcuni modelli di riferimento che descrivano le funzionalità minime e/o ottimali che devono necessariamente essere realizzate all'interno dell'Organizzazione, senza ricorso all'outsourcing.

4.1.1 Introduzione al modello di controllo

È ormai esigenza consolidata che la Sicurezza dell'Informazione vada affrontata sia sul fronte manageriale/organizzativo, che su quello tecnologico. Di conseguenza, nessun sistema informativo può essere ritenuto sicuro senza che ci sia dietro una buona organizzazione ed una strategia manageriale mirata all'individuazione di ruoli, responsabilità, norme comportamentali ed attività da svolgere per garantire il mantenimento di un adeguato livello di Sicurezza in linea con le politiche dell'Organizzazione.

Un tale approccio alla Sicurezza, nelle ormai sempre più complesse realtà tecnologiche, deve coinvolgere ogni livello di elaborazione dell'informazione, in modo da impedire che l'anello più debole della catena comprometta gli sforzi complessivi.

L'intero processo di Gestione della Sicurezza dell'Informazione deve quindi coinvolgere in modo strutturato ed efficace anche tutti i fornitori che erogano servizi in outsourcing per conto dell'Organizzazione, così come tutti i gestori interni (insourcer), mediante la definizione e la condivisione puntuale di un Modello di Controllo che garantisca un modus operandi, sia dell'Organizzazione che dell'Outsourcer, conformemente alle politiche e direttive dell'Organizzazione in materia di Sicurezza.

Il seguito del presente capitolo propone una linea guida per la definizione di un Modello di Controllo che dovrà essere realizzato tenendo conto dell'ambito di applicazione, contesto e criticità dei servizi oggetto di outsourcing. Inoltre, il concetto di outsourcing può prevedere varie forme operative quali ad esempio la gestione dei servizi presso i locali del committente piuttosto che presso i locali del Fornitore. La presente esposizione (studio, ricerca) assume un carattere generale indipendente dalla particolare forma di outsourcing; l'applicazione, pertanto, del Modello di Controllo va adattata caso per caso, valutando e definendo le rispettive responsabilità tra Committente e Fornitore.

Si riportano qui di seguito le macro-componenti che costituiscono il Modello di Controllo degli Outsourcer/Insourcer che saranno descritte nei paragrafi successivi:

- Outsourcing Information Security Risk Management.
- Valutazione e selezione dell'Outsourcer.
- Definizione e contrattualizzazione delle politiche di sicurezza nell'erogazione dei servizi.
- Audit di Sicurezza dei Servizi in Outsourcing.

Si osservi che il Modello di Controllo qui trattato si riferisce ai soli aspetti di Sicurezza dell'informazione senza quindi entrare nel merito del servizio e relative caratteristiche da affidare in outsourcing.

4.1.2 Outsourcing Information Security Risk Management

Con l'affidamento di un Servizio in outsourcing il Fornitore diventa a tutti gli effetti un Partner che entra a far parte del ciclo operativo dell'Azienda e della sua catena del valore. Ciò implica che una nuova Organizzazione "virtuale" si configura, con la conseguente introduzione di nuovi rischi per il bene "Informazione"

a cui l'Organizzazione deve far fronte in modo adeguato sin dall'inizio.

Da ciò deriva l'esigenza di definire ed adottare uno specifico processo di analisi e gestione dei rischi, focalizzato sugli aspetti d'integrazione dei fornitori nella struttura organizzativa per l'erogazione dei servizi in outsourcing.

L'Outsourcing Information Security Risk Management rappresenta quel processo che, partendo dalla valutazione della criticità del servizio da affidare in outsourcing, consente di definire i livelli di rischio per il bene informazione derivanti dall'affidamento dello stesso ad un Fornitore e di delineare le contromisure idonee alla gestione efficace di tale rischio, il tutto in relazione alle politiche di sicurezza dell'Organizzazione.

Dall'Outsourcing Information Security Risk Management ne deriverà quindi un insieme dei controlli di sicurezza da adottare per la mitigazione del rischio (siano esse di natura organizzativa piuttosto che tecnologica) che, relativamente al contesto, in parte potranno essere a carico dell'Organizzazione, in parte a carico dell'Outsourcer ed in parte ad entrambi.

L'Outsourcing Information Security Risk Management, nel complesso, consente di ampliare il processo di Information Security Risk Management dell'Organizzazione per far fronte alla nuova "Organizzazione Virtuale" determinando l'applicazione delle politiche di Sicurezza dell'Organizzazione all'intera Organizzazione Virtuale e quindi anche ai partner coinvolti nell'outsourcing dei servizi.

Risulta importante sottolineare che: da un lato l'Outsourcing Information Security Risk Management non deve operare in modo indipendente dal processo di Information Security Risk Management ma ne costituisce un'estensione che ne amplia l'ambito di applicazione, dall'altro la ciclicità operativa deve tener fortemente conto della dinamicità del processo di outsourcing in quanto dipendente da fattori e cambiamenti esterni all'Organizzazione, e quindi indipendenti da essa, che devono essere necessariamente sottoposti a frequenti controlli.

Infine, l'Outsourcing Information Security Risk Management deve accompagnare tutto il ciclo di vita del processo di outsourcing. Esso pertanto deve trovare applicazione sin dal principio, intervenendo dalle prime fasi decisionali sull'esternalizzare o meno di un servizio (il risultato dell'analisi dei rischi potrebbe evidenziare un'eccessiva pericolosità nel passaggio all'outsourcing), alla scelta del Fornitore e continuare ad essere manutenuto per tutta la durata del processo di outsourcing e nella gestione di tutte le sue forme ed evoluzioni. Infatti, da esso deriva un notevole supporto nella scelta del Fornitore, nella contrattualizzazione dei controlli di sicurezza organizzativa, fisica e logica da adottare e fornisce inoltre un contributo alla valutazione degli investimenti per la gestione degli impatti sulla sicurezza e quindi all'applicazione delle politiche di sicurezza dell'Organizzazione nell'adozione dell'outsourcing.

4.1.3 Valutazione e Selezione dell'Outsourcer

La scelta di un Fornitore dei servizi in outsourcing adeguato è il risultato di un complesso processo di valutazione che va dall'analisi delle capacità professionali dell'Outsourcer, all'accertamento di un'adeguata esperienza nel settore, alla valutazione dell'organizzazione e delle dimensioni del Fornitore che devono essere commisurati all'entità ed alla qualità del servizio da erogare, alla valutazione tecnico-economica di quanto offerto in relazione ai requisiti richiesti propri del servizio da affidare in outsourcing.

In generale, l'Outsourcer deve di conseguenza dare le massime garanzie di affidabilità e di competenza, oltre che offrire un ottimo rapporto qualità/ prezzo.

Quanto indicato precedentemente costituisce però una condizione necessaria ma non sufficiente per una scelta ottimale del Fornitore nell'ottica più globale del servizio, che include tutte le considerazioni in materia di sicurezza.

La scelta del Fornitore, di fatto, non può prescindere nè dalla valutazione delle capacità professionali in ambito di sicurezza, nè

dall'analisi delle modalità con cui il Fornitore intende garantire tutti gli aspetti di Information Security relativi al servizio oggetto di outsourcing nella misura anche determinata dai risultati del processo di Outsourcing Information Security Risk Management precedentemente trattato. In generale, quindi, gli aspetti su cui focalizzare l'analisi valutativa sono due:

Maturità del Fornitore nell' "Organizzazione della Sicurezza" che rappresenta un prerequisito di fondamentale importanza e che assume sempre più peso in dipendenza della sensibilità e criticità del servizio.

Aspetti tecnico-economici relativamente all'integrazione delle contromisure di sicurezza logica, fisica ed organizzativa, determinati dall'Outsourcing Information Security Risk Management, nel processo di gestione proprio del servizio da affidare in outsourcing.

Si vuole qui soffermare l'attenzione sul concetto di "Maturità in materia di Organizzazione della Sicurezza".

Come anticipato nei precedenti paragrafi, la Sicurezza dell'Informazione va affrontata, oltre che sul piano tecnologico, anche sul fronte manageriale/organizzativo; attraverso la definizione di uno specifico framework organizzativo che consenta il raggiungimento ed il mantenimento di adeguati livelli di protezione in relazione agli obiettivi di sicurezza dell'Organizzazione.

A tal proposito è opportuno citare lo standard BS7799, recepito dall' ISO/IEC come 17799 (BS7799:1) e 27001 (BS7799:2), che rappresenta il punto di riferimento mondiale in materia di "Organizzazione della Sicurezza".

La norma definita dal British Standard BS 7799, infatti, introduce il concetto di Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) per una più efficace tutela della riservatezza, integrità e disponibilità dell'informazione stessa, in relazione al business dell'Organizzazione e all'insieme delle norme e direttive nazionali ed internazionali.

Il Sistema di Gestione per la Sicurezza dell'Informazione è il complesso di regole, procedure e misure di protezione di tipo fisi-

co, logico ed organizzativo, attuate e mantenute dall'organizzazione per garantire, nel tempo, il compimento della politica di sicurezza. I controlli e le procedure per la sicurezza delle informazioni devono essere gestiti e mantenuti costantemente nel tempo.

Tale Sistema di gestione, includendo dei "feedback loops", consente inoltre il monitoraggio e il controllo efficace della sicurezza dell'Informazione, minimizzando il rischio residuo ed assicurando la continuità del business nel soddisfacimento dei requisiti aziendali.

E' importante quindi a riguardo che l'Outsourcer sia già dotato di una propria "Organizzazione della Sicurezza", ovvero abbia adottato un "Sistema di Gestione per la Sicurezza dell'Informazione" che abbia raggiunto uno sviluppo tale da offrire i livelli di sicurezza richiesti dall'Organizzazione per l'outsourcing del servizio.

Solo attraverso un'adeguata maturità nell'ambito di Security si possono offrire livelli di sicurezza idonei alle aspettative dell'Organizzazione, in quanto, la Sicurezza non è un qualcosa di aggiuntivo ma un vero e proprio modo di operare, una forma mentis raggiungibile solo attraverso una graduale integrazione del processo di Sicurezza coi processi interni fino a diventarne parte integrante.

La maturità dell'Outsourcer deve infine esse tangibile e dimostrabile, e quindi accertabile da parte dell'Organizzazione che intende affidare un servizio in outsourcing. A riguardo, elemento di discriminazione potrebbe essere il possesso di un "Sistema di Gestione per la Sicurezza dell'Informazione" Certificato in riferimento a standard riconosciuti quali ad esempio il sopra citato BS7799.

4.1.4 Definizione delle politiche di sicurezza

Un aspetto rilevante ai fini del rispetto dei requisiti di Information Security relativi al servizio da trasferire in outsourcing è la contrattualizzazione degli SLA di sicurezza, ossia l'impegno formale da parte del Fornitore al rispetto e all'applicazione

delle politiche di Sicurezza dell'Organizzazione nell'ambito della fornitura del servizio in outsourcing.

Nel presente paragrafo si fornisce una visione d'insieme di ciò che dovrebbe essere preso in considerazione contrattualmente, facendo osservare che l'adozione di quanto indicato dipenderà dal contesto di applicazione ed in particolare dalle caratteristiche e criticità dei servizi da affidare in outsourcing.

In generale, gli aspetti di Information Security su cui focalizzare l'attenzione nel processo di contrattualizzazione sono i seguenti:

- Definizione del perimetro di azione Fisico e Logico del fornitore.
- Definizione delle Responsabilità di Security, nell'ambito delle specificità del servizio offerto.
- Protezione degli asset informativi ed attuazione e manteni mento di idonee contromisure logiche, fisiche ed organizzati ve, con relativa garanzia di performance e modalità di reporting.
- Confidenzialità unilaterale/bilaterale e proprietà intellettuale.
- Gestione del Subappalto: divieto di subappalto o garanzia di rispetto della security da parte dei Subappaltatori.
- Conformità con i requisiti legislativi e standard di riferimento.
- Responsabilità di Privacy, secondo quanto dettato dalla legislazione.
- Definizione di un idoneo processo per la gestione degli incidenti.
- Diritto di Monitoraggio e Audit da parte dell'Organizzazione o suoi delegati.
- Requisiti di Business Continuity
- Flessibilità della prestazione legata al cambiamento del business e/o requisiti di sicurezza e definizione di un processo di gestione del cambiamento.

- Livello di formazione e sensibilità alle tematiche di security delle risorse impiegate.
- Controllo di frequenza del "turnover".

4.1.4.1 Definizione del perimetro di azione Fisico e Logico del Fornitore

Sin dalla fase di contrattualizzazione va puntualmente definito il perimetro di azione che il Fornitore deve rispettare nell'ambito della fornitura del servizio in outsourcing.

Il perimetro di azione dovrà essere considerato definendo sia l'ambito logico (sistemi, applicazioni, ecc..) che fisico (locali, aree, ecc..) e per ognuno di essi vanno anche fissati i rispettivi livelli di accesso (es. utenze administrator piuttosto che user).

Inoltre, durante l'erogazione del servizio, è opportuno che gli aspetti di formalizzazione del perimetro di azione vadano sempre mantenuti aggiornati in seguito ad eventuali cambiamenti dovuti per esempio ad evoluzioni del servizio.

4.1.4.2 Definizione delle Responsabilità di Security

All'interno dell'intero framework organizzativo di outsourcing, è importante che siano identificati e definiti in generale i compiti e le responsabilità del personale dell'Outsourcer per lo specifico servizio (amministratori di sistema, addetti al trattamento dei dati personali, security team, team di incident management, ecc.) ed in particolare, per quanto concerne i propri addetti alla sicurezza. Infatti, il team degli esperti di sicurezza del fornitore dovrà avere ruoli e responsabilità ben definite. Tale Team dovrà essere caratterizzato da specialisti aventi, quanto meno, i seguenti ruoli:

- Responsabile della Sicurezza,
- Security Manager,

- Security System Architect, Security Application Architect e Security Network Architect relativamente al contesto e alle contromisure eventualmente adottate.

Per personale con funzioni di elevata criticità (ad esempio addetti al trattamento dei dati personali) deve essere siglata una dichiarazione di confidenzialità: le informazioni accedute non devono essere pubblicate e/o trasferite a terze parti o a personale interno non autorizzato.

Inoltre, anche i collaboratori esterni dell'Outsourcer devono essere sottoposti alle stesse procedure con clausole ugualmente stringenti.

4.1.4.3 Protezione degli asset informativi ed attuazione e mantenimento di idonee contromisure logiche, fisiche ed organizzative, relativa garanzia di performance e modalità di reporting

Riguarda la formalizzazione dell'impegno da parte del Fornitore a realizzare l'insieme di contromisure idonee a garantire i livelli di sicurezza richiesti dall'Organizzazione.

Relativamente a ciascuna contromisura vanno puntualmente definiti: sia gli SLA di performance che dovranno essere garantiti dal Fornitore, sia tutto il framework di reportistica che dovrà essere prodotta al fine di consentire all'organizzazione di valutare l'efficacia di quanto messo in atto.

4.1.4.4 Confidenzialità unilaterale/bilaterale e proprietà intellettuale

Un elemento da considerare con particolare attenzione è la formalizzazione degli aspetti inerenti il rispetto della confidenzialità delle informazioni relative al servizio da trasferire in outsourcing, che in taluni casi va affrontata sia in modo unilaterale che bilaterale. Infatti, il non rispetto di idonee contromisure volte a garantire tale requisito potrebbe provocare notevoli danni all'Organizzazione con impatti non solo sugli aspetti di business ma anche legali e di immagine.

In ultima analisi non vanno trascurati gli adempimenti atti a garantire la protezione della proprietà intellettuale.

4.1.4.5 Gestione del Subappalto:

All'interno della fase di formalizzazione degli obblighi contrattuali in materia di sicurezza è buona pratica prendere in esame gli aspetti inerenti la gestione dei subappalti. Nello specifico, devono essere definite le modalità con cui l'Outsourcer può operare in tale ambito.

In particolare, deve essere chiaramente esplicitato se e in quale misura l'Outsourcer può ricorrere a subforniture; in tal caso deve esser fatto obbligo all'Outsourcer di contrattualizzare l'applicazione e il rispetto delle misure di sicurezza richieste dall'Organizzazione verso il Subfornitore.

Allo stesso modo, anche il Subfornitore dovrà a sua volta definire tali misure nell'eventuale subappalto di lavori.

4.1.4.6 Conformità con i requisiti legislativi e stan dard di riferimento

Un aspetto di rilievo da prendere in considerazione e quindi formalizzare è il contesto normativo, legislativo e gli standard di riferimento, come ad esempio BS7799, identificati dall'Organizzazione.

L'Outsourcer deve: sia ottemperare alle disposizioni legislative vigenti, che possono anche variare a seconda della dislocazione geografica dei sistemi e della trasmissione dell'informazione tra sistemi dislocati in Stati diversi, sia rispettare puntualmente quanto richiesto dall'Organizzazione in relazione ad eventuali standard considerati come riferimento.

Per quanto concerne il contesto normativo italiano è opportuno sottolineare l'importanza che assume il rispetto del Testo Unico sulla Privacy e quindi la chiara definizione dei compiti e responsabilità per il trattamento dei dati personali nella specifici-

tà del servizio da trasferire in outsourcing.

Inoltre, è necessario formalizzare come l'Outsourcer garantirà il mantenimento e la disponibilità di copie della documentazione progettuale pertinente per dimostrare l'osservanza dei requisiti legislativi in caso di controlli da parte degli organi di sorveglianza competenti.

4.1.4.7 Definizione di un idoneo processo per la gestione degli incidenti

Per incidente si intende qualsiasi evento accidentale che causi un danno agli asset informativi dell'Organizzazione.

L'Outsourcer deve garantire una struttura di gestione degli incidenti che assicuri la possibilità di rispondere in modo rapido ed efficace al verificarsi di un incidente. In particolare, deve essere previsto il contenimento e la riparazione del danno derivante dagli incidenti e la prevenzione dai danni futuri.

Il processo di gestione deve inoltre includere un'attenta e tempestiva attività di notifica dell'incidente all'Organizzazione, comunicando informazioni quali:

- la tipologia dell'incidente e le eventuali responsabilità,
- il bene coinvolto,
- la data e l'ora dell'incidente,
- i tempi stimati di ripristino,
- le eventuali azioni già intraprese e/o da intraprendere.
- l'avvenuta risoluzione dell'incidente.

4.1.4.8 Diritto di Monitoraggio e Audit da parte dell Organizzazione o suoi delegati

Sia le attività di Monitoraggio che di Audit rappresentano uno strumento efficace per l'Organizzazione al fine di valutare che quanto messo in opera risponda ai requisiti predefiniti.

Nella contrattualizzazione è pertanto fondamentale formalizzare il diritto da parte dell'Organizzazione di effettuare attività di monitoraggio ed audit, specificando opportunamente le modalità ed i tempi con cui tali attività saranno svolte.

4.1.4.9 Requisiti di Business Continuity

La Business Continuity nell'outsourcing è costituita da tutti quei servizi che assicurano la continuità del servizio al verificarsi di eventi che ne compromettono l'operatività. Pertanto, nella definizione degli impegni contrattuali dell'Outsourcer, uno degli aspetti che dovrebbe essere preso in esame è la responsabilità del fornitore nel garantire i requisiti di Business Continuity.

A tal proposito, gli aspetti che dovrebbero essere presi in esame saranno trattati nei prossimi paragrafi.

4.1.4.9.1 Disaster/Recovery

Nel caso si verificasse un evento disastroso, il Disaster Recovery garantisce il ripristino dell'erogazione dei servizi, secondo determinati tempi e priorità operative. Per evento disastroso si intende un evento accidentale o doloso che renda inutilizzabili le infrastrutture e i sistemi per un tempo tale da compromettere il business, la produttività o l'immagine dell'Organizzazione.

4.1.4.9.2 High Availabilty

L'alta disponibilità si basa sulla predisposizione di più sistemi configurati in modo da operare come una singola entità funzionale. Ciò consente di spostare l'erogazione di un servizio da un sistema primario, che ha subito un failure, ad un sistema secondario pronto a subentrare; ottenendo in tempi brevi un ripristino del servizio da essa erogato.

A seconda dalla criticità del servizio, andranno definiti livelli di servizio idonei a garantire tempi di disservizio accettabili per l'Organizzazione.

4.1.4.9.3 Back-up/Restore

È importante che sia garantita dall'Outsourcer la regolarità di esecuzione delle copie di back-up secondo una procedura formale ben definita. La frequenza dei back-up deve essere commensurata all'importanza delle informazioni relative al servizio.

L'Outsourcer deve inoltre proteggere le copie di back-up contro furti, manomissioni, danneggiamenti e disastri naturali custodendole in locali sicuri e conformi ai requisiti della politica di accesso fisico.

4.1.4.10 Flessibilità della prestazione legata al cambiamento del business e/o requisiti di sicurezza e definizione di un processo di gestione del cambiamento

Il fornitore dovrà garantire un approccio flessibile nell'erogazione del servizio in outsourcing in relazione ad eventuali cambiamenti che potrebbero coinvolgere gli aspetti di sicurezza. Infatti, cambiamenti riguardanti gli obiettivi di business e/o requisiti di sicurezza dell'Organizzazione potrebbero implicare eventuali impatti sul servizio, in particolare, sugli aspetti di security ad esso associati. In ciò il fornitore deve dare sin dal principio la propria disponibilità a farsi carico dell'adeguamento degli aspetti di security secondo quanto richiesto dall'Organizzazione.

A riguardo, è buona pratica definire e condividere già in fase di contrattualizzazione un opportuno processo di gestione dei cambiamenti.

4.1.4.11 Livello di formazione e sensibilità alle tematiche di security delle risorse impiegate

E' opportuno richiedere al fornitore che le risorse impiegate per l'erogazione del servizio in outsourcing siano opportunamen-

te formate e sensibilizzate sugli aspetti di security, prevedendo ove necessario opportune sessioni di training specialistiche.

4.1.4.12 Controllo di frequenza del turnover"

Un ulteriore aspetto che andrebbe preso in esame è il turnover delle risorse impiegate nell'erogazione del servizio in outsourcing. Infatti, un elevato turnover del personale potrebbe avere impatti non solo sulla qualità del servizio ma anche sugli aspetti di security.

A tale proposito quindi, sin dalla fase di contrattualizzazione è necessario condividere un adeguato processo che regoli il turnover del personale in relazione agli obiettivi di sicurezza dell'Organizzazione.

4.1.5 Audit di Sicurezza dei Servizi in Outsourcing

Il processo di auditing è un elemento fondamentale all'interno di ogni sistema di gestione e quindi di un Sistema di Gestione per la Sicurezza dell'Informazione (SGSI).

L'adozione di un processo di Auditing rappresenta uno strumento di gestione per tenere sotto controllo e verificare l'efficace attuazione dei livelli qualitativi prefissati, rilevando le potenziali criticità o aree di rischio e proponendo, se necessario, le misure o best-practice per il raggiungimento dei livelli desiderati.

Nel caso di affidamento dei servizi in outsourcing, relativamente agli aspetti di security, viene a costituirsi di fatto un Sistema di Gestione per la Sicurezza dell'Informazione che prevede come ambito di applicazione il servizio in outsourcing e la cui efficacia assume sempre più importanza in relazione alla criticità del servizio.

A riguardo, come per ogni sistema di gestione, è di conseguenza necessario sottoporre il SGSI del servizio in outsourcer ad un continuo processo valutativo che ne analizzi costantemente l'efficacia in relazione agli obiettivi di sicurezza prefissati e contrattualizzati; il tutto secondo un approccio metodologico ben

strutturato e predefinito.

Senza entrare nel merito delle attività proprie del processo di Auditing, per le quali si rimanda a standard e best-practice internazionalmente riconosciuti (quali ad esempio UNI EN ISO 19011), si vuole qui sottolineare l'importanza che assume l'attuazione di un efficace processo di Audit di Sicurezza all'interno di tutto il processo di affidamento dei Servizi in Outsourcing e si vogliono evidenziare quali devono essere gli obiettivi primari dell'Audit di Sicurezza dei Servizi in Outsourcing in quanto esso deve essere guidato da una duplice visione, una focalizzata sugli aspetti Contrattuali formalizzati con il Fornitore e l'altra sulle Politiche di Sicurezza dell'Organizzazione. Precisamente:

- In relazione agli impegni assunti dall'Outsorcer per gli aspetti di security in sede di contrattazione, l'Audit di Sicurezza deve verificare che quanto messo in atto sia rispondente a quanto contrattualmente definito

- In relazione alle Politiche di Sicurezza dell'Organizzazione, l'Audit di Sicurezza deve verificare l'efficacia di quanto messo in atto; identificando eventuali aree di miglioramento o evoluzioni dovute magari a cambiamenti degli obiettivi originariamente prefissati.

In ultima analisi, il quadro di gestione della sicurezza (o SGSI) relativo al servizio in outsourcing potrebbe essere adottato, cosa auspicabile, in conformità a modelli o standard quali BS7799. In tal caso gli obiettivi primari dell'Audit di Sicurezza ne risulterebbero estesi in quanto dovrebbero comprendere anche la valutazione di conformità rispetto allo standard adottato come riferimento.

4.1.5.1 Lo standard SAS 70

Lo "Statement on Auditing Standard" (SAS) No. 70, Service Organizations, è uno standard di Audit emesso da American Institute of Certified Public Accountants (AICPA) che indica le regole di comportamento e fornisce la guida per abilitare un Revisore Service all'emissione di un'opinione indipendente sulla

descrizione dei controlli fornita da una Service Organization attraverso un Service Auditor's Report (si veda successivamente).

Il SAS 70 è stato originariamente sviluppato per supportare le attività di revisione di bilancio da parte dei revisori contabili. Attualmente, il SAS 70, si è affermato anche come standard per le attività di revisione della conformità di un'Entità ai fini del Sarbanes Oxley Act 2002 (Report di Tipo 2, si veda di seguito).

Prima di svolgere le considerazioni sullo standard SAS 70, introduciamo il significato dei seguenti termini:

- Service Organization: un'azienda che eroga servizi come ad esempio: un ASP, un Internet Data Center o un centro per il processamento di transazioni bancarie. Tale termine è da intendersi equivalente al termine Outsourcer usato nel resto del documento.

- Cliente: un utente dei servizi offerti da una Service Organization.

- Revisore del Cliente: l'Entità incaricata delle revisione del bilancio della Società "Cliente".

- Revisore del Servizio: l'Entità incaricata di fornire un Report SAS 70 alla Service Organization.

Il processo di Audit svolto in conformità al SAS 70 si conclude sempre con un report (i.e. "Service Autitor's Report") che viene rilasciato dal Revisore Service alla Service Organization al termine del lavoro.

SAS 70 non specifica un insieme di obiettivi di controllo o attività di controllo (come COBIT o ISO 17799) che la Service Organization deve raggiungere o possedere, ed è genericamente applicabile qualora il Revisore del Cliente stia revisionando il bilancio di un Cliente che fa uso dei servizi forniti dalla Service Organization.

Uno dei modi più efficaci per una Service Organization al fine di comunicare informazioni sui propri controlli è il "Service Auditor's Report". Esistono due tipi di Service Auditor's Report: di Tipo 1 e di Tipo 2.

Nel Report di Tipo 1, il Revisore Service esprime un'opinione su:

- la rappresentazione imparziale della descrizione dei controlli, in tutti gli aspetti rilevanti, gli aspetti rilevanti dei controlli della Service Organization che sono stati implementati e operanti a partire da una specifica data;

- l'adeguato disegno dei controlli per il raggiungimento degli obiettivi di controllo.

Questa tipologia di report è molto utile per fornire al Revisore del Cliente della Service Organization la comprensione dei controlli necessari a pianificare l'audit sul Cliente, disegnare i test ed eseguirli in maniera indipendente.

Nel Report di Tipo 2, il Revisore Service esprime un'opinione sugli stessi argomenti del Report di Tipo 1 ed inoltre:

- sul fatto che i controlli verificati presentino un sufficiente livello di efficacia per fornire una ragionevole, ma non assoluta, confidenza che gli obiettivi di controllo sono stati assolti.

Questa tipologia di report è utile per fornire al Revisore del Cliente della Service Organization la comprensione dei controlli necessari a pianificare l'audit sul Cliente, inoltre possono fornire una base per valutare al ribasso i rischi relativi all'assenza di tali controlli.

Gli Audit ai fini del rilascio di un Report SAS 70 sono svolti da professionisti con esperienza di contabilità, Audit e Sicurezza delle Informazioni.

Il rilascio di un report SAS 70 può essere svolto soltanto da enti registrati presso AICPA.

Per le Service Organization il valore di un Service Auditor's Report SAS 70 risiede:

- nella differenziazione dell'offerta rispetto ai suoi peer nell'industria di riferimento;

- nel tempo risparmiato per il personale di Operation della Service Organization nelle molteplici attività di audit da parte dei

clienti dell'Entità (in molti casi il "Service Auditor's Report" soddisferà a tutte le richieste da parte del Revisore del cliente);

- nell'identificazione di opportunità di miglioramento a seguito del processo di Audit;

Per i Clienti il valore di un Service Auditor's Report SAS 70 risiede nella:

- comprensione dei controlli della Service Organization e della loro efficacia;

- valutazione dell'implementazione e dell'efficacia operativa dei controlli (solo Tipo 2);

- riduzione dei costi associati alle attività di revisione del bilancio interne (svolte da Revisori certificati).

Per quanto concerne l'ambito di analisi della presente sezione si nota, in questo contesto, il fatto che per il rilascio di un Report SAS 70 non venga specificato alcun insieme di controlli o attività di controllo specifiche.

Tutto ciò implica che non necessariamente un Service Auditor's Report SAS 70 possa essere di utilità nelle attività specifiche di Audit della Sicurezza del servizio di outsourcing, oggetto della presente sezione.

In caso però di presenza di un Report SAS 70, sarà necessaria la valutazione di personale professionista esperto (preferibilmente qualificato come Revisore, per essere in grado di comprendere l'opinione tecnica) nelle tematiche di Risk Management e Information Security al fine di stabilire l'effettiva utilità ai fini dell'Audit di Sicurezza del servizio di Outsourcing che si vuole svolgere.

E' di fondamentale importanza notare che tale Report SAS 70 dovrebbe essere considerato congiuntamente con la descrizione dei controlli del Cliente per avere una valutazione completa della Sicurezza del servizio di Outsourcing.

4.2 Service Out-Sourcing

4.2.1 Contratti

Da un certo numero di anni si è diffusa presso le aziende la necessità di affidare a società esterne quelle attività che non risultano direttamente attinenti ai processi produttivi principali, ad esempio la gestione dei cedolini paga e di tutti gli aspetti correlati, i call center, le strutture ICT, etc.

Il mercato richiede, o per meglio dire impone, alle aziende di raggiungere un livello di qualità e flessibilità molto alto e questo comporta una razionalizzazione dei processi connessi al ciclo produttivo.

In questo contesto alle strutture ICT viene richiesto un elevato grado di flessibilità ed adattabilità alle condizioni del mercato ed in parallelo il controllo dei costi operativi: ecco perché l'outsourcing, nell'accezione più ampia del termine, assume un importanza rilevante.

In genere le aziende decidono di affidare ad organizzazioni esterne specializzate le attività ICT non solo per meglio focalizzarsi sulle attività a maggior valore aggiunto ma anche per contenere i costi in modo da avere i servizi ed i prodotti necessari per il proprio sviluppo, trasformando un costo in un canone d'uso dei servizi utilizzati.

La riduzione dei costi deriva dalle economie di scala che il fornitore di servizi riesce a realizzare.

Per un'azienda esternalizzare comporta il passaggio della disponibilità di beni e servizi da rapporti in seno alla stessa azienda a rapporti fra soggetti diversi che necessitano di un adeguata disciplina contrattuale in cui nulla deve essere lasciato al caso o alla buona volontà.

I contratti di esternalizzazione, nella pratica corrente, oltre alla disciplina italiana risentono anche di contaminazioni legate ai modelli proposti da grandi operatori internazionali e la loro struttura varia con la tipologia dei servizi erogati.

In generale dovrebbero essere strutturati in modo da prevedere:

- una parte generale, in pratica la parte giuridica regolata dal codice civile; in particolare dovrebbero essere sempre presenti clausole relative:

- alla tutela a fronte di violazioni di brevetti e copyright;

- alla cessione del contratto, al subappalto;

- alla cessione del credito;

- al vincolo della riservatezza e della protezione dei dati.

- capitolati d'appalto, sinteticamente potrebbero essere:

- disciplinare economico, descrive i corrispettivi corrisposti all'appaltatore per i servizi resi;

- disciplinare dei livelli di servizio, in esso vengono definite le prestazioni, i livelli di servizio e i parametri quantitativi (minimi e massimi);

- disciplinare operativo, contiene i servizi e la modalità di resa, sicurezza (back-up e disaster recovery), controllo dei servizi;

- disciplinari tecnici.

In taluni casi al contratto di esternalizzazione possono essere collegati altri contratti relativi ad esempio alla cessione dell'hardware, del software, di immobili, di altri beni, ed accordi relativi al trasferimento o cessione di personale.

L'offerta dei servizi di outsourcing nel settore ICT si è molto specializzata nel corso degli anni, una possibile classificazione è quella di seguito riportata:

- Service Contract;

- Outsourcing;

- Facility Management;

- Application Service Providing;

- Disaster Recovery;

- Web Hosting e Web Housing.

Nel seguito verranno brevemente descritti i vari modelli.

4.2.1.1 Service Contract

In pratica è il primo esempio di contratto di esternalizzazione di servizi o funzioni ICT. In genere riguarda l'acquisizione dati (data entry) e la successiva elaborazione (pre-processing).

4.2.1.2 Outsourcing

È la tipologia più complessa ed articolata di contratto e può comprendere:

- la messa a disposizione dell'hardware e del software;
- la gestione tecnico operativa;
- le prestazioni sistemistica-applicative;
- la manutenzione delle applicazioni;
- le attività di sviluppo delle applicazioni;
- la manutenzione dell'hardware;
- l'aggiornamento tecnologico;
- i servizi di interconnessione;
- i servizi di Business Continuity e Disaster Recovery;
- i servizi di call center ed help desk;
- i servizi di gestione della sicurezza.

In pratica i servizi di outsourcing sopra descritti possono venire erogati sia presso l'azienda sia in remoto attraverso una connessione di rete.

In questa tipologia è opportuno inserire, oltre alle clausole sopra citate, ulteriori clausole per meglio disciplinare i rapporti fra i vari attori del contratto. A tale scopo è opportuno inserire le seguenti clausole:

- periodo di migrazione, passaggio di consegne e partenza delle attività, in modo da stabilire "chi fa cosa" e "come";

- verifica dei parametri contrattuali, nei casi in cui sia complesso stabilire parametri qualitativi e quantitativi per la valutazione dei servizi, in tale modo si ha la possibilità di modificare i parametri di qualità in corso di validità del contratto;

- attivazione del servizio;

- decorrenza, durata e recesso anticipato, data la complessità del servizio questo tipo di contratti richiedono una durata compresa fra i 5 e i 10 anni, in queste clausole dovrebbero essere riportate anche le attività che devono essere svolte in caso di recesso;

- software applicativo e software di base del committente, dell'appaltatore;

- auditing, una parte terza, esterna al committente ed all'appaltatore, svolge un controllo sull'appaltatore per valutarne, periodicamente, il livello di sicurezza operativa e controlli il livello del servizio reso;

- garanzie e rappresentazioni delle parti;

- responsabilità delle parti ed obblighi di indennizzo;

- penalità per il mancato rispetto degli indicatori di qualità;

- diffida ad adempiere;

- risoluzione per inadempimento;

- esclusione di responsabilità;

- fatturazione e pagamenti;

- gestione del contratto;

- arbitrato;

- clausole generali.

L'elenco delle clausole sopra riportato è valido in generale e per questo non è esaustivo in quanto devono, sempre, essere

tenute in conto le necessità degli attori del contratto e la tipologia del servizio reso.

Inoltre, questa tipologia di contratto risulta complessa per il fatto che in alcuni casi è previsto il trasferimento del personale del committente o la cessazione; questo è un argomento particolarmente delicato che necessita di un confronto fra servizio legale, servizio personale ed organizzazioni sindacali.

4.2.1.3 Facility Management

Questa tipologia di contratto, più semplice della precedente, riguarda la gestione sistemistica delle risorse hardware e del software di base della soluzione informatica del committente, senza che avvenga un trasferimento dei beni e senza ulteriori servizi.

Ovviamente in questo caso il committente gestisce in proprio le applicazioni informatiche, la manutenzione ed il loro sviluppo e la strategia di sviluppo del proprio sistema informatico; in questo caso dovrà comunque coordinarsi con l'appaltatore.

La struttura del contratto di facility management non è molto dissimile da quella del contratto di outsourcing, si differenzia essenzialmente per quanto riguarda le clausole che disciplinano la gestione dei mezzi hardware e software del committente e la gestione dei sistemi, dell'hardware e del software di base dell'appaltatore. Possono essere previste ulteriori clausole che regolano altre funzioni a carico del committente.

Per questa tipologia andranno opportunamente adeguate le clausole viste per il contratto di outsourcing tenendo conto della diversa allocazione dei compiti, dei rischi e delle responsabilità.

4.2.1.4 ASP - Application Service Providing

Nel caso degli ASP un fornitore permette l'uso, dietro pagamento di un canone di affitto, di programmi applicativi che risiedono "in remoto" presso i propri server. Chi fornisce tali servizi è, di solito, un operatore specializzato che eroga servizi di gestio-

ne e aggiornamento di applicazioni software ai quali si accede mediante linee dedicate o commutate.

In questo caso assumono particolare importanza:

- la definizione dell'oggetto del contratto;
- l'elenco dei servizi;
- gli SLA.

Ulteriori clausole su cui porre l'attenzione sono quelle relative alla sicurezza, tutela e protezione dei dati e degli archivi.

Il contratto può assumere una struttura simile a quello di outsourcing, salvo che in questo caso la prestazione dei servizi non è legata alla disponibilità di un ambiente hardware e software, conseguentemente nel contratto non è necessario inserire clausole relative alla migrazione dei sistemi e non sarà necessario verificare la cedibilità di beni e contratti preesistenti.

4.2.1.5 Disaster Recovery

Questa tipologia di contratto è simile a quella dell'outsourcing, in quanto riguarda la messa a disposizione del committente di una soluzione informatica completa, legata, però, al verificarsi di un evento catastrofico presso il committente.

In questa tipologia occorre porre molta attenzione alla definizione di evento catastrofico, che diventa il fattore abilitante alla fruizione del servizio da parte del committente, e l'impegno da parte del fornitore a mettere a disposizione le proprie risorse fino a saturare la propria capacità sulla base del principio "primo arrivato primo servito". Queste clausole sono molto importanti in quanto errori di valutazione o sviste potrebbero avere conseguenze fondamentali sulla possibile fruizione del servizio.

In alcuni casi il contratto di disaster recovery è un contratto autonomo, molto più spesso è integrativo di un contratto di outsourcing.

Ulteriori punti di attenzione in questi contratti sono:

- Il limite della durata dei servizi di disaster recovery una volta

attivati, superato questo limite il committente non può più utilizzarli;

- La tutela e protezione degli archivi, la conservazione ed il trasferimento degli archivi di dati.

Dopo l'11 settembre 2001 molti committenti hanno richiesto un allargamento dei servizi richiesti inserendo anche le strutture necessarie per permettere la continuazione delle attività del committente (uffici, PC, fax, ecc.).

4.2.1.6 Web Hosting e Web Housing

Il Web Hosting indica il servizio erogato dagli Internet Service Provider (ISP) atto a "ospitare" e rendere visibile un sito sulla rete Internet.

Anche in questo caso il contratto non presenta sostanziali differenze con il contratto di outsourcing visto in precedenza. Come nel caso dei contratti ASP occorre precisare bene l'oggetto del contratto, dei servizi, delle prestazioni e degli SLA.

Occorre considerare, inoltre, che all'appaltatore possono essere richieste prestazioni aggiuntive come:

- l'attribuzione e la registrazione del domain name;
- sviluppo del layout del sito;
- sviluppo dei contenuti del sito.

Queste attività possono essere svolte direttamente dall'ISP oppure possono essere svolte da subfornitori, è allora necessario definire con attenzione le clausole relative alla proprietà intellettuale ed alla titolarità del domain name.

Ulteriori clausole su cui porre l'attenzione sono quelle relative alla sicurezza, tutela e protezione dei dati e degli archivi.

Per quanto riguarda gli ambienti hardware e software vale quanto detto nel caso dei contratti ASP a cui si rimanda.

5 - Requisiti generali di uno SLA

In letteratura il termine SLA (Service Level Agreement) connota "il contratto/accordo complessivo sull'ambito, la funzione e le prestazioni attese di livello di un servizio, nonché su un'individuale, dettagliata misura per ciascun requisito del servizio. In questa linea guida seguiremo questa definizione. Misure individuali sono riferite come livelli di servizio, o accordi di servizio e non usano l'acronimo SLA.

Lo SLA contiene "… contrattualmente clausole binding che documentano le performance standard e la qualità del servizio concordata tra il cliente ed il provider. Il principale scopo dello SLA è quello di specificare e rendere chiare le prestazioni aspettate, stabilire una contabilizzazione ed i rimedi o le conseguenze se le prestazioni o la qualità del servizio non sono quelli concordati" [BITS 01, Appendix 4, p 62].

In effetti lo SLA è un accordo tra il cliente ed il fornitore di servizio che quantifica i livelli minimi accettabili del servizio in oggetto dal punto di vista del cliente [Hiles 02].

Lo SLA è probabilmente il documento più importante in una relazione MSS cliente/fornitore. Uno SLA, quando scritto propriamente, è distinguibile da chiarezza, semplicità del linguaggio e dall'essere focalizzato sulle necessità e le volontà delle attività commerciali del cliente [CIO 01].

In altre parole, uno SLA mutuamente concordabile richiede un lavoro di buona diligenza da entrambe le parti.

Un provider tipicamente sviluppa un suo SLA sulla base delle misure del livello di servizio mediate su un insieme di clienti. Tipicamente i provider vogliono far accettare il loro SLA ai clienti come accordo contrattuale. "Sempre più spesso, gli accordi a livello di servizio dei provider apparentemente assicurano il livello del servizio, ma in realtà sono stati progettati per limitare le responsabilità del provider. I provider che costruiscono gli SLA per proteggere i loro introiti tipicamente usano una combinazione di indicatori di servizio non specifici o non misurabili, esclusione che nega ciò che dovrebbe essere un impegno rigoroso alla fornitura del servizio e alle rispettive penali" [Nicolett 02].

"Uno SLA è un contratto vincolante che specifica la fornitura delle prestazioni e della qualità di un servizio tra due entità legali (il provider ed il cliente). Non bisogna firmare con semplicità una bozza emanata dal provider. Al contrario bisogna assumere un legale che sia familiare con la legislazione commerciale e quella in materia di new-economy (includendo gli aspetti di proprietà intellettuale) e tale legale deve sviluppare insieme al fornitore del servizio ed al suo consulente legale lo SLA" [NM 01].

I clienti dovrebbero andare all'interno del processo di negoziazione con un proprio SLA come punto di partenza e prendendo in considerazione allo stesso tempo quello del provider. Lo SLA del cliente dovrebbe essere allineato con i propri beni critici, le rispettive strategie, politiche e procedure di protezione e dovrebbe essere definito in modo da soddisfare i requisiti di confidenzialità, integrità e disponibilità.

I clienti devono determinare gli aspetti maggiormente critici di un servizio ed assicurare che gli SLA siano definiti e negoziati in modo da trattare tali criticità. Queste generalmente includono sicurezza del servizio, livelli del servizio, tempi di risposta, uptime/downtime di infrastrutture, prestazioni della rete, scalabilità, reportistica, soddisfazione del cliente, prestazioni globali delle caratteristiche del servizio e processo di escalation.

Lo SLA definisce i ruoli di cliente e fornitore. Come risultato, il cliente comprende esattamente cosa il provider è tenuto a fare e cosa il provider ha accordato di fare per parte del cliente. Lo SLA deve essere il più preciso possibile. Deve definire a quali risorse il provider accederà e quali funzioni il provider può eseguire su tali risorse [Navarro 01]. É critico coinvolgere nel processo di sviluppo dello SLA tutti gli stakeholders del cliente che sono necessari per assicurare conformità allo SLA. Questi tipicamente includono membri dello staff di sicurezza e del team IT.

"Laddove siano coinvolti più fornitori nella consegna del servizio, sono necessari dei sub-SLA in modo tale che il fornitore principale possa fornire uno SLA complessivo direttamente al cliente. Questi sub-SLA possono anche essere conosciuti come SLA stratificati o SLA multi-livello" [Hiles 2].

Laddove possibile contrattualmente, le linee guide descritte di seguito dovrebbero applicarsi a tutti i provider coinvolti nella fornitura del servizio (anche multi-livello). Quando ciò non sia possibile, il provider deve descrivere al suo cliente come il sotto-fornitore verrà tenuto in conto per tutti i requisiti contrattuali di livello del servizio in cui partecipa. I clienti da parte loro dovrebbero considerare l'inserzione di un contratto o di clausole nello SLA che affermino che il fornitore principale resta l'unico responsabile per ogni eventuale danno o prestazione sotto specifica causata da suoi sotto-fornitori.

Il contratto complessivo tra cliente e fornitore include lo SLA. Oltre a coprire i contenuti dello SLA, questa pratica fornisce una giuda sui contenuti contrattuali relativi alla sicurezza che sono tipicamente fuori dagli scopi dello SLA. Come minimo uno SLA definisce misure delle prestazioni attese di uno specifico servizio (vedi Service Attributes).

Alcune linee guida sugli attributi di business, riportate nella sezione 5.2, sono appropriate per uno SLA mentre altre possono essere più appropriate per altre sezioni del contratto cliente/fornitore. Similmente le pratiche di sicurezza, riportate nella sezione 5.4 descrivono la qualità di pratiche di sicurezza operative che il provider deve rispettare nel caso in cui esso è custode dei beni infor-

mativi del cliente, a prescindere dal servizio specifico. Ancora una volta, alcune di queste linee guida possono essere più appropriate per altre sezioni del contratto cliente/fornitore.

A prescindere da ciò comunque, tutti i requisiti sono descritti come parte di un accordo sul livello di servizio. Rimane da definire sia per il cliente che per il fornitore come meglio presentare questa informazione in forma contrattuale.

Come parte di creazione dello SLA, il cliente si assicura ed afferma che altri SLA con lo stesso provider non vanno in conflitto con lo SLA sotto negoziazione [Alner 01].

5.1 Linee guida generali per uno SLA

Uno SLA dovrebbe contenere le sezioni riportate nei prossimi paragrafi.

5.1.1 Sommario esecutivo

Questa sezione contiene una panoramica ed una descrizione sullo scopo del documento, che generalmente effettua una descrizione del servizio e sugli accordi raggiunti. Il sommario include inoltre la durata dell'accordo ed identifica gli stakeholder ed i proprietari chiave del cliente per la gestione di ogni servizio ed assicura che gli accordi sui servizi siano rispettati.

5.1.2 Descrizione del Servizio

Questa sezione contiene una descrizione dettagliata dei servizi e dei rispettivi accordi per ciascuno di essi. C'è una sottosezione per ciascuna categoria di servizio (per esempio gestione dei firewall, gestione del sistema di rilevamento delle intrusioni, accesso remoto ed analisi della vulnerabilità). Ci sono poi sottosezioni addizionali per gli attributi commerciali o le pratiche di sicurezza che sono indipendenti dallo specifico servizio e si applicano a più servizi.

5.1.3 Definizione del livello di servizio

Per ciascun servizio vanno inclusi dei descrittori chiave del servizio come segue:

1) Definizione: una precisa, non ambigua descrizione del servizio che sta per essere erogato, misurato e documentato.

2) Intervalli temporali di misura: istanti di tempo (giorni, date e tempi) di quando verranno effettuate le misure del servizio. Indica se l'ambito di misura include tutti i 365 giorni dell'anno o se i giorni selezionati sono esclusi. Descrive l'intervallo di tempo (tipicamente giorni o settimane) su cui le misure vanno fatte in modo che il cliente possa determinare se l'accordo sulla fornitura del servizio è rispettato, non rispettato o in eccesso.

3) Responsabilità: specifica i ruoli e le responsabilità del cliente e del fornitore che devono essere portate a termine per essere a norma con gli accordi sul servizio. Identifica chi è responsabile per eseguire le misure e come ciascuna misura viene validata. Identifica i punti di contatto primari e secondari per entrambe le organizzazioni così come per tutti gli eventuali sottofornitori.

4) Metriche del livello di servizio:

a) Le misure e gli intervalli di misura per il servizio sotto contratto come tempo di risposta e disponibilità del servizio. Tipicamente, i livelli di servizio sono descritti con la rispettiva percentuale. Comunque i fornitori necessitano di proporre misure specificate in termini di prestazioni commerciali del cliente, con l'assistenza di quest'ultimo.

b) Attenzione alle metriche di livello di un servizio che sono calcolate basandosi sulle prestazioni aggregate di risorse multiple (come ad esempio server multipli). Prestazioni medie tra risorse multiple raramente cadono sotto i livelli prestabiliti anche se tali risorse critiche non stanno funzionando in maniera accettabile.

c) Laddove un intervallo di livello del servizio è accertabile, si consideri di specificare una soglia desiderata di livello del servizio così come un livello minimo accettabile (caso

peggiore), con rispettive riconoscimenti e penalità associate a ciascuno di essi.

d) Per i livelli di servizio che sono difficili da determinare in anticipo senza il supporto di qualche esperienza operativa, si consideri un intervallo di tempo specifico di realizzazione pilota e revisione prima che questi vengano documentati nello SLA.

5) Formule di misura: qui si descrivono le equazioni di misura matematica che saranno utilizzate insieme ad un esempio. Vanno identificate ogni prestazione di monitoraggio o strumento di misura usato dal provider ed il documento di conferma del cliente che questi strumenti sono accettabili.

6) Servizi condivisi: quando clienti multipli condividono le stesse risorse di servizio di un provider, un consumo eccessivo da parte di un cliente può avere effetto sulle prestazioni di un altro cliente. Questo può essere indirizzato con la garanzia del provider sull'adeguata capacità, sulla realizzazione di un blocco quando la domanda eccede limiti prestabiliti o dall'opzione di acquisire un accesso esclusivo al servizio.

7) Sorgenti dei dati: questa sezione descrive dove i dati di misura vengono raccolti, cosa è raccolto, come è memorizzato e chi è responsabile per la raccolta.

8) Attività di escalation: quando si verificano situazioni di fuori-specifica, in questa sezione si descrive che cosa notificare e sotto quali condizioni. Questo include situazioni fuori specifica sia giornaliere che relative ai periodi di misura, così come fuori servizio del sistema, di una sede e altre situazioni di rilievo per la continuità dell'attività commerciale ed il recupero da disastri.

9) Eccezioni contrattuali, Riconoscimenti e Penalità: questa sezione descrive tutte le eccezioni, i riconoscimenti e le penalità negoziate che sono incluse nello SLA e vanno applicate al servizio in esame. Indica le responsabilità per cliente e fornitore di reporting per l'aver notato un'eccezione, un riconoscimento o una penalità. Alcuni provider richiedono al cliente la notifica scritta, entro un certo periodo, per ricevere il pagamento od il riconoscimento

della penale.

10) Formula di calcolo del riconoscimento/penale: descrive la formula matematica usata ed un esempio. Se il cliente od il fornitore usa codici di priorità o severità questi vanno inclusi in questa sezione.

5.1.4 Gestione del livello di servizio

Documenta i seguenti processi necessari per la gestione dei livelli di servizio. Include inoltre l'evento o l'intervallo di tempo che scatena l'esecuzione del processo.

1) Tracciamento delle misure e rendicontazione delle stesse.
2) Problem escalation e risoluzione delle dispute.
3) Richiesta di cambiamento del servizio che includano la rinegoziazione dei termini di misura del servizio. Bisogna essere sicuri di specificare che i livelli di servizio siano periodicamente rivisti ed aggiornati per riflettere gli standard industriali [CIO 01].
4) Implementazione di nuovi servizi e nuovi livelli di servizio.
5) Processo di revisione del livello di servizio.
6) Processo di approvazione.

5.1.5 Ruoli e Responsabilità

Questa sezione descrive i ruoli e le responsabilità generali di tutte le parti che non sono coperte dalla definizione dei livelli di servizio sopraccitata. Questo include i clienti, i fornitori, ogni sottofornitori ed ogni comitato governativo o stakeholder chiave che gestisce questo contratto.

In particolare i clienti, essendo i principali attori, come parte delle loro responsabilità dovrebbero fornire:

- Una completa e dettagliata informazione relativa alla loro infrastruttura e agli ambienti nei quali i servizi del provider vanno

ad inserirsi;

- Un'informazione completa e tempestiva su eventuali cambiamenti o problemi (come ad esempio aggiornamenti alla configurazione di rete, problemi con la connessione Internet, eventuali vulnerabilità individuate, attività di rete anomala, ecc.)

Per fare ciò si suggerisce un approccio che consideri anche i seguenti aspetti:

- Piani di disaster recovery,
- data center per il backup,
- sicurezza fisica,
- protezione delle persone e dei beni,
- gestione delle policy

Come descritto nel paragrafo 4.1.2, per gestire e tenere sotto controllo gli aspetti sopra citati, è auspicabile, istituire uno staff capace di combinare le differenti visioni di un'organizzazione in modo da contribuire, in accordo al ruolo e alla responsabilità ricoperta, alla mitigazione di eventuali minacce.

Macroscopicamente esistono i seguenti approcci:

- Corporate View (CEO);
- Business Process Owner;
- Responsabile IT (CIO).

I principali requisiti del CEO sono:

- Assicurare che la Sicurezza delle informazioni dell'Organizzazione venga gestita nella sua interezza;
- La completa responsabilità della gestione dei rischi dell'Organizzazione;
- Garantire la rispondenza con le leggi.

I principali requisiti del (Business) Process Owner sono:

- Definire proattivamente gli elementi dell'infrastruttura IT necessari per soddisfare i requisiti di business
- Consolidare e standardizzare un insieme di policy, architetture e servizi di sicurezza IT validi per tutta l'Organizzazione

I principali requisiti del CIO sono:

- Trasparenza su specifici rischi relativi ai processi di business;
- Definizione di adeguate contromisure;
- Definizione di modelli di gestione del rischio residuo.

In questo contesto si suggerisce di istituire all'interno dell'organizzazione la figura del CSO (Chief Security Officier) con il ruolo di responsabile della sicurezza, il quale si focalizza sui processi aziendali di rilievo (e quello di outsourcing è certamente da considerare tale) e misura il livello sicurezza raggiunto.

La definizione di un tale processo permette di istituire a supporto del CSO una squadra di risorse garanti che interfaccino e misurino i rispettivi interlocutori.

Applicando questo modello ad un contratto di servizi a terzi si può:

1) definire il target da raggiungere

2) identificare, nella gestione di contratto, gli eventuali scostamenti.

Tutti i ruoli afferenti al contesto organizzativo in esame devono cooperare per assicurare il buon esito della gestione di un contratto di servizi analizzando e comparandone l'evoluzione nel tempo.

Stage	Bu`s View of Security Value	Security Budget	Operations Management	BU Risk Management
1 Hunter Gatherer	No perception No awareness	No identified dedicated budget	Deployment	Not Applicable
2 Feudal	Security is a technical requirement	100%of the security budgets comes from the IT budget 100% of the budget for infrastructure security	Monitoring and Problem Resolution	Infrastructure Security CIRT
3 Renaissance	IT risks can damage business activity. Business transaction security needed	25% of the security budget comes from the business for transaction security; 75% for infrastructure security	Configuration and Change Management	Security Architecture Proactive Risk Analysis
4 Industrial	Security is a quality of the IT environment that can provide competitive advantage	70% of the security budget comes from the business for transaction security; 30% dedicated to infrastructure security	Transaction Incident Management	Transaction Risk Management

Tabella 6: La gestione della sicurezza nelle diverse epoche

5.2 Attributi Commerciali

Gli attributi commerciali sono uno degli elementi tra i requisiti del cliente. Questi comprendono le caratteristiche, le politiche, i processi e le procedure che bisogna definire precisamente e concordare mutuamente negli SLA e nel contratto cliente/fornitore. Questi includono:

- Realizzabilità (VI)
- Soddisfazione del Cliente (CS)
- Relazioni con altre parti (RO)
- Valutazioni Indipendenti (IE)
- Personale (PR)
- Proprietà dei beni (AO)
- Eccezioni contrattuali; Penalità e Riconoscimenti (CE)
- Accordi sui livelli di servizio (SA)
- Strategia di uscita (ES)
- Piano di realizzazione (IP)

- Punti di Contatto (PC)
- Piano di realizzazione (IP)
- Punti di Contatto (PC)

Lo SLA deve trattare in modo soddisfacente tutti gli attributi commerciali presentati nel l'RFP del cliente come modificati dalla proposta del fornitore. Alcune linee guida su come descrivere gli attributi commerciali sono riportate di seguito.

5.2.1 Realizzabilità (VI)

[VI1] Si consideri l'inserzione di modalità di notifica per il cliente nel caso del verificarsi di eventi tipo [BITS 01, Section 5.2, p 26; Section 5.13.3, p 34]:

a) Cessazione imminente dell'attività del provider o di quel la di un suo sottofornitore e ogni piano contingente nel l'evento di notifica di un tale disservizio.

b) Difficoltà finanziarie che possono impattare la fornitura del servizio.

c) Cambiamenti sostanziali nelle decisioni tattiche o strategi che riguardanti l'acquisto od il supporto di hardware o software legato all'elaborazione del servizio.

d) Riduzioni significative del personale o cambiamenti in ruoli chiave dello staff che possono inficiare la capacità del provider a fornire il supporto al servizio.

e) La decisione di dare in outsourcing, vendere o acquisire aree operative significative od il supporto associato nelle applicazioni, dati, reti o altre componenti critiche del- l'ambiente usato per fornire i servizi al cliente.

f) Press Release pendenti su ogni soggetto che può impat- tare il cliente.

[VI2] Si consideri di incorporare clausole per la protezio- ne dei beni del cliente nel caso in cui si verifichino uno o più dei

seguenti eventi:

a) Riconoscere il diritto al cliente di accedere e manipolare i loro sistemi, dischi, nastri di backup ed il desiderio di evitare che dati sensibili risiedano su risorse che devono essere vendute.

b) Apporre etichette sull'apparecchiatura del cliente in modo da stabilire la sua proprietà e mantenere un inven tario aggiornato dell'hardware in modo da prevenire che apparecchiature del cliente siano vendute o sezionate. Questo risolve inoltre la questione della proprietà nel l'evento in cui vengano acquistate la attività commerciali del provider.

5.2.2 Soddisfazione del Cliente (CS)

[CS1] Descrivere il livello di supporto del servizio che verrà fornito al cliente includendo ore di servizio, uso di metodologie automatiche, tempi di risoluzione di eventuali problemi e tempi garantiti di richiamata [BITS 01, Section 5.1.1, p 25].

[CS2] Si consideri di concordare col provider (ed eventuali suoi sottofornitori) l'analisi periodica di un questionario di valutazione della soddisfazione del cliente e di una procedura di report dei risultati al cliente. Il questionario è volto a misurare qualitativamente la percezione del cliente della qualità del servizio fornito. I risultati dell'analisi possono essere fattorizzati secondo formule di riconoscimenti/penalità per il provider. Fattori da includere sono [Hiles 02]:

a) Disponibilità del servizio e tempi di risposta;
b) Facilità d'uso;
c) Qualità del supporto ai servizi del cliente;
d) Addestramento;
e) Disservizio accettabile includendo costi ed impatti;

[CS3] In assenza di un accordo col provider, il cliente può eventualmente considerare di condurre tali questionari interna-

mente riportando i risultati al provider.

5.2.3 Relazioni con altre parti (RO)

[RO1] Il cliente ed il provider decidono a quali documenti è necessario che ogni sottofornitore abbia accesso e ne forniscono l'uso dei dati contenuti dopo che sia stato firmato un permesso scritto.

[RO2] Documentazione fornita dal provider contenente le responsabilità e gli orari di lavoro per ogni sottofornitore coinvolto nella fornitura del servizio in esame.

[RO3] Il provider asserisce la propria responsabilità contrattuale per le prestazioni dei sub-provider includendo la soddisfazione per tutti i servizi concordati in cui il sottofornitore partecipa.

[RO4] Il provider mostra mezzi ed accordi di servizio che usa per comunicare con i sottofornitori e per assicurare che tali sottofornitori rispettino i suddetti accordi.

5.2.4 Valutazione indipendente (IE)

[IE1] Il provider regolarmente fornisce al cliente i risultati di valutazioni sul sistema complessivo, sui rischi di sicurezza, sulla valutazione delle vulnerabilità, e sui test d'intrusione eseguiti da una terza parte mutuamente concordata [Alner 01]. Lo SLA specifica chi esegue ciascuna valutazione e quanto spesso questa debba essere fatta. Il contratto tra il cliente ed il provider definisce quali eventi o circostanze allertano queste valutazioni così come chi si prende carico dei rispettivi costi. Il cliente può considerare di richiedere che lo staff di valutazione interno possa eseguire almeno un accesso annuale ad eseguire valutazioni sulle operazioni, sulle tecnologie IT e sulle finanze del provider.

[IE2] Il cliente ed il provider mutuamente fissano dei piani di priorità e risoluzione [BITS 01, Section 4.1, p 20]. Il clien-

te può voler specificare intervalli di tempo per una certa classe di problemi come ad esempio vulnerabilità ad alta priorità identificate da un'analisi delle vulnerabilità.

5.2.5 Personale (PR)

[PR1] Il cliente deve esplicitamente identificare il trasferimento delle competenze come un obbiettivo chiave della relazione col provider in modo da assicurare che possa dirigere il servizio nell'evento che la gestione del servizio debba essere portata in casa[Cramm 01].

[PR2] Il cliente ed il provider firmano mutui accordi di confidenzialità e non divulgazione ove richiesto.

[PR3] Il provider deve assicurarsi che i membri dello staff del cliente non creino inavvertitamente rischi esposti per la sicurezza come risultato di non conoscenza. Questo può essere ottenuto conducendo programmi di addestramento e presa di coscienza e monitorando le azioni degli utenti.

5.2.6 Proprietà dei beni (AO)

[AO1] Lo SLA od il contratto:

a) Descrive come i beni vengano trasferiti alla fine del con tratto laddove la proprietà è del provider ma è richiesto che il cliente la usi durante la fornitura del servizio. Questo include beni come le licenze software ottenute dal provider per conto del cliente.

b) Deve trasferire i necessari diritti di proprietà intellettuale e copyrights dal provider al cliente in modo tale che il cliente possa aggiornare i dati in futuro ed usarli alla fine della relazione.

5.2.7 Eccezioni contrattuali (CE)

[CE1] Lo SLA specifica i ricorsi ad eventuali azioni che devono essere intraprese nel caso gli accordi non vengano rispettati (da entrambe le parti). Considera inoltre bonus per forniture del servizio sopra gli standard pattuiti o riconoscimenti non monetari come documentazione dell'esperienza in pubblicazioni. Negozia inoltre le penalità per servizi sotto lo standard concordato, includendo eventualmente la risoluzione del contratto. Documenta le implicazioni legali nel caso in cui una delle parti non soddisfi i propri obblighi [Alner 01].

[CE2] Un provider rispettabile dovrebbe essere disposto ad accettare una penale del 100% dei propri compensi nel caso vengano riportati, entro un certo tempo, fallimenti nella fornitura del servizio. Se il provider non è pronto ad accettare questo, deve essere trattato con molto cautela [Hiles 02]. Ci si guardi dalle protezioni di penalità proposte dal provider come quelle di spese per dodici o diciotto mesi di servizio e per ogni clausola che affermi che ogni specifica penalità nelle prestazioni è il solo ed esclusivo rimedio per il cliente [CIO 01].

[CE3] Lo SLA deve specificare che i livelli di servizio possono essere rinegoziati durante la contrattazione delle prestazioni. Questa descrizione deve specificare ogni predeterminata condizione sotto la quale tale rinegoziazione può avvenire.

5.2.8 Accordi sul livello di servizio (SA)

Vedi paragrafo 5.1.

5.2.9 Strategia d'uscita (ES)

[ES1] Essere sicuri che il contratto includa una descrizione di quello che costituisce il normale completamento del contratto così come una terminazione anticipata. L'interruzione del contratto può avvenire sotto le seguenti circostanze:

a) terminazione per cause che includono falle nel contratto come l'incapacità ad operare o serie carenze nella sicurezza (confidenzialità, integrità, disponibilità).

b) Convenienza;

c) Insolvenza o bancarotta del provider;

d) Cambiamento della proprietà commerciale del provider o del suo controllo come ad esempio quelli che avvengono durante le acquisizioni o fusioni.

[ES2] Essere sicuri che la descrizione indirizzi:

a) Le responsabilità del provider includendo quelle necessa rie ad assicurare una transizione col minimo disservizio dal lato cliente;

b) Responsabilità del cliente;

c) Trasferimento dei beni chiave (dati, software, hardware, strumenti). Laddove il provider ha la proprietà di codice sorgente applicativo per il servizio, il contratto deve includere i seguenti dettagli:

   i) Un luogo di impegno (escrow) di terza parte, concordato da entrambe le parti, dove la versione base del software verrà tenuta.

   ii) Requisiti contrattuali per mantenere aggiornato e completo il codice sorgente e la relativa documentazione.

   iii) Determinazione di chi paga i costi di impegno, così come le condizioni specifiche sotto le quali l'impegno è disponibile per il cliente.

   iv) Punti di contatto scelti da cliente e fornitore, come chi fornisce accesso al materiale per la verifica, nel l'evento che qualsiasi clausola sia invocata, come quando il cliente prende il codice sorgente, a chi tale codice è rilasciato e quando è rilasciato.

   v) Il tipo di mezzo sul quale il codice sorgente è memorizzato.

vi) La specifica di tutti gli elementi di carattere operativo sotto cui il codice sorgente è leggibile/eseguibile, etc.

vii) La distruzione e/o la restituzione di dati di proprie tà del cliente o di altre informazioni sensibili.

d) La distruzione o la restituzione di proprietà del cliente o di informazioni sensibili

e) Penalità imposte dal provider e pagamento di danni al cliente si devono se un qualsiasi membro (attuale o passato) dello staff del provider viola i termini dell'accordo di non divulgazione o ogni altro accordo che si estenda sul periodo di fornitura del servizio.

f) Tempo di transizione.

5.2.10 Piano di realizzazione (IP)

Vedi paragrafo 5.2.11.

5.2.11 Punti di contatto (PC)

[PC1] Identificare i punti di contatto tra cliente e fornitore che servano da interfaccia principale tra le due organizzazioni per la messa in opera del servizio e la gestione giornaliera.

5.3 Attributi del servizio

Gli attributi del servizio sono un secondo elemento nei requisiti del cliente. Descrivono la qualità del servizio che deve essere fornito ed i livelli di prestazione del servizio da rispettare. Questi includono:

- Requisiti di sicurezza top-level (SR)
- Disponibilità del servizio (SY)
- Architettura del servizio (SA)

- Hardware e Software del servizio (HS)
- Scalabiltà del servizio (SS)
- Livelli del servizio (SL)
- Requisiti di reporting (RR)
- Ambito del servizio (SP)
- Costo (CO)

In uno SLA il provider descrive come dimostrerà aderenza a tutti gli attributi del servizio durante l'esecuzione del contratto, come presentato nell'RFP del cliente e come modificato dalla proposta del provider stesso. Gli attributi del servizio includono i livelli del servizio e le prestazioni standard, le responsabilità del cliente nel supportarle, i requisiti di reporting, le responsabilità per eventuali problemi, la problem escalation, le forniture di continui miglioramenti e le conseguenze ed i rimedi di non-performance [BITS 01, Section 5.1.2, p 26]. Linee guida per attributi specifici sono presentate di seguito.

5.3.1 Requisiti di sicurezza top-level (SR)

[SR1] Il provider assicura ed è capace di dimostrare che la confidenzialità, la disponibilità e l'integrità dei beni del cliente (HW, SW e dati) vengano mantenuti nella fornitura del servizio.

[SR2] La privacy del cliente è protetta ed include, non essendo limitata comunque ai soli dati del cliente, lo stato delle vulnerabilità e lo stato degli attacchi.

[SR3] Il provider assicura che dati specifici del cliente risiedano solo su territorio specificato dal cliente in modo da soddisfare le leggi locali/regionali sulla privacy dei dati.

5.3.2 Disponibilità del servizio (SY)

[SY1] Descrive il processo e l'intervallo temporale per la realizzazione e la messa in opera del servizio.

[SY2] Descrive gli intervalli di tempo di disponibilità del

servizio ed ogni limitazione fino a ventiquattro ore al giorno, sette giorni la settimana e 365 giorni all'anno, a seconda del servizio.

[SY3] Descrive i periodi di uptime secondo le linee guida RFP.

[SY4] Specifica il tempo di risposta quando si verifica un guasto ed il servizio diventa non disponibile. La definizione di Tempi di Risposta Garantiti (Guaranteed Response Time, GRT) è un requisito chiave dello SLA. La specifica del tempo di risposta del provider consente di indirizzare i requisiti del cliente sui sistemi di servizio che il provider sta gestendo come tempo di risposta:

a) Per scoprire tentativi di intrusione o intrusioni.

b) Per mettere in atto una richiesta di cambiamento nella configurazione.

c) Per sviluppare una patch contro una nuova vulnerabilità.

d) Eseguire la manutenzione di hardware o software.

[SY5] Il provider colleziona sufficienti informazioni per riportare tempo di disservizio (downtime), le ragioni per ogni eventuale guasto e relativo impatto sui livelli del servizio.

[SY6] Descrizione anticipata dell'efficienza che si acquisisce da miglioramenti tecnologici [BITS 01, Section 5.1.2, p 26].

5.3.3 Architettura del servizio (SA)

Descrive l'architettura del servizio anche in termini di alternative su luoghi e tempi in cui il servizio dovrà essere sviluppato [Navarro 01].

5.3.4 Hardware e Software del servizio (HS)

Descrive i servizi di supporto hardware e software da fornire [BITS 01, Section 5.1.1, p 25].

5.3.5 Scalabiltà del servizio (SS)

[SS1] Il provider colleziona e riporta statistiche relative alla capacità come l'utilizzazione di banda e la percentuale di sistema usata del servizio. Il cliente specifica anticipatamente i tassi di crescita della capacità, le necessità di memorizzazione ed eventuali picchi legati a promozioni o eventi stagionali [BITS 01, Section 5.1.2, p 26]. Il provider progetta l'impatto dalla crescita della capacità sulla disponibilità del servizio e sugli standard prestazionali.

5.3.6 Livelli del servizio (SL)

[SL1] Definisce e descrive specificatamente i requisiti prestazionali del servizio come ad esempio il tempo di risposta, i tempi di processamento del servizio, la frequenza del monitoraggio, il tempo di risoluzione di un problema e le attività di supporto all'analisi [BITS 01, Section 5.1.2, p 26].

[SL2] Considera l'uso di una tessera a punti che riassume e dà la priorità ai livelli di servizio pesandoli sulla base della loro importanza relativa. Nel caso in cui un provider soddisfa o eccede i livelli di servizio concordati, gli vengono accreditati "punti" positivi. Prestazioni sotto la soglia di servizio concordata corrispondono invece a punti che vengono sottratti. Se il punteggio totale è sotto una soglia prestabilita il cliente può richiedere che gli vengano riconosciute le penalità pattuite [Hiles 02].

[SL3] Specifica come vengono gestite le emergenze. Identifica quali autorizzazioni sono richieste per risolvere i problemi, quali problemi verranno gestiti dal cliente e quali dal provider.

[SL4] Specifica come vengono gestite speciali richieste del cliente, includendo costi addizionali e tempi di risposta [Alner 01].

5.3.7 Requisiti di reporting (RR)

[RR1] Per ciascun tipo di report si specifica la frequenza, il formato ed il relativo contenuto. Si allegano alcuni report di

esempio:

a) Report sulle misure dei livelli di servizio, come ad esempio prestazione del servizio fornito rispetto a dei livelli minimi di servizio;

b) Report di violazioni: tentativi d'intrusione o intrusioni con violazione d'accesso;

c) Report di incidenti: tentativi di intrusione o intrusioni.

[RR2] Negozia il contenuto del report che è basato sull'esperienza dell'utente finale su un servizio, piuttosto che su un sistema di metriche di risposta aggregato. Questo tipo di report fornisce una rappresentazione più significativa del servizio di cui l'utente finale sta fruendo.

[RR3] Specifica l'intervallo massimo di tempo per notificare nuovi problemi e azioni nel sistema di tracciamento dei problemi dopo la loro scoperta.

5.3.8 Ambito del servizio (SP)

[SP1] Descrive i diritti del cliente nel fare cambiamenti ai servizi ed i processi richiesti e gli obblighi per aggiungere nuovi servizi, modificare quelli correnti o combinare insieme più servizi [BITS 01, Section 5.1.1, p 25-26].

[SP2] Descrive "le considerazioni e la fornitura di tecnologie emergenti per rimpiazzare, ridurre o aggiungere servizi sulla base dei cambiamenti tecnologici" [BITS 01, Section 5.1.1 p 26].

5.3.9 Costo (CO)

Non applicabile, vengono indirizzati fuori dallo SLA.

5.4 Pratiche di sicurezza

Le pratiche di sicurezza sono il terzo elemento dei requisiti del cliente. Le prestazioni del servizio fornito dal provider devo-

no essere a specifica con le politiche e le procedure di sicurezza del cliente. Il provider deve dimostrare che le loro pratiche di sicurezza sono effettivamente implementate ed in uso come specificato nell'RFP e nelle modifiche alla proposta del provider. Questo include la dimostrazione che:

La rete del provider e le sue infrastrutture sono rese sicure così come quelle di ogni eventuale sottofornitore al quale esso si affida.

La rete del cliente e le sue infrastrutture rimarrà sicura quando il servizio fornito dal provider verrà messo in opera.

Lo SLA dovrebbe indirizzare i dettagli delle pratiche di sicurezza specificate nell'RFP, includendo:

- Politiche, Procedure e Regolamentazioni di sicurezza (PP)
- Piano di contingenza; Recupero da disastro ed Operazionale (DR)
- Sicurezza Fisica (PS)
- Gestione dei dati (DH)
- Autenticazione ed Autorizzazione (AA)
- Controllo di Accesso (AC)
- Integrità del Software (SI)
- Configurazione di sicurezza dei beni (SC)
- Backup (BU)
- Monitoraggio e valutazione (MA)
- Gestione degli incidenti (IM)

Considerazioni specifiche per lo SLA per le stesse pratiche sono descritte di seguito.

5.4.1 Politiche e regolamentazioni di sicurezza (PP)

[PP1] Il cliente deve determinare quali sono i requisiti dei servizi completamente o parzialmente implementati del provider.

Tali requisiti includono regolamentazione, legislazione, standard, politiche ed altri requisiti. Il cliente alloca esplicitamente questi requisiti dove il provider è coinvolto. Il provider deve accettare questa ripartizione. Entrambi, cliente e fornitore, devono assicurarsi che questa condivisione di responsabilità può soddisfare una valutazione di terze parti di tali requisiti, dimostrando la completa conformità del provider.

[PP2] Controlla i conflitti tra le politiche e le procedure di sicurezza di cliente e fornitore. Se esistono conflitti, bisogna che questi vengano risolti nello SLA.

[PP3] Sia cliente che provider possono dimostrare la loro conformità ad uno standard appropriato per la messa in sicurezza dei beni informativi. Questo è principalmente ottenuto attraverso politiche e procedure di sicurezza che sono documentate e fatte rispettare insieme alle pratiche di sicurezza che sono state sviluppate [Alner 01].

[PP4] Il provider descrive i meccanismi usati per verificare la conformità dell'utente alle politiche di password del provider così come ad ogni altra procedura di autenticazione dell'utente.

[PP5] Il provider dimostra che la sua implementazione di separazione delle funzioni è consistente con i requisiti del cliente, includendo: (1) amministrazione della sicurezza, rassegna degli accessi utente, reporting degli incidenti e (2) tra gli sviluppi, le operazioni, e lo staff del provider. Indirizza inoltre altri potenziali ruoli di conflitto se necessario [BITS 01, Section 5.6.5, p 30].

5.4.2 Piano di contingenza (DR)

[DR1] Il provider descrive le situazioni che richiedono recupero operazionale, gli obbiettivi sui tempi di recupero (quando tempo è necessario per recuperare il servizio), gli obbiettivi sui punti di recupero (quanto distanti, a quale punto nell'elaborazione del servizio, considerando quali informazioni possono essere state perse).

[DR2] Nel caso in cui si verifica un disastro o un'emergen-

za simile, il provider specifica il minimo ed il massimo:

a) Tempo di recupero associato con le risorse di calcolo del provider e del cliente.

b) Tempo di validazione dei dati del cliente.

c) Tempo per il quale il cliente sarà sprovvisto dei servizi del provider.

[DR3] Determina le politiche di problem escalation del provider, i suoi processi ed i tempi di reporting. Gli intervalli di tempo per l'escalation reporting devono corrispondere ai requisiti del cliente. Per questioni di sicurezza critica è appropriato un tempo di reporting corto (15 minuti è lo standard). Per questioni meno critiche, un tempo di un'ora, un giorno o all'interno del report mensile può essere accettabile. Il cliente deve designare le categorie costituenti come serie, meno critiche e così via.

5.4.3 Sicurezza Fisica (PS)

[PS1] Il provider controlla l'accesso fisico a beni informativi, servizi IT e risorse sulla base della loro importanza; inoltre monitora e revisiona tutti gli accessi fisici. Ciò include:

a) Identificazione ed autenticazione del personale del cliente e del provider che hanno accesso fisico ai beni che costituisco no i servizi offerti al cliente.

b) Il processo di richiesta ed approvazione dell'accesso fisico.

c) Se i beni fisici sono dedicati solo al cliente o sono condivisi tra più clienti.

d) Come i beni fisici sono separati (fisicamente) e segregati in modo sicuro da altri beni del provider e da beni di altri clienti.

e) La protezione dei beni del cliente da accesso fisico non autorizzato.

[PS2] Il provider dimostra la presenza di sistemi di sicu-

rezza fisica quali: generatori di riserva, sistemi di climatizzazione ridondanti, sistemi antincendio per la protezione e prevenzione.

5.4.4 Gestione dei dati (DH)

[DH1] L'uso dei dati del cliente da parte del provider per operazioni di data mining o qualsiasi altro proposito che va oltre gli scopi del servizio non è permesso senza una esplicito consenso scritto del proprietario dei dati.

[DH2] Il provider afferma che tutti i dati dei clienti verranno rimossi da tutti i computer.

5.4.5 Autenticazione ed Autorizzazione (AA)

[AA1] Il provider dichiara un intervallo di tempo di risposta per:

a) La fornitura di nuovi accessi utente dal tempo di ricezione della richiesta [BITS 01, Section 5.5.1, p 29].

b) La creazione, il cambiamento o la cancellazione di user ID e password.

[AA2] Il provider tiene un registro di tutte le autorizzazioni e le richieste d'accesso includendo l'origine della richiesta [BITS 01, Section 5.5.2-5.5.3, p 29].

5.4.6 Controllo d'Accesso (AC)

[AC1] Determina quali dati appartengono al cliente e quali dati che richiedono l'accesso del cliente appartengono al provider. Il proprietario dei dati determina i diritti d'accesso.

[AC2] Documenti che richiedono l'uso della cifratura, il mantenimento delle rispettive chiavi e d'ogni altro requisito infrastrutturale ad esse collegato. Indirizza "l'intera transazione (sorgente, immagazzinamento, percorso di rete, backup, recupero ed ogni altro requisito richiesto dalla legislazione" [BITS 01, Section 5.4.7, p 28].

[AC3] Lo SLA dovrebbe specificare:

a) a quali beni il provider deve essere in grado di accedere per realizzare la fornitura del servizio contrattato;

b) che il cliente è pronto ed è in grado di fornire il diritto a tale accesso.

5.4.7 Integrità del Software (SI)

[SI1] Specifica la frequenza col quale il provider compara i controlli delle chiavi crittografiche col set base di quelle riconosciute ed immagazzinate in modo sicuro.

5.4.8 Configurazione di sicurezza dei beni (SC)

[SC1] Il provider informa il cliente su ogni modifica all'hardware o al software che lo può interessare, prima che tali cambiamenti vengano fatti. Questo tipo di cambiamenti potrebbe coinvolgere ogni cosa, dall'installazione di un nuovo server all'aggiornamento di software per la sicurezza. Se richiesto, al cliente dovrebbe essere data l'opportunità di testare questi cambiamenti prima che questi vengano realizzati, fornendo un resoconto al provider [Alner 01].

[SC2] Tutti i cambiamenti del provider che possono interessare i servizi od i dati del cliente insieme all'impatto anticipato del cliente sono comunicati al punto di contatto designato dal cliente. Il cliente può aver necessità di negoziare il ritegno al diritto di approvazione per tutti questi cambiamenti. Questo livello di servizio specifica il numero di giorni o settimane d'anticipo con cui deve essere notificato il cliente.

[SC3] Per la valutazione delle vulnerabilità ed i test d'intrusione, identifica i ruoli e le responsabilità di cliente e provider, la frequenza di valutazione, il tempo per la notifica delle vulnerabilità identificate e sulla base del livello di rischio della vulnerabilità il tempo di risoluzione. Tali test devono essere coordinati col provider e non dovrebbero aver impatto sulla disponibilità del

sistema, sui livelli di mancato servizio, downtime o insoddisfazione del cliente [BITS 01, Section 5.7, p 31].

[SC4] Il provider specifica il processo ed il tempo per l'applicazione e la verifica di eventuali patch.

[SC5] Specifica che cambiamenti non documentati o configurazioni non riportate sono causa di penalità contrattuali. Il cliente può identificare tali penalità eseguendo una revisione della configurazione, un accertamento della vulnerabilità che includa un test di intrusione che sfrutta cambiamenti non documentati.

5.4.9 Backup (BU)

[BU1] Definisce le responsabilità per il backup dei dati insieme alla descrizione delle linee guida per l'intero ciclo di vita di protezione dei dati (creazione, uso e distruzione). Include:

a) Linee guida per la frequenza dei backup (tipo backup completi settimanali e backup parziali giornalieri).

b) Tempi di ristoro da backup.

c) Tempi di conservazione (tipo un mese per i file memorizzati sul sito primario).

d) Tempi di distruzione.

e) Luoghi di immagazzinamento fuori dal sito e tempi (tipo un anno per file memorizzati in un sito secondario per il recupero da disastri).

[BU2] Se il provider gestisce i sistemi di servizio che sono critici per la missione del cliente, un mancato funzionamento del sistema può precludere il cliente dall'abilità di adempiere a tale missione. Si consideri un accordo che specifichi un tempo accettabile per recuperare i dati da backup fidati dopo un guasto nelle apparecchiature o qualsiasi altro problema nel sistema.

[BU3] Si specifichi una livello di penalità per il mancato svolgimento dei backup entro i tempi richiesti.

5.4.10 Monitoraggio e valutazione (MA)

[MA1] Il provider usa appropriate sistemi di monitoraggio, verifica ed ispezione ed afferma la propria responsabilità per le attività di reporting, valutazione e risposta ad eventi e condizioni su sistemi e reti. Ciò include:

a) Uso regolare di strumenti per il monitoraggio di sistemi e reti, esaminando i risultati prodotti.

b) Uso regolare di strumenti di filtro ed analisi di log, esaminando i risultati prodotti.

c) Filtraggio delle informazioni di logging usando strumenti automatici per diminuire l'ammontare delle informazioni che gli analisti devono ispezionare. Il provider descrive quanto spesso in condizioni normali i risultati del monitoraggio vengono ispezionati.

[MA2] Il provider assicura che i risultati dell'attività di monitoraggio ed i file di log vengono generati su memorie WORM (Write Once Read More) in modo da non poter essere sovrascritte o danneggiate e poi memorizzati su supporti a sola lettura. Questo assicura che utenti non autorizzati possano alterare o cancellare il contenuto dei file.

[MA3] Il provider descrive:

a) Quanto spesso l'attività di monitoraggio viene effettuata e se questa è fatta in tempo reale o meno.

b) Come vengono monitorati i sistemi e le reti.

c) Se il monitoraggio include tutto il traffico entrante ed uscente dalla rete.

d) Se il monitoraggio include l'intero traffico di rete (fire wall, rilevazione di intrusione, router, server applicazioni del cliente) e come viene eseguita la correlazione tra tutte le sorgenti di dati.

e) Come vengono riportati i risultati significativi dell'attività di monitoraggio.

f) Come vengono immagazzinati i risultati di monitoraggio, includendo i log.

g) Come gli strumenti di monitoraggio sono protetti e resi sicuri.

[MA4] Il provider descrive i loro processi in corso per un'analisi globale delle vulnerabilità e delle minaccie insieme alle sorgenti utilizzate per tali analisi.

5.4.11 Gestione degli incidenti (IM)

[IM1] Descrive il livello degli eventi accidentali che il provider gestisce (assumendo che il provider monitori l'attività corrente) e quale livello dell'evento va riportato al cliente [Alner 01]. Questo include se consultare o meno il cliente prima che ogni azione venga messa in pratica. Alcuni provider preferiscono prima agire per fermare l'attacco e poi informare il cliente di quello che è accaduto [DeJesus 01].

[IM2] Specifica i ruoli e le responsabilità del provider nell'evento di un attacco. La risposta del provider può ampiamente variare da una notifica post-attacco ad una consultazione in diretta per avere piena responsabilità per risposte in tempo reale, investigazioni e procedimenti civili o penali. Ogni limitazione nella risposta del provider pone una difficoltà ulteriore per il cliente. Specifica il personale chiave (includendo backup) in entrambe le organizzazioni e come essi devono essere notificati degli eventi e sotto quali condizioni [DeJesus 01].

[IM3] Se il provider deve gestire le problematiche e le questioni di sicurezza degli utenti e del cliente, le linee guida dello SLA devono delineare cosa il provider dovrebbe maneggiare, di chi è richiesta l'autorizzazione per indirizzare problemi di routine e quali tipo di problematiche dovrebbero essere riferite allo staff proprio del cliente.

[IM4] Descrive i dati richiesti per i report di violazione e l'abilità del provider nel supportare ogni eventuale investigazione. La revisione e l'investigazione di tali violazioni possono essere

meglio gestite dallo staff interno del cliente perchè questo conosce meglio quali sono i dati critici [Alner 01].

[IM5] Il cliente ed il provider devono concordare sui requisiti e sui processi per la gestione degli incidenti e su come documentarli, assumendo che questo servizio sia fornito. Questo processo include [BITS 01, Section 5.6, p 29-30]:

a) Identificazione di cosa costituisce un incidente e dei livelli di severità:
    i) Verifica o tentativo di violazione dell'accesso utente.
    ii) Tentativo d'intrusione sul sistema del provider o sulla rete usata dal provider per la fornitura del servizio al cliente.
    iii) Tentativo d'intrusione sul sistema del cliente e sulla sua rete.
b) Log di tutti gli incidenti.
c) Escalation e monitoraggio delle azioni intraprese incluse le circostanze sotto cui il servizio è stato interrotto.
d) Notifica automatica (ad esempio via allarme) di incidenti seri ed a chi tale notifica deve essere inoltrata.
e) Log (in un formato elettronico sicuro) da fornire alle parti responsabili per la revisione; quanto tempo tali log devono essere mantenuti.
f) Il lasso di tempo tra l'incidente e la notifica verbale al cliente.
g) Qualsiasi requisito per la notifica ridondante basata sulla severità dell'incidente (come telefono, email ,fax, etc.).
h) Forensic analysis.
i) Investigazioni civili o penali includendo la necessaria interfaccia con le autorità giudiziarie.

[IM6] Il cliente o il provider possono trovarsi ad affrontare "i costi per rimediare a problemi di sicurezza laddove ciò sia

dovuto ad un mancato adempimento degli obblighi, più che ad una falla o una violazione" [BITS 01, Section 5.6, p 29]. Come risultato, è critico che ruoli e responsabilità siano chiaramente definiti nel processo di gestione degli incidenti menzionato sopra.

5.5 L'outsourcing dei servizi di Telecomunicazioni

In questo esempio si considera lo specifico ambito dei servizi di telecomunicazione quale oggetto dell'affidamento in outsourcing. Lo scopo è di esemplificare l'attuazione delle clausole contrattuali suggerite nei paragrafi precedenti in un reale contesto applicativo.

Viene mostrata una metodologia che consiste nel comprendere se è necessario applicare ciascuna specifica clausola al servizio in oggetto (una rete di Telecomunicazioni). In tal senso si intende anche dare una breve spiegazione dei motivi che portano ad escludere l'applicazione di una serie di clausole.

Di fatto si propone un case-study per la compilazione di una matrice di corrispondenza tra le clausole dello SLA prototipo (mostrato nei paragrafi precedenti) ed i servizi di Telecomunicazioni.

Per comprendere il contesto del caso di studio è necessario innanzitutto definire "l'oggetto dell'outsourcing", che trattandosi appunto di un case-study non è riferito ad uno specifico caso reale ma è però ispirato da diverse esperienze nell'acquisizione di servizi di Telecomunicazioni.

Definiamo innanzi tutto il perimetro dei servizi che sono oggetto dell'outsourcing in questo case-study:

- Il progetto dell'infrastruttura di rete
- La realizzazione dell'infrastruttura di rete (backbone e accesso)
- La gestione dell'infrastruttura di rete di backbone
- La gestione dell'infrastruttura della rete di accesso.

Il committente affiderà la fornitura dei servizi di outsourcing in fasi differenti e con contratti separati, secondo la separazione indicata nei punti sopra citati.

In pratica con un progetto un primo outsourcer realizzerà l'infrastruttura di rete (sia per la parte relativa al backbone che per la parte relativa alla sezione di accesso, comprendendo le apparecchiature di rete e i vettori trasmissivi).

L'infrastruttura di rete, che sarà di proprietà del committente, fatta eccezione per i vettori trasmissivi, affittati dall'outsourcer, viene poi affidata in gestione ad un outsourcer, per tutte le attività inerenti l'erogazione dei servizi end-to-end della rete stessa.

Il committente intende peraltro riservarsi tutti i diritti di monitoraggio e governo dell'infrastruttura, prevedendo la partecipazione anche di proprie risorse alla gestione, configurando perciò una situazione di non completo outsourcing (qualcuno lo chiama "cosourcing") per conservare le proprie legittime prerogative sul controllo dell'infrastruttura stessa.

Nel seguito vengono approfonditi soprattutto gli aspetti inerenti la fase di gestione dell'infrastruttura (mentre non viene approfondita la fase realizzativa, che segue uno schema "a progetto") con lo scopo di evidenziare come le clausole contrattuali entrino in gioco (o non vengano, invece, ritenute necessarie) per le caratteristiche intrinseche del servizio affidato in outsourcing, oppure in base alle scelte di natura organizzativa associate ai processi connessi al servizio.

Nella Tabella 7 si correlano le clausole contrattuali suggerite nei paragrafi precedenti alla loro possibile attuazione nel contesto appena descritto (per semplificare la lettura, nella seconda colonna si richiama in modo molto sintetico il contenuto della clausola).

Laddove nella Tabella 7 siano state individuate clausole normalmente non impiegate oppure impiegate in modo parziale, viene data nel seguito una motivazione riferita alla specifica nota:

Clausola	*Descrizione sintetica*	*E' applicata?*
VI1	Trasparenza verso il cliente	**SI**
VI2	Protezione dei beni del cliente	**SI**
CS1	Requisiti di livello di servizio su problema	**SI**
CS2	Analisi periodica di soddisfazione (outsourcer)	**NO(1)**
CS3	Analisi periodica di soddisfazione (committente)	**SI**
RO1	Protezione della documentazione	**SI(2)**
RO2	Trasparenza gestione subfornitori	**SI**
RO3	Responsabilità rispetto ai subfornitori	**SI**
RO4	Evidenza contrattuale verso i subfornitori	**SI(3)**
IE1	Assessment di terze parti	**NO(4)**
IE2	SLA per Assessment di terze parti	**NO(4)**
PR1	Trasferimento della conoscenza al committente	**SI**
PR2	Rapporti di confidenzialità	**SI**
PR3	Processo di sicurezza per il cliente	**NO(5)**
AO1	Proprietà dei beni	**SI**
CE1	Ricorsi e azioni	**SI(6)**
CE2	Penali fino al 100% della fornitura	**NO(7)**
CE3	Rinegoziabilità degli SLA	**SI(8)**
ES1	Terminazione normale e anticip.	**SI**
ES2	Definizione resp. Contrattuali	**SI**
PC1	Punti di contatto cliente/forn.	**SI**
SY1	Piano temporale di messa in opera	**SI**
SY2	Criteri temporali di valutazione della disponibilità del servizio	**SI**
SY3	Periodi di uptime	**SI(9)**
SY4	Tempi di risposta al guasto	**SI**
SY5	Raccolta dati sul tempo di disserv.	**SI**
SY6	Proattività efficienza tecnologica	**NO(10)**
SS1	Scalabilità	**SI**
SL1	Requisiti prestazionali	**SI**
SL2	Pesatura dei servizi	**SI(11)**
SL3	Definizione responsabilità per emergenze	**SI**
SL4	Gestione richieste speciali	**NO(12)**
RR1	Struttura dei report	**SI**
RR2	Contenuto dei report	**SI**
RR3	Intervalli temporali di reporting	**SI**
SP1	Change request management	**SI**

Tabella 7: clausole contrattuali

SP1	Change request management	**SI**
SP2	Adeguamento tecnologico	**SI**
PP1	Definizione e condivisione req. sicurezza	**SI**
PP2	Accertamento conflitti di sicurezza tra cliente e outsourcer	**SI**
PP3	Conformità ad uno standard comune	**SI**
PP4	L'outsourcer descrive le proprie metodologie di sicurezza	**SI**
PP5	L'outsourcer dimostra la conformità dell'implementazione ai requisiti di sicurezza	**SI**
DR1	Descrizione degli scenari DR	**SI**
DR2	Tempi di recupero in caso di DR	**SI**
DR3	Processi di escalation in caso di DR	**NO**(13)
DH1	Gestione dei dati del cliente	**SI**
DH2	Cancellazione dei dati del cliente	**SI**
AA1	Tempi di provisioning per la sicurezza	**SI**
AA2	Tenuta dei log e dei registri d'abilitazione	**SI**
AC1	Gestione dei diritti d'accesso	**SI**
AC2	Utilizzo della cifratura	**NO**(14)
AC3	Accesso alle risorse del cliente	**SI**(15)
SI1	Controllo delle chiavi crittografiche	**NO**(14)
SC1	Notifica dei cambiamenti	**SI**
SC2	Approvazione dei cambiamenti (e tempi associati)	**SI**
SC3	Test di vulnerabilità	**NO**(4)
SC4	Patch management	**SI**
SC5	I cambiamenti non documentati sono causa di penalità	**SI**
BU1	Backup dei dati	**SI**(16)
BU2	Tempi di ripristino dei dati	**SI**(16)
BU3	Penalità per mancato backup	**SI**(16)
IM1	Politiche di Incident Management	**SI**
IM2	Ruoli in caso d'attacco	**SI**
IM3	Definizioni dei confini di competenza	**SI**
IM4	Report e supporto all'investigazione	**SI**
IM5	Documentazione processi di sicurezza	**SI**
IM6	Responsabilità civili per incidente	**SI**(17)

Tabella 7: clausole contrattuali

- CS2 Analisi periodica di soddisfazione (outsourcer): Questa attività viene svolta internamente poiché la rete è proprietaria

- RO1 Protezione della documentazione: Questa clausola è in realtà di natura generale e non specifica per ogni documento

- RO4 Evidenza contrattuale verso i subfornitori: Clausola di natura generale che prevede la piena responsabilità dell'outsourcer (in realtà non equivale pienamente alla clausola suggerita)

- IE1 Assessment di terze parti -- IE2 SLA per Assessment di terze parti -- SC3 Test di vulnerabilità: Data la natura del rapporto di gestione dell'infrastruttura di rete queste attività rimangono totalmente in capo al committente in quanto proprietario dell'infrastruttura. Peraltro ciò consente un maggior grado di flessibilità nella scelta delle eventuali terze parti. L'accesso alla infrastruttura da parte del committente non deve essere vincolato ad autorizzazione ma basta una normale comunicazione

- PR3 Processo di sicurezza per il cliente: La responsabilità della gestione della infrastruttura viene di fatto condivisa tra committente e outsourcer secondo quanto deve essere specificato in clausole di natura più generale. L'addestramento del personale del committente e la condivisione dei requisiti di sicurezza è parte integrante del processo di gestione. Se specificata, questa clausola rischia d'essere solo una sorta di manleva per l'outsourcer

- CE1 Ricorsi e azioni: Nel caso delle infrastrutture di rete ogni forma di miglioramento delle prestazioni si considera di fatto incorporata all'atto della negoziazione (se l'outsourcer ha la possibilità di fornire uno SLA migliore normalmente lo dichiara). Pertanto non è usuale l'adozione del "bonus". Per il resto, la clausola è prevista

- CE2 Penali fino al 100% della fornitura: Il 100% di penale non è normalmente applicata. In alternativa è possibile pretendere meccanismi di rivalsa sotto forma di risarcimento danni, per massimali anche superiori al 100% del valore del contratto. Si tratta però di una clausola ben diversa anche dal punto di vista della sua esecuzione

- CE3 Rinegoziabilità degli SLA: La rinegoziazione viene

richiesta ma in modo che sia unilaterale (a favore del committente). Se non può essere così, meglio non chiederla

- SY3 Periodi di Uptime: Nel caso delle reti di telecomunicazioni viene normalmente richiesto il rispetto di un complesso capitolato di parametri di uptime (spesso riferiti a specifiche forniture). Questo punto quindi viene "esploso" in uno specifico allegato abbastanza complesso. In generale la clausola è necessaria per governare il roll-out e la gestione successiva

- SY6 Proattività efficienza tecnologica: Il criterio secondo il quale l'outsourcer si impegna ad adeguare (o almeno a proporre gli adeguamenti) i propri sistemi per "meglio servire" il committente ben si applica al caso del software. Nel caso delle reti invece questo miglioramento tecnologico viene forzato dal committente nella previsione di scalabilità funzionale. In caso contrario si affiderebbe all'outsourcer una sorta di delega all'adeguamento hardware (con incorporata una probabile attribuzione di costi)

- SL2 Pesatura dei servizi: Come già detto, nel caso delle reti di telecomunicazione non viene normalmente previsto un criterio di bonus. La pesatura è comunque un aspetto utilizzato per calcolare le condizioni di non rispetto del valore di SLA concordato

- SL4 Gestione richieste speciali: Questo requisito è di fatto incorporato nella gestione del change management (le richieste speciali che richiedono nuove acquisizioni di solito sfociano in contratti specifici)

- DR3 Processi di escalation in caso di DR: Si intende l'infrastruttura come già pienamente ridondata anche a supporto delle funzioni di DR dei servizi ICT del committente. Pertanto il processo di escalation in caso di DR (sia dell'infrastruttura stessa che dei servizi da essa supportati) è incorporato nei rapporti di escalation ICT

- AC2 Utilizzo della cifratura -- SI1 Controllo delle chiavi crittografiche: L'infrastruttura oggetto di outsourcing viene considerata come sistema di trasporto. La cifratura (quando necessaria) viene attivata a livello committente, per esempio impiegando tunnel IPSEC. Il committente è autonomo nella gestione delle chiavi

- AC3 Accesso alle risorse del cliente: A parte l'accesso fisico ai luoghi di installazione, non è normalmente richiesto l'accesso a servizi del committente da parte dell'outsourcer. Questa clausola viene espressa piuttosto nella definizione dei meccanismi di calcolo dei tempi di ripristino (ritardi nel ripristino non imputabili all'outsourcer). Ad esempio quando l'outsourcer non può accedere ad una sede per riparare un guasto per motivi dipendenti dal committente

- BU1 Backup dei dati -- BU2 Tempi di ripristino dei dati -- BU3 Penalità per mancato backup: Le infrastrutture di rete richiedono questo servizio solo per le funzioni ospitate dagli apparati di rete e dai sistemi di management. Queste funzioni sono richieste a livello di progetto ma gestite dal committente (o in modo congiunto)

- IM6 Responsabilità civili per incidente: Vengono normalmente richieste forme di assicurazione rispetto ai possibili danni.

E' opportuno ricordare che le clausole contrattuali costituiscono solo lo strumento di conduzione dell'infrastruttura. Ciascuna delle clausole richiede uno sforzo a volte consistente per l'esercizio del diritto cui corrisponde.

Nel caso delle infrastrutture di Telecomunicazione spesso le clausole che introducono le penali, per quanto punitive, non rappresentano una soluzione ai possibili maggiori danni dovuti al mancato rispetto delle clausole contrattuali.

Per questo motivo vengono a volte adottati dei meccanismi di monitoraggio proattivo finalizzato a individuare possibili degradi del servizio ben prima che questi possano rappresentare una fonte di contenzioso contrattuale. E' importante che il committente abbia costante visibilità del comportamento degli apparati di rete e che quindi i sistemi di gestione siano accessibili anche in modo diretto.

Nota a margine: occorre evidenziare, relativamente alla gestione operativa di una grande infrastruttura critica nazionale, che l'approccio ad un outsourcing completo, sia esso riferito a puri

Servizi di Telecomunicazioni che a Servizi Informatici, è necessariamente di tipo cautelativo. Le considerazioni riportate nel presente paragrafo, con riferimento alle clausole contrattuali enunciate in Tabella 7, risentono, di fatto, delle scelte di modelli contrattuali adottati dall'azienda oggetto dell'esempio.

Outsourcing e sicurezza

Appendice A
Lista degli acronimi

Acronimo	Significato
SLA	Service Level Agreement
OLA	Operation Level Agreement
ISO	International Standards Organization
IEC	International Electrotechnical Commission
IT	Information Technology
ICT	Information & Communication Technology
ITIL	IT Infrastructure Library
ROI	Return On Investment
TCO	Total Cost of Ownership
COBIT	Control OBjectives for Information and related Technology
CNIPA	Centro Nazionale per Informatica nella Pubblica Amministrazione
EAI	Enterprise Application Integration
CRM	Customer Relationship Management
SAS	Statement on Auditing Standard
AICPA	American Institute of Certified Public Accountants
CEO	Chief Executive Officer
CIO	Chief IT Officer
CSO	Chief Security Officer

Appendice B
Riferimenti

[ISCOM 01] Linee guida sulla sicurezza delle reti - DALL'ANALISI DEL RISCHIO ALLE STRATEGIE DI PROTEZIONE, ISCOM, 2005.

http://www.iscom.gov.it/documenti/files/news/

pub_002_ita.pdf

[ISCOM 02] Linee guida sulla sicurezza delle reti - NELLE INFRASTRUTTURE CRITICHE, ISCOM, 2005.
http://www.iscom.gov.it/documenti/files/news/pub_003_ita.pdf

[CNIPA 01] Elenco dei servizi, www.cnipa.gov.it

[BITS 01] BITS Framework: Managing Technology Risk for Information Technology (IT) Service Provider Relationships, Version 3.2a. BITS IT Service Providers Working Group, October, 2001. Available at
http://www.bitsinfo.org/FrameworkVer32.doc.

[Hiles 02] Hiles, Andrew. The Complete Guide to IT Service Level Agreements: Aligning IT Service to Business Needs, Third Edition. Rothstein Associates Inc., Brookfield, CN, 2002. Ordering information is available at http://www.servicelevelbooks.com.

[CIO 01] "Service Level Agreement," CIO.com. Available at http://www.cio.com/summaries/outsourcing/sla/index.html.

[Nicolett 02] Nicolett, M., Matlus, R. "SLAs With Outsourcers May Provide Less Than You Realize." Gartner Commentary, 21 January 2002.

[NM 01] Network Magazine India. "Crafting the Service Level Agreement. India Express Group, 2001. Available at http://www.networkmagazineindia.com/200111/focus1.htm

[Navarro 01] Navarro, Luis. "Information Security Risks and Managed Security Service." Information Security Technical Report, Vol 6, No. 3, Elsevier, 2001.

[Hiles 02] Hiles, Andrew. The Complete Guide to IT Service Level Agreements: Aligning IT Service to Business Needs, Third Edition. Rothstein Associates Inc., Brookfield, CN, 2002. Ordering information is available at http://www.servicelevelbooks.com.

[Alner 01] Alner, Marie. "The Effects of Outsourcing on Information Security." Information Systems Security. Auerbach Publications, CRC Press LLC, May/June 2001.

[Cramm 01] Cramm, Susan. "The Dark Side of Outsourcing." CIO Magazine, Nov 15, 2001. Available at http://www.cio.com/archive/111501/hs_handson.html

[DeJesus 01] DeJesus, Edmund. "Managing Managed Security." Information Security Magazine, January, 2001. Available at http://www.infosecuritymag.com/articles/january01/cover.shtml.

[SAS70 01] http://www.sas70.com.

[SAS70 02] http://www.ahpplc.com.

Tutte le Linee Guida Iscom sono scaricabili dal sito
www.iscom.gov.it

realizzazione GRAPHICLAB
SETTORE DIVULGAZIONE E COMUNICAZIONE ESTERNA ISCOM

Ministero delle Comunicazioni

iscom
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

DIVULGAZIONE E
COMUNICAZIONE ESTERNA

LINEE GUIDA ISCOM PUBBLICATE

SICUREZZA DELLE RETI DALL'ANALISI DEL RISCHIO ALLE STRATEGIE DI PROTEZIONE

SICUREZZA DELLE RETI NELLE INFRASTRUTTURE CRITICHE

LA QUALITÀ DEI SERVIZI NELLE RETI ICT

GESTIONE DELLE EMERGENZE LOCALI

RISK ANALYSIS APPROFONDIMENTI

QUALITÀ DEL SERVIZIO SU UMTS

QUALITÀ DEI SERVIZI PER LE PMI SU RETI FISSE A LARGA BANDA

CERTIFICAZIONE DELLA SICUREZZA ICT

OUTSOURCING E SICUREZZA