

Certificazione tecnica di Telecom Italia per l'anno 2010 (ex delibera AGCOM 152/02/CONS, art. 2, c.7)



TOGETHER. FREE YOUR ENERGIES

Stato documento: PUBBLICO *draft* ☐ *approvato* ☐ *consegnato* ☒

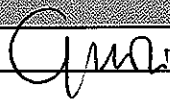
Riferimento TWA152/10-RP

Versione NA

Data creazione 22/06/2010

CW

REVISIONE E APPROVAZIONE

FUNZIONE	NOME	DATA	FIRMA
Capgemini Italia	Corrado Giustozzi	22/06/2010	

INDICE

1. SCOPO DEL DOCUMENTO.....	4
1.1 Struttura del documento	4
1.2 Documenti applicabili e di riferimento.....	4
1.3 Abbreviazioni.....	5
2. PREMESSA	6
2.1 Contesto normativo e regolamentare	6
2.1.1 L'AGCOM e la delibera 152/02/CONS.....	6
2.1.2 L'evoluzione della norma: ulteriori delibere AGCOM.....	8
2.2 Le attività di adeguamento messe in atto da Telecom Italia	9
2.2.1 Le misure adottate.....	9
2.2.2 La certificazione tecnica	10
3. L'ATTIVITÀ DI CERTIFICAZIONE TECNICA	12
3.1 La metodologia.....	12
3.2 L'ambito d'intervento	12
3.3 La modalità d'indagine	13
3.4 Il risultato atteso sui sistemi.....	13
4. LA CERTIFICAZIONE TECNICA 2010.....	16
4.1 Funzioni aziendali interessate	16
4.2 Piano delle attività	17
4.3 Dettaglio delle attività svolte	19
5. ESITI DELL'ATTIVITÀ.....	22
5.1 Verifiche sui sistemi oggetto d'indagine	22
5.2 Verifiche sulle azioni "non sui sistemi"	23
5.2.1 Diffusione del codice di comportamento	23
5.2.2 Copertura delle clausole contrattuali.....	23
5.2.3 Gestione e controllo automatizzato delle abilitazione delle utenze	24
6. CONCLUSIONI DELLA CERTIFICAZIONE TECNICA	25
6.1 Valutazione dei sistemi oggetto d'indagine	25
6.2 Valutazione delle azioni "non sui sistemi".....	26
6.3 Valutazione conclusiva	27
6.4 Suggerimenti e raccomandazioni.....	28

1. SCOPO DEL DOCUMENTO

Questo documento costituisce la relazione finale di sintesi dell'attività di certificazione tecnica che Capgemini Italia S.p.A. (di seguito anche Capgemini), in qualità di "soggetto terzo", ha svolto nei confronti di Telecom Italia S.p.A. (di seguito anche Telecom oppure TI) nel corso dell'anno 2010 allo scopo di verificare l'avvenuta separazione tra i sistemi informativi delle funzioni di rete e delle funzioni commerciali, come richiesto al comma 7 dell'articolo 2 della delibera 152/02/CONS *"Misure atte a garantire la piena applicazione del principio di parità di trattamento interna ed esterna da parte degli operatori aventi notevole forza di mercato nella telefonia fissa"*.

1.1 Struttura del documento

Questa relazione di sintesi è così organizzata:

- ▶ il presente **Capitolo 1 (Scopo del documento)** riporta le usuali **informazioni di servizio** sul documento quali lo scopo, i riferimenti e le abbreviazioni utilizzate nel testo;
- ▶ il **Capitolo 2 (Premessa)** descrive il **contesto normativo ed organizzativo** nel quale si colloca l'attività di certificazione e ne descrive finalità ed obiettivi;
- ▶ il **Capitolo 3 (L'attività di certificazione tecnica)** descrive il **processo generale** messo a punto per lo svolgimento dell'attività di certificazione;
- ▶ il **Capitolo 4 (La certificazione tecnica 2010)** descrive il **progetto di certificazione tecnica relativo all'anno 2010** descrivendone sinteticamente le caratteristiche, le modalità operative con cui è stato svolto, le attività che sono state effettuate;
- ▶ il **Capitolo 5 (Esiti dell'attività)** riporta i **risultati ottenuti** al termine del progetto, in termini di rispondenza delle misure riscontrate rispetto ai risultati attesi;
- ▶ il **Capitolo 6 (Conclusioni della certificazione tecnica)** riporta specificamente, ed in sintesi, le **valutazioni conclusive finali** dell'attività di indagine effettuata.

1.2 Documenti applicabili e di riferimento

I seguenti documenti sono richiamati nella relazione e/o costituiscono riferimenti primari per le attività descritte.

ID.	NOME	RIFERIMENTO
152/02/CONS	Delibera AGCOM: "Misure atte a garantire la piena applicazione del principio di parità di trattamento interna ed esterna da parte degli operatori aventi notevole forza di mercato nella telefonia fissa"	

Riferimento: TWA152/10-RP	Versione: NA	Data Creazione: 22/06/2010
PUBBLICO		Pagina 4 di 28

1.3 Abbreviazioni

Le seguenti sigle ed acronimi sono utilizzati nella relazione.

ABBREVIAZIONE	SIGNIFICATO
AGCOM	Autorità per le Garanzie nelle Comunicazioni
CPS	Carrier Pre Selection
CS	Carrier Selection
GUI	Graphical User Interface
MIMIP	Misure Minime Privacy (sistema di gestione)
NP	Number Portability
OLO	Other Licensed Operators
TI	Telecom Italia
ULL	Unbundling Local Loop

2. PREMESSA

Questo capitolo introduttivo descrive il contesto nel quale si colloca l'attività di certificazione e ne descrive finalità ed obiettivi.

2.1 Contesto normativo e regolamentare

L'esigenza per Telecom Italia di sottoporsi annualmente ad una certificazione tecnica di terza parte, la quale verifichi l'effettiva *"separazione tra sistemi informativi delle funzioni di rete e delle funzioni commerciali"*, nasce da un preciso obbligo regolamentare imposto dall'Autorità per le garanzie nelle comunicazioni.

In questa sezione è brevemente richiamato il contesto normativo e regolamentare nel quale si origina l'attività di certificazione.

2.1.1 L'AGCOM e la delibera 152/02/CONS

L'Autorità per le garanzie nelle comunicazioni (AGCOM) è un'autorità amministrativa indipendente, istituita in Italia con la legge 31 luglio 1997 n. 249, che ha in sostanza ereditato le funzioni in precedenza attribuite all'ex "Garante per la radiodiffusione e l'editoria". Essa ha il duplice compito di assicurare la corretta competizione degli operatori sul mercato e di tutelare i consumi nel rispetto delle libertà fondamentali dei cittadini attraverso garanzie che riguardano sia gli operatori che gli utenti.

L'Autorità svolge una funzione attiva di controllo dell'intero mercato delle comunicazioni, i cui attori devono conformarsi in primis ai principi dell'art. 21 della Costituzione: pluralismo e promozione della concorrenza, garanzia di un'informazione imparziale, completa, obiettiva e di qualità. Ha inoltre competenze in materia tariffaria, di qualità, nonché di controllo degli operatori del mercato.

Nell'ottemperanza dei suoi compiti, nel 2002 l'AGCOM ha emanato la delibera 152/02/CONS *"Misure atte a garantire la piena applicazione del principio di parità di trattamento interna ed esterna da parte degli operatori aventi notevole forza di mercato nella telefonia fissa"*.

In particolare l'articolo 2 della Delibera 152/02/CONS prevede quanto segue:

"(Condizioni per assicurare la parità di trattamento)

- 1. L'operatore notificato garantisce che, entro il 31 dicembre 2002, mediante opportune misure organizzative sul piano della separazione amministrativa e contabile e della trasparenza, da sottoporre all'approvazione dell'Autorità, le unità organizzative preposte alla gestione della rete siano sufficientemente separate da quelle preposte alla vendita dei servizi finali.*

2. L'Autorità verifica che le misure adottate garantiscano:
- a. che la fornitura di servizi di rete alle proprie unità organizzative commerciali avvenga attraverso accordi che esplicitino le condizioni generali di fornitura tecnico-economiche. Tali accordi devono contenere almeno le clausole di cui all'allegato C;
 - b. che la fornitura di servizi di rete avvenga assicurando il medesimo livello di servizio e assistenza sul territorio agli operatori interconnessi e alle unità organizzative commerciali interne o a società collegate o controllate;
 - c. che la contrattualizzazione e la vendita di servizi di rete sia condotta da soggetti distinti da quelli che operano nelle unità organizzative commerciali che offrono servizi finali;
 - d. che la gestione di dati commerciali e di informazioni relative al traffico degli operatori interconnessi sia separata dalla gestione e l'utilizzo dei dati a fini commerciali. In particolare, i sistemi informativi e gestionali relativi ai dati degli operatori interconnessi sono gestiti da personale differente da quello preposto alle attività commerciali verso i clienti finali e tali sistemi non sono accessibili al personale delle unità organizzative commerciali che forniscono servizi ai clienti finali;
 - e. che a seguito dell'implementazione delle misure organizzative di cui al presente articolo la contabilità regolatoria rifletta adeguatamente l'evoluzione dei trasferimenti interni tra le varie unità.
3. L'operatore notificato, nell'esecuzione degli accordi di cui al comma 2, lett. a), assicura la parità di trattamento interna/esterna sugli aspetti relativi alla fornitura (di seguito provisioning), alle azioni sistematiche per la garanzia di rispondenza alle specifiche e di qualità complessiva per le attività elementari (di seguito assurance), necessarie sia alla fornitura del servizio commerciale all'utente finale, sia alla fornitura di servizi intermedi per gli OLO. In particolare, le condizioni generali di fornitura tecnico-economiche e i valori degli indicatori di qualità contenuti negli ordinativi interni relativi a ciascun servizio di rete offerto dalle unità organizzative preposte alla gestione della rete dell'operatore notificato (rete di trasporto e rete di accesso nella contabilità regolatoria) alle proprie unità organizzative commerciali sono le medesime offerte agli OLO per ciascun analogo servizio di rete.
4. L'operatore notificato comunica all'Autorità, contestualmente all'adozione delle misure di cui al comma 1, le modalità e le condizioni generali di fornitura tecnico- economiche, ivi inclusi gli indicatori di qualità, di cui al comma 3, previste negli ordinativi interni relativi ai servizi di rete tra le proprie funzioni di rete e commerciali, nonché gli accordi tra funzioni di rete e OLO. Eventuali variazioni alle condizioni tecniche succitate sono comunicate all'Autorità con 30 giorni di anticipo.
5. Le condizioni tecniche di fornitura sopra indicate sono oggetto di una relazione semestrale da parte dell'operatore notificato. Tale relazione, da presentarsi entro il 31 dicembre 2002 e successivamente ogni sei mesi, riporta in allegato una tabella comparativa dei

valori, misurati dall'operatore notificato, degli indicatori di cui all'allegato C, in modo tale che sia possibile verificare la qualità erogata alle proprie funzioni commerciali e agli OLO che fanno uso dei medesimi beni intermedi. L'Autorità utilizza i dati così ricavati anche ai fini della verifica del rispetto della parità di trattamento.

6. *Qualora emerga una differenza persistente in un indicatore tecnico rispetto al valore previsto dagli accordi interni o esterni, l'Autorità, salvo quanto previsto dall'art. 5, comma 1, adotta i necessari provvedimenti al fine di assicurare la parità di trattamento.*
7. *L'operatore notificato presenta sotto la propria responsabilità, a partire dal 30 giugno 2003, una relazione annuale certificata da un soggetto terzo che comprovi la separazione tra sistemi informativi delle funzioni di rete e delle funzioni commerciali. Tale relazione indica inoltre quali misure siano adottate per impedire l'utilizzo dei dati riservati relativi alla clientela degli OLO, in possesso delle funzioni di rete, da parte delle divisioni commerciali dell'operatore notificato."*

2.1.2 L'evoluzione della norma: ulteriori delibere AGCOM

Nel corso degli anni l'AGCOM ha emesso ulteriori delibere che hanno confermato sostanzialmente quanto disposto dalla 152/02/CONS, ne hanno ulteriormente definito l'ambito e le modalità di applicazione.

Di particolare rilevanza le seguenti delibere, già acquisite nelle certificazioni tecniche svolte negli anni precedenti:

- ▶ la delibera n. 274/07/CONS (art. 4, comma 2) prevede che la procedura di trasmissione delle richieste di attivazione di un servizio di accesso, dalla direzione rete a quella commerciale, venga inclusa nella relazione annuale di cui all'art. 2 comma 7 della delibera 152/02/CONS.
- ▶ la delibera n. 718/08/CONS, che "[...] mira ad integrare e rafforzare le disposizioni della delibera 152/02/CONS in materia di parità di trattamento",

inoltre, nel corso del 2009, successivamente alla conclusione dell'attività di certificazione, l'AGCOM ha inoltre emesso le seguenti delibere che richiamano per alcuni aspetti la 152/02/CONS:

- ▶ la delibera n. 52/09/CIR (art. 2 comma 10) prevede che l'accesso da parte del personale di Telecom Italia ai sistemi informativi preposti alla verifica del codice segreto sia protetto mediante l'adozione delle misure di riservatezza di cui alla delibera 152/02/CONS.

- la delibera n. 731/09/CONS richiama gli "obblighi di trasparenza" (art.6 comma 2), gli "obblighi di non discriminazione" (art.7) e il "principio di separazione amministrativa" (art. 7 comma 6) introdotti con la delibera 152/02/CONS.
- la delibera n. 2/10/CONS, oltre a richiamare gli "obblighi di trasparenza" e gli "obblighi di non discriminazione" imposti a Telecom Italia in qualità di operatore avente significativo potere di mercato nel mercato rilevante, descrive le condizioni attuative degli obblighi imposti. In particolare l'articolo 16 richiede esplicitamente la produzione di una relazione certificata da soggetto terzo in merito alle misure adottate per garantire il rispetto del principio di separazione amministrativa introdotto con la delibera 152/02/CONS.

2.2 Le attività di adeguamento messe in atto da Telecom Italia

A partire dal 2002, per dare attuazione a quanto richiesto dall'art. 2 della delibera 152/02/CONS, Telecom ha individuato e comunicato all'Autorità per le Garanzie nelle Telecomunicazioni (AGCOM) le misure da introdurre e una metodologia per verificarle.

Dal giugno 2003, in ottemperanza al comma 7 dell'art. 2 della delibera, Telecom presenta inoltre all'Autorità *"una relazione annuale certificata da un soggetto terzo che comprovi la separazione tra sistemi informativi delle funzioni di rete e delle funzioni commerciali. Tale relazione indica inoltre quali misure siano adottate per impedire l'utilizzo dei dati riservati relativi alla clientela degli OLO, in possesso delle funzioni di rete, da parte delle divisioni commerciali dell'operatore notificato"*.

In questa sezione vengono sinteticamente riassunte le misure adottate da Telecom Italia per ottemperare alle richieste della delibera 152/02/CONS, ed in particolare descrivono l'attività di certificazione tecnica annuale da essa richiesta.

2.2.1 Le misure adottate

L'art. 2 della delibera prevede che Telecom Italia disponga la separazione dei sistemi informativi (*"separazione tra sistemi informativi delle funzioni di rete e delle funzioni commerciali"*) e che si doti di apposite misure di riservatezza (*"misure per impedire l'utilizzo dei dati riservati relativi alla clientela degli OLO, in possesso delle funzioni di rete, da parte delle divisioni commerciali"*).

Tali richieste sono state indirizzate da Telecom adottando i principi e le modalità brevemente descritte qui di seguito.

2.2.1.1 Separazione dei sistemi informativi

Per quanto attiene alla separazione dei sistemi informativi, essa viene attuata adottando i seguenti principi:

Riferimento: TWA152/10-RP	Versione: NA	Data Creazione: 22/06/2010
PUBBLICO		Pagina 9 di 28

► **Separazione fisica:**

- il sistema informativo che contiene dati riservati dell'OLO e/o della sua clientela non è acceduto da personale dell'area Commerciale retail;
- il sistema informativo acceduto da personale dell'area Commerciale retail non contiene dati riservati dell'OLO e/o della sua clientela.

► **Separazione logica:**

- il sistema informativo che contiene dati riservati dell'OLO e/o della sua clientela è acceduto da personale dell'area Commerciale retail attraverso profili di accesso che non consentono la visualizzazione e/o gestione dei suddetti dati riservati;
- l'accesso ai dati riservati dell'OLO e/o della sua clientela da parte di personale dell'area Commerciale retail è ammesso per la sola gestione di specifici eventi di business preventivamente censiti ed autorizzati.

2.2.1.2 Misure di riservatezza

Per quanto attiene alle misure di riservatezza, esse vengono attuate adottando i seguenti principi:

► **Misure di riservatezza sui sistemi informativi:**

- Controllo delle abilitazioni per accesso utente e accesso diretto;
- Impiego di informative all'accesso a sistemi che contengono dati riservati dell'OLO e/o della sua clientela e labeling della reportistica prodotta dal sistema stesso;
- Regole a protezione delle postazioni utente con accesso a sistemi contenenti dati riservati dell'OLO e/o sua clientela.

► **Misure di riservatezza non sui sistemi informativi (legali, organizzative):**

- Codice di Comportamento per il rispetto della riservatezza;
- Gruppo di Lavoro permanente – adempimenti delibera 152/02/CONS;
- Classificazione delle informazioni riservate dell'OLO e/o della sua clientela e relativa gestione;
- Clausole contrattuali per Terze Parti ed Outsourcers;
- Formazione a tutto il personale interessato dai temi della delibera

2.2.2 La certificazione tecnica

Riferimento: TWA152/10-RP	Versione: NA	Data Creazione: 22/06/2010
PUBBLICO		Pagina 10 di 28

Obiettivo della certificazione tecnica è verificare la correttezza e la congruità della relazione con la quale Telecom Italia, secondo quanto disposto dalla delibera 152/02/CONS, comunica ad AGCOM che:

- ▶ le misure di sicurezza adottate sui propri sistemi relativamente all'ambito di rete fissa, già comunicate ad AGCOM nella relazione relativa all'anno precedente, siano state mantenute nel tempo;
- ▶ sui nuovi sistemi che contengono dati riservati OLO, entrati in esercizio successivamente alla precedente relazione, siano state attuate tutte le misure di sicurezza attese;
- ▶ siano state messe in atto azioni "non sui sistemi" atte a garantire il continuo presidio delle raccomandazioni di cui alla delibera 152/02/CONS.

La certificazione tecnica, pertanto, deve valutare:

- ▶ i criteri secondo cui Telecom Italia autorizza e controlla l'accesso ai sistemi informativi contenenti dati riservati relativi all'OLO e/o sua clientela;
- ▶ la rispondenza di tali criteri con quanto disposto dalla delibera 152/02/CONS;
- ▶ l'attuazione di misure e procedure idonee ad assicurare il continuo rispetto di tali criteri.

3. L'ATTIVITÀ DI CERTIFICAZIONE TECNICA

Questo capitolo descrive nel dettaglio il processo messo a punto per lo svolgimento dell'attività di certificazione descrivendo la metodologia adottata ed identificando gli elementi che la costituiscono, le azioni da essa previste e le modalità definite per la conduzione dell'attività.

3.1 La metodologia

La metodologia che Telecom si è data sin dal 2002, ispirata ai principi della norma BS7799 (successivamente divenuta ISO17799 / ISO27001), definisce gli elementi di base della Certificazione tecnica e stabilisce le misure che i sistemi informativi devono attuare in ottemperanza ai principi stabiliti dalla Delibera 152/02/CONS, articolo 2, comma 7.

Nell'ambito di tale metodologia sono state poste le seguenti definizioni:

- ▶ **Asset da proteggere:** "insieme dei dati relativi alla clientela dell'OLO" da proteggere contro la possibilità di utilizzo in contrasto con le raccomandazioni della delibera 152/02/CONS;
- ▶ **Area d'Indagine:** il perimetro, costituito da *sistemi e funzioni utente*, entro il quale devono essere applicate e rispettate le misure di riservatezza. In particolare, *L'Area d'Indagine* è composta dai sistemi informativi che contengono dati dell'Asset da proteggere, e dagli utenti che hanno necessità di utilizzo e/o visibilità dei dati riservati, presenti in tali sistemi, per lo svolgimento delle proprie mansioni operative.
- ▶ **Categorie dei sistemi:** classificazione dei sistemi dell'Area d'Indagine in categorie omogenee per area di appartenenza (area Retail, area Wholesale o area Rete), modalità di utilizzo (dedicato o condiviso tra aree di appartenenza) e caratteristica del sistema (es. datawarehouse).
- ▶ **Misure di riservatezza:** insieme delle azioni (misure tecniche di riservatezza) mirate alla prevenzione della diffusione non autorizzata, nei confronti delle divisioni dell'area Commerciale retail, dei dati riservati dell'Asset. In particolare, sono considerate 4 classi di misure di sicurezza, a protezione della riservatezza dei dati dell'OLO e/o sua clientela, nei confronti delle divisioni dell'area Commerciale retail di TI:
 - ▶ Policy e procedure per il rispetto della riservatezza;
 - ▶ Classificazione delle informazioni;
 - ▶ Controllo degli accessi ai dati dell'Asset;
 - ▶ Protezione dell'accesso alle postazioni utente.

3.2 L'ambito d'intervento

Riferimento: TWA152/10-RP	Versione: NA	Data Creazione: 22/06/2010
PUBBLICO		Pagina 12 di 28

L'ambito d'intervento della certificazione tecnica si compone dei seguenti elementi:

- ▶ Funzioni aziendali coinvolte
- ▶ GdL permanente adempimenti delibera 152/02/CONS
- ▶ Area indagine Funzioni
- ▶ Area indagine Sistemi
- ▶ Policy e linee guida
- ▶ Procedure aggiuntive e requisiti
- ▶ Procedure operative

3.3 La modalità d'indagine

L'attività di certificazione tecnica fa uso, per l'acquisizione delle informazioni e delle evidenze necessarie, degli strumenti d'indagine descritti nella seguente tabella.

STRUMENTO	FINALITÀ
Interviste ai Responsabili di Funzione	Acquisire informazioni relative all'utilizzo dei dati dell'OLO e/o della sua clientela e all'applicazione delle relative policy e procedure da parte del personale della Funzione
Questionari ai Responsabili dei sistemi già presenti nella certificazione 2009	Confermare e aggiornare informazioni relative rispettivamente ai sistemi già in esercizio durante la precedente certificazione e a quelli entrati in esercizio successivamente ad essa
Interviste ai Responsabili dei sistemi non presenti nella certificazione 2009	
Sonde a campione (funzioni utente)	Analizzare i tracciamenti delle abilitazioni, verificare le modalità di accesso ai dati dell'OLO e/o della sua clientela, verificare l'applicazione delle procedure di riferimento per il sistema, rispettivamente per gli Utenti e gli Addetti IT
Sonde a campione (funzioni addetti IT)	
Site visit	Verificare l'attuazione sul territorio degli adempimenti in riferimento a policy, procedure, utilizzo dei sistemi contenenti dati dell'OLO e/o della sua clientela

3.4 Il risultato atteso sui sistemi

Il risultato atteso al termine della certificazione è che tutti i sistemi siano conformi alle misure precedentemente descritte.

Tale risultato può essere sinteticamente descritto con la tabella seguente, che riporta analiticamente per ciascuna classe di sistemi censiti i risultati attesi in termini di rispetto della presenza ed efficacia delle misure di riservatezza stabilite.

In tale tabella col simbolo '√' sono indicate le misure attese, mentre con '-' quelle non applicabili.

CATEGORIA SISTEMI	MISURE ATTESE							
	Profilatura per livello di accesso	Procedura di abilitazione degli accessi	Procedura di esercizio	Tracciamento statico degli accessi	Tracciamento dinamico degli accessi	Tracciamento dinamico delle attività	Classificazione delle informazioni	Procedura Accesso Diretto
Sistemi condivisi Retail	Completo Parziale Nullo	√	√	√	√	√	√	√
Sistemi dedicati Retail	Nullo	-	√	-	-	-	-	√
Sistemi Frodi, Info12 ed Integrity Billing	Completo Nullo	√	√	√	√	-	√	√
Sistemi di datawarehouse Retail	Nullo	-	√	-	-	-	-	√
Sistemi dedicati Wholesale	Completo	√	√	√	√	-	√	√
Sistemi di datawarehouse Rete	Completo Nullo	√	√	√	√	-	√	√
Sistemi di Rete	Completo Nullo	√	√	√	√	-	√	√
Sistemi tecnici di Rete	Completo Nullo	√	√	√	-	-	√	√

Profilatura per i livelli di accesso:

- ▶ **Completo:** non vi sono restrizioni nell'accesso ai dati riservati;
- ▶ **Parziale:** è consentita la visualizzazione dei dati riservati dell'OLO solo per l'elaborazione di eventi gestionali retail censiti ed autorizzati;
- ▶ **Nulla:** non è consentito alcun accesso ai dati dell'Asset.

4. LA CERTIFICAZIONE TECNICA 2010

La certificazione tecnica per l'anno 2010 è stata svolta da Capgemini Italia, risultata aggiudicataria della gara predisposta da Telecom all'inizio del 2010 per l'individuazione sul mercato del *soggetto terzo* cui affidare la certificazione stessa. L'attività si è svolta fra i mesi di aprile e giugno ed è stata effettuata secondo le modalità descritte nel presente capitolo.

Al fine di mantenere la continuità logica ed operativa con le analoghe attività svolte negli anni precedenti a cura di altri Certificatori, così da minimizzare gli impatti sui processi e sulle strutture oggetto di certificazione, ed al fine di mantenere la consistenza della documentazione e la ripetibilità degli atti rispetto alle precedenti certificazioni, l'attività di certificazione tecnica per il 2010 è stata effettuata utilizzando la medesima metodologia, la stessa nomenclatura, le stesse convenzioni e gli stessi modelli cartacei predisposti da Telecom per le passate certificazioni, ed in particolare per quella relativa all'anno 2009.

4.1 Funzioni aziendali interessate

Stante la profonda riorganizzazione che ha interessato le strutture di Telecom Italia rispetto alla situazione dell'anno precedente, la quale inoltre ha comportato ulteriori cambiamenti previsti ed avvenuti durante il periodo di svolgimento della certificazione, l'ambito d'intervento è stato tracciato tenendo in considerazione il modello organizzativo consolidato alla data dell'8 aprile 2010 convenzionalmente assunta come inizio formale delle attività.

Al fine di mantenere la consistenza nella nomenclatura nei confronti delle precedenti relazioni e dello stesso disposto della delibera 152/02/CONS, sono state adottate le seguenti convenzioni:

- ▶ con **area Rete** si intende la direzione *Technology & Operations* articolata in:
 - ▶ Open Access;
 - ▶ Network;
 - ▶ Information Technology;
- ▶ con **area Wholesale** si intende la direzione *National Wholesale Services*;
- ▶ con **area Commerciale Retail** si indica la direzione *Domestic Market Operations* articolata in:
 - ▶ Consumer;
 - ▶ Business;
 - ▶ Top Clients;
 - ▶ Public Sector;

» Customer Operations;

» con **area Corporate** si indica l'insieme delle seguenti funzioni:

- » TI Audit and Compliance Services;
- » Equivalence & Regulatory Affairs;
- » Domestic Legal Affairs;
- » Human Resources & Organization;
- » Purchasing.

4.2 Piano delle attività

Seguendo la metodologia adottata per le precedenti certificazioni, anche le attività relative al processo di certificazione tecnica 2010 sono state organizzate lungo un articolato percorso progettuale suddiviso in tre macro-fasi, ciascuna delle quali a sua volta strutturata per comprendere diverse specifiche attività operative.

La Figura 1 qui sotto illustra la struttura organizzativa e temporale del processo adottato, nonché la relazione tra le varie fasi del progetto di certificazione.

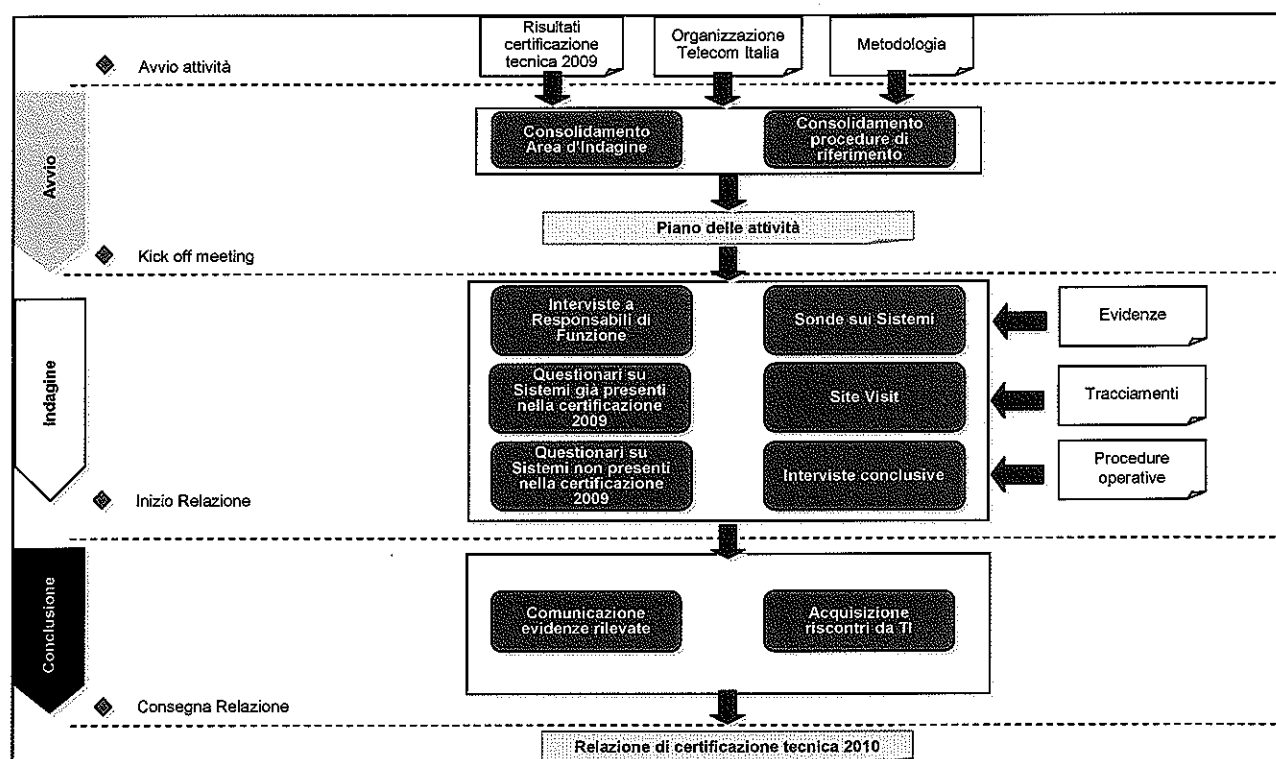


Figura 1: Le macrofasi del progetto di certificazione tecnica 2010

Riferimento: TWA152/10-RP	Versione: NA	Data Creazione: 22/06/2010
PUBBLICO		Pagina 17 di 28

La prima fase del progetto è stata quella di Avvio. In tale fase, di natura conoscitiva e preparatoria alle successive, il Gruppo di Lavoro ha acquisito formalmente la metodologia adottata da Telecom ed i risultati della certificazione tecnica 2009, nonché la nuova organizzazione 2010 di Telecom. Sulla base di queste informazioni ha consolidato l'Area di indagine e le procedure di riferimento, predisponendo quindi il piano di dettaglio delle attività relative alle fasi di indagine vera e propria.

In particolare durante questa fase sono state effettuate:

- ▶ l'acquisizione e l'analisi delle indicazioni della certificazione tecnica 2009;
- ▶ l'acquisizione e l'analisi della nuova struttura organizzativa di Telecom Italia;
- ▶ la definizione dell'area di indagine 2010 attraverso:
 - ▶▶ il censimento dei sistemi contenenti dati dell'OLO e/o sua clientela;
 - ▶▶ il censimento delle funzioni aziendali che hanno necessità di utilizzo/visibilità di tali dati.
- ▶ il censimento dell'elenco delle procedure (policy e linee guida) di riferimento per l'esecuzione delle attività di indagine;
- ▶ la definizione del piano delle attività d'indagine.

Il progetto di certificazione 2010 è stato formalmente presentato ai referenti aziendali coinvolti nelle attività mediante un'apposita riunione di kick-off tenutasi il 12 aprile. Nel corso di tale riunione, che ha segnato di fatto l'avvio della seconda fase operativa del progetto, oltre all'Ambito di riferimento è stato illustrato anche il piano di dettaglio delle successive attività di indagine, concordando con i referenti il calendario dei relativi incontri.

La seconda fase del progetto è stata quella di indagine vera e propria, avente come scopo la conduzione di attività finalizzate a raccogliere le informazioni necessarie alla produzione della certificazione tecnica. Durante tale fase il Gruppo di Lavoro ha raccolto gli elementi informativi e documentali necessari al fine di consolidare la conoscenza dei sistemi oggetto di indagine tecnica. In questa fase, oltre alle necessarie acquisizioni documentali (evidenze, tracciamenti, ...), si sono svolte le interviste ai responsabili di funzione e di sistema, le sonde a campione per funzioni utente e funzioni addetti IT, le site visit.

In particolare durante questa fase sono state effettuate:

- ▶ le interviste ai responsabili delle funzioni aziendali coinvolte nell'utilizzo/trattamento dei dati dell'OLO e/o sua clientela;
- ▶ le interviste ai responsabili dei sistemi contenenti dati dell'OLO e/o sua clientela;
- ▶ le sonde su un campione di sistemi appartenenti all'area di indagine nelle modalità:
 - ▶▶ accesso utente;
 - ▶▶ accesso addetto IT (diretto).
- ▶ le verifiche a campione sul territorio mediante site visit alle strutture coinvolte nella gestione dei dati dell'OLO e/o sua clientela.

La terza fase è stata quella di Conclusioni, nella quale si sono svolte l'analisi ed il consolidamento delle informazioni acquisite ed è stata prodotta la relazione finale. Durante tale fase il Gruppo di Lavoro ha svolto tutte le necessarie analisi incrociate di congruenza e consistenza sulle informazioni documentali e sulle evidenze raccolte durante le sonde e le site visit, chiedendo specifici chiarimenti e/o approfondimenti a Telecom laddove necessario, e raccogliendo i relativi riscontri. Sulla base di tali analisi è stata infine redatta la relazione finale.

4.3 Dettaglio delle attività svolte

Le indagini svolte nell'ambito delle attività di certificazione hanno riguardato:

- ▶ sistemi Telecom Italia che contengono dati dell'OLO e/o sua clientela;
- ▶ funzioni aziendali che hanno necessità di gestire dati riservati dell'OLO e/o sua clientela;
- ▶ funzioni aziendali che non devono avere accesso ai dati riservati dell'OLO e/o sua clientela.

Nel corso dell'attività sono state svolte:

- ▶ 28 interviste a responsabili di funzione, di cui:
 - ▶▶ 19 dell'area Commerciale retail;
 - ▶▶ 5 dell'area Rete;
 - ▶▶ 4 dell'area Wholesale.
- ▶ 6 interviste a responsabili di sistema (relativamente ai sistemi di nuova introduzione nel perimetro 2010);
- ▶ 48 sonde a campione, di cui:
 - ▶▶ 34 sonde su accessi utente;
 - ▶▶ 14 sonde su accessi addetti IT.
- ▶ 9 site visit;
- ▶ 2 interviste conclusive con:
 - ▶▶ Technology & Operations – Information Technology;
 - ▶▶ Equivalence and Regulatory Affairs – Regolamentazione Nazionale.

Sono stati altresì acquisiti ed analizzati:

- ▶ 71 questionari a sistema, di cui:
 - ▶▶ 65 relativi a sistemi già presenti nel perimetro 2009;
 - ▶▶ 6 relativi a sistemi di nuova introduzione nel perimetro 2010.
- ▶ 2 codici di comportamento;
- ▶ 6 policy e linee guida;
- ▶ 3 procedure aggiuntive e requisiti;
- ▶ 103 schemi dei profili e procedure operative di accesso ai sistemi, di cui:
 - ▶▶ 79 schemi profili di IDM;
 - ▶▶ 16 schemi profili di TSSC;
 - ▶▶ 8 procedure operative.
- ▶ circa 250 file contenenti evidenze di processi autorizzativi e verifiche periodiche;
- ▶ circa 250 file di tracciamenti statici e dinamici;
- ▶ circa 98.000 record di tracciamento, di cui:
 - ▶▶ 93.000 tracciamenti utente;
 - ▶▶ 5.000 tracciamenti addetti IT.

Nel corso delle sonde sono state coinvolte 84 utenze attive (utenti e addetti IT) e raccolte circa 850 schermate dei sistemi.

Nell'ambito delle verifiche effettuate sugli accessi ai sistemi è stato svolto un approfondimento su 2.684 tracciamenti e 522 utenze.

Tali attività hanno consentito di:

- ▶ consolidare l'Area di indagine 2010 costituita dai sistemi che contengono dati riservati dell'OLO e/o sua clientela;

- ▶ verificare che per i sistemi già oggetto della certificazione tecnica 2009 le misure di sicurezza siano state mantenute;
- ▶ verificare che per i nuovi sistemi le misure di sicurezza siano state introdotte.

Al termine dell'attività lo stato dei sistemi è stato formalizzato in termini di misure attese (come definite dalla metodologia) e misure effettivamente riscontrate.

5. ESITI DELL'ATTIVITÀ

In questo capitolo sono riportati gli esiti puntuali delle attività di verifica svolte nell'ambito della certificazione tecnica per l'anno 2010, in termini di misure riscontrate e risultati ottenuti.

5.1 Verifiche sui sistemi oggetto d'indagine

Le indagini condotte sui sistemi Telecom Italia hanno consentito di verificare l'effettiva separazione tra i sistemi delle aree Rete e Wholesale rispetto a quelli dell'area Commerciale retail; tale separazione è realizzata mediante la *separazione fisica* tra i sistemi o la *separazione logica* dei dati gestiti.

In particolare:

- ▶ il personale dell'area Wholesale utilizza, per la commercializzazione e la fatturazione dei servizi OLO, propri sistemi informativi cui il personale Retail non accede;
- ▶ il personale dell'area Commerciale retail che utilizza sistemi di Rete non accede ai dati riservati dell'OLO e/o sua clientela;
- ▶ la movimentazione dei servizi telefonici su linea Cliente Telecom Italia è realizzata attraverso l'emissione di ordinativi di lavoro sui sistemi dell'area Commerciale retail predisposti alla gestione del Cliente finale. Il provisioning dei servizi OLO che interessano la linea telefonica del Cliente finale Telecom Italia (CPS, ULL, VULL, WLR e NP, ...) coinvolge anche i suddetti sistemi;
- ▶ la gestione di alcuni eventi retail riguardanti il Cliente Finale Telecom Italia rende in taluni casi necessario l'accesso alla consistenza completa dei servizi attivi sulla linea del Cliente, che può includere anche dati riservati dell'OLO e/o sua clientela:
 - ▶▶ l'accesso a tali dati riservati, nei sistemi dell'area Commerciale retail, è consentito solo per la gestione di *eventi censiti ed autorizzati*, e solo da parte di personale Commerciale retail che ricopre uno specifico ruolo (ad esempio *"supervisore autorizzato"*);
 - ▶▶ tale personale autorizzato, al pari di tutto il rimanente personale Telecom Italia, è tenuto al rispetto di quanto stabilito dal "Codice di comportamento" e, nel caso specifico del *"supervisore autorizzato"*, da un'apposita procedura operativa che regola il *"trattamento dei dati riservati dell'OLO da parte del personale autorizzato di Customer Operations"*;
 - ▶▶ gli *eventi censiti ed autorizzati* che richiedono la visualizzazione dei dati riservati dell'OLO e/o sua clientela si riferiscono alle attività di:

- gestione reclamo;
- gestione prodotti su linea ceduta ad altro Operatore;
- scorporo fattura;
- gestione frodi;
- integrity billing.

- le attività del personale che dispone di accesso ai dati riservati dell'OLO e/o sua clientela sono regolate da apposite policy e linee guida, e/o procedure aggiuntive.

5.2 Verifiche sulle azioni "non sui sistemi"

Oltre alle verifiche puntuali sui sistemi, le attività d'indagine hanno compreso anche alcuni accertamenti su azioni "non sui sistemi" con l'obiettivo di verificare la presenza di adeguate misure comportamentali ed organizzative a supporto delle iniziative di rispetto del mandato della direttiva 152/02/CONS.

5.2.1 Diffusione del codice di comportamento

Sono previste (entro il 30 giugno 2010) la nuova diffusione via posta elettronica del codice comportamentale previsto dalla delibera 152/02/CONS e la contestuale diffusione del codice di comportamento conseguente agli impegni assunti da TI ed approvati con la delibera 718/08/CONS.

Entrambi i codici saranno resi disponibili a tutti i dipendenti sul portale intranet, in una specifica sezione che si chiamerà "*Parità di trattamento: i codici comportamentali*".

Nel corso dell'ultimo anno non è stata erogata formazione specifica relativamente ai temi della delibera 152/02/CONS essendo stata svolta in modo massivo lo scorso anno interessando circa 40.000 risorse.

5.2.2 Copertura delle clausole contrattuali

È stata praticamente ultimata l'integrazione, nei contratti già in essere e nei nuovi contratti con società terze interessate dalla tematica della delibera 152/02/CONS, dell'apposita clausola contrattuale a tutela della riservatezza dei dati degli OLO.

In particolare la verifica sui 491 contratti in essere ha riscontrato solo due eccezioni, per le quali è in corso la relativa integrazione contrattuale.

Riferimento: TWA152/10-RP	Versione: NA	Data Creazione: 22/06/2010
PUBBLICO		Pagina 23 di 28

5.2.3 Gestione e controllo automatizzato delle abilitazione delle utenze

È proseguita, così come negli anni precedenti, l'integrazione dei sistemi dell'area di indagine con sistemi automatici di gestione delle abilitazioni all'accesso.

In particolare, per quanto riguarda la gestione ed il controllo automatizzati delle abilitazioni all'accesso degli utenti:

- ▶ dei 55 sistemi gestiti da Technology, 54 (il 98%) risultano integrati con sistemi automatici;
- ▶ dei 10 sistemi gestiti a livello dipartimentale, 3 (il 33%) risultano integrati con sistemi automatici mentre per i rimanenti 7 è utilizzato un workflow autorizzativo manuale;
- ▶ i restanti 6 sistemi non posseggono interfaccia utente e quindi non richiedono l'integrazione con sistemi automatici.

Per quanto riguarda invece la gestione ed il controllo automatizzati delle abilitazioni all'accesso degli addetti IT:

- ▶ dei 66 sistemi gestiti da Technology, tutti (il 100%) risultano integrati con sistemi automatici;
- ▶ dei rimanenti 5 sistemi, 2 (il 40%) sono integrati con un sistema automatico mentre per i rimanenti 3 è utilizzato un workflow autorizzativo manuale.

6. CONCLUSIONI DELLA CERTIFICAZIONE TECNICA

Questo capitolo riporta le valutazioni conclusive della certificazione tecnica 2010 come emergono dai risultati delle attività di indagine descritte in dettaglio nel capitolo precedente.

6.1 Valutazione dei sistemi oggetto d'indagine

Con riferimento ai principi espressi dalla delibera 152/02/CONS, articolo 2, comma 7, è stato riscontrato quanto segue:

- ▶ i sistemi informativi dell'area Commerciale retail sono separati da quelli dell'area Rete/Wholesale;
- ▶ i sistemi informativi dell'area Commerciale retail, contenenti dati riservati dell'OLO e/o sua clientela, posseggono misure di riservatezza che non consentono alle divisioni dell'area Commerciale retail l'utilizzo *non autorizzato* dei suddetti dati;
- ▶ i sistemi informativi dell'area Rete e Wholesale posseggono misure di riservatezza che non consentono alle divisioni dell'area Commerciale retail l'utilizzo dei dati riservati dell'OLO e/o sua clientela.

La tabella di sintesi riportata nella pagina seguente riassume, per ciascuna categoria dei sistemi oggetto d'indagine, le misure di riservatezza riscontrate e riporta l'esito finale dell'indagine compiuta.

In tale tabella i risultati delle verifiche sono rappresentati mediante le seguenti codifiche:

- ▶ '√': copertura completa della misura attesa;
- ▶ 'x': copertura non adeguata della misura;
- ▶ '-': misura non prevista e/o non richiesta nel contesto;

CATEGORIA SISTEMI	MISURE RILEVATE								Esito dell'indagine
	Profilatura per livello di accesso	Procedura di abilitazione degli accessi	Procedura di esercizio	Tracciamento statico degli accessi	Tracciamento dinamico degli accessi	Tracciamento dinamico delle attività	Classificazione delle informazioni	Procedura Accesso Diretto	
Sistemi condivisi Retail	Completo Parziale Nullo	√	√	√	√	√	√	√	OK
Sistemi dedicati Retail	Nullo	-	√	-	-	-	-	√	OK
Sistemi Frodi, Info12 ed Integrity Billing	Completo Nullo	√	√	√	√	-	√	√	OK
Sistemi di datawarehouse Retail	Nullo	-	√	-	-	-	-	√	OK
Sistemi dedicati Wholesale	Completo	√	√	√	√	-	√	√	OK
Sistemi di datawarehouse Rete	Completo Nullo	√	√	√	√	-	√	√	OK
Sistemi di Rete	Completo Nullo	√	√	√	√	-	√	√	OK
Sistemi tecnici di Rete	Completo Nullo	√	√	√	-	-	√	√	OK

6.2 Valutazione delle azioni “non sui sistemi”

Oltre alle azioni tecniche previste sui sistemi oggetto di indagine, Telecom Italia ha attuato una serie di ulteriori azioni “non sui sistemi” (organizzative, legali, di formazione) atte a garantire il

Riferimento: TWA152/10-RP	Versione: NA	Data Creazione: 22/06/2010
PUBBLICO		Pagina 26 di 28

continuo rispetto da parte del personale delle raccomandazioni della delibera 152/02/CONS, articolo 2, comma 7.

In particolare è stato riscontrato che:

- ▶ è prevista, e verrà effettuata entro il 30 giugno 2010, una nuova emissione via posta elettronica del Codice di comportamento previsto dalla delibera 152/02/CONS; assieme ad essa avverrà diffuso anche il codice di comportamento conseguente agli impegni assunti da TI ed approvati con la delibera 718/08/CONS. Ciò conferma la volontà di Telecom Italia di tutelare la confidenzialità dei dati riservati dell'OLO nei confronti del personale dell'area Commerciale retail, e rafforzare la responsabilizzazione di ogni dipendente verso il continuo rispetto della riservatezza dei dati dell'OLO e/o sua clientela e della parità di trattamento in generale;
- ▶ è stata ridefinita la composizione del "Gruppo di lavoro permanente – Adempimenti delibera 152" in coerenza con le variazioni nell'assetto organizzativo di Telecom Italia;
- ▶ è proseguita l'integrazione dei sistemi appartenenti all'area d'indagine con sistemi automatici di gestione delle abilitazioni all'accesso;
- ▶ è stata sostanzialmente completata l'integrazione, nei contratti già in essere e nei nuovi contratti con società terze interessate dalla tematica di cui alla delibera 152/02/CONS, dell'apposita clausola contrattuale a tutela della riservatezza dei dati dell'OLO.

È stata inoltre riscontrata, presso le strutture visitate, una diffusa conoscenza della problematica connessa alla gestione dei dati OLO ed una radicata sensibilità del personale nei confronti degli obblighi discendenti dalla delibera 152/02/CONS.

6.3 Valutazione conclusiva

Per quanto in precedenza dettagliatamente esposto, la conclusione sintetica dell'attività di certificazione tecnica è che:

- ▶ i sistemi appartenenti all'area d'indagine 2010 **posseggono le misure di riservatezza necessarie e sufficienti a garantire la parità di trattamento interna ed esterna** ai sensi della delibera 152/02/CONS, articolo 2, comma 7;
- ▶ sono state intraprese anche idonee misure "non sui sistemi" (organizzative, legali, di formazione) atte a garantire il presidio ed il continuo rispetto da parte del personale delle raccomandazioni della delibera 152/02/CONS, articolo 2, comma 7.

6.4 Suggerimenti e raccomandazioni

A conclusione dell'attività di certificazione tecnica 2010, ed in considerazione della sempre maggior importanza delle tematiche indirizzate dalle delibere AGCOM 152/02/CONS e 718/08/CONS, Capgemini desidera esporre a Telecom Italia alcune raccomandazioni riguardanti azioni che potrebbero essere utilmente intraprese al fine di proseguire nel processo di continuo miglioramento del livello di presidio sulle dette tematiche e/o sulle modalità di svolgimento della certificazione tecnica.

In particolare si raccomanda a Telecom di:

- ▶ valutare la possibilità di ingegnerizzare e razionalizzare l'attuale insieme dei processi di gestione degli adempimenti ex delibera 152/02/CONS costituendo un "sistema centralizzato di gestione" ad hoc basato sul modello di riferimento ISO 27001, che comporterebbe oltre ad una ed maggiore efficienza alla possibilità di automatizzare buona parte delle funzioni di gestione, la possibilità di spostare sul sistema stesso di gestione il focus delle verifiche amministrative e documentali, lasciando più ampio spazio alle attività di indagine sul campo (sonde, site visit);
- ▶ provvedere ad un aggiornamento/raffinamento delle attuali policy e procedure riguardanti la gestione dei dati riservati dell'OLO e/o sua clientela, con l'obiettivo di definire con maggiore puntualità le tipologie di estrazione dei dati (ad esempio: report, estrazione, screen dump, ...) e soprattutto indicare in modo maggiormente chiaro ed univoco le relative modalità di labeling, al fine di indirizzare il problema ricorrente costituito dalle estrazioni di dati nel formato nativo delle applicazioni client (ad esempio: Excel, Access, ...);
- ▶ avviare una maggiore integrazione tra i sistemi di work flow autorizzativi delle utenze e quelli di provisioning delle stesse, in modo da diminuire la possibilità di errore umano nell'attivazione delle utenze;
- ▶ effettuare con maggiore frequenza nel corso dell'anno le verifiche di congruità attuate mediante il sistema Catone il quale, pur essendo un utile strumento di controllo, consente tuttavia il solo rilevamento di potenziali anomalie già avvenute, pertanto maggiore è la frequenza di analisi minore è il rischio che esse possano verificarsi.

