Certificazione tecnica di Telecom Italia per l'anno 2011 (ex delibera AGCOM 152/02/CONS, art. 2 comma 7)

Relazione sintetica pubblicabile

Giugno 2011

ERNST & YOUNG
Quality In Everything We Do

Sommario

Descrizione dell'incarico

Ernst & Young ha ricevuto da Telecom Italia S.p.A. l'incarico, quale soggetto terzo, per la verifica dell'avvenuta separazione tra i sistemi informativi delle funzioni di rete e delle funzioni commerciali in ottemperanza al comma 7, art. 2 ex 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*".

La verifica richiesta ha pertanto l'obiettivo di comprovare la separazione tra sistemi informativi delle funzioni di rete e delle funzioni commerciali di Telecom Italia attraverso l'analisi, la valutazione e il test delle misure atte a impedire l'utilizzo di dati riservati, relativi alla clientela degli OLO, da parte delle funzioni commerciali di Telecom.

1 Scopo del documento

Il documento rappresenta la relazione conclusiva di sintesi dell'attività che Ernst & Young Financial Business Advisors S.p.A. (di seguito anche Ernst & Young), in qualità di "soggetto terzo", ha svolto nel corso dell'anno 2011 allo scopo di verificare la separazione tra i sistemi informativi delle funzioni di rete e delle funzioni commerciali di Telecom Italia, come richiesto dal 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 La struttura del documento

Allo scopo di fornire una visione strutturata e metodologicamente coerente dell'attività svolta e delle conclusioni raggiunte la presente relazione di sintesi è organizzata secondo il seguente percorso logico/espositivo:

- ***Capitolo 1*** **(Scopo del documento)**
- ***Capitolo 2*** **(Executive Summary):** riepiloga la metodologia applicata, le attività svolte e la valutazione conclusiva con riferimento a quanto richiesto dalla normativa;
- ***Capitolo 3*** **(Contesto di riferimento):** descrive il contesto regolamentare e organizzativo nel quale si colloca l'attività di certificazione tecnica;
- ***Capitolo 4*** **(La Metodologia di Telecom Italia per la certificazione):** riporta la metodologia che Telecom Italia ha adottato per la Certificazione tecnica;
- ***Capitolo 5*** **(La Certificazione tecnica 2011):** descrive il progetto di certificazione tecnica relativa all'anno 2011, illustrandone le caratteristiche, le modalità operative con cui è stato svolto, le attività che sono state effettuate;
- ***Capitolo 6*** **(Esiti delle attività):** riporta in dettaglio i risultati ottenuti;
- ***Capitolo 7*** **(Conclusioni della Certificazione tecnica):** riporta le valutazioni conclusive dell'attività di indagine;

2 Executive Summary

2.1 Il contesto di riferimento

L'AGCom, mediante Delibera 152/02/CONS, ha stabilito che l'operatore con significativo potere di mercato (SPM), e quindi Telecom Italia, debba garantire che:

- le unità organizzative preposte alla gestione della rete siano separate da quelle preposte alla vendita dei servizi finali;
- i sistemi informativi e gestionali relativi ai dati degli operatori alternativi siano gestiti da personale differente da quello preposto alle attività commerciali verso i clienti finali;
- i sistemi e le relative informazioni non siano accessibili al personale delle unità organizzative commerciali che forniscono servizi ai clienti finali, e che tale condizione sia assicurata tramite l'individuazione di apposite misure di sicurezza.

Telecom Italia, al fine di garantire la riservatezza dei dati gestiti e in attuazione del citato disposto normativo, dal 2002 ha individuato e implementato le misure sopra richieste. Tali misure sono verificate sulla base della specifica metodologia definita da Telecom: annualmente Telecom Italia presenta all'Autorità Garante delle Comunicazioni, in ottemperanza al disposto contenuto nel comma 7 dell'art. 2 della Delibera 152/02/CONS, "*una relazione annuale certificata da un soggetto terzo che comprovi la separazione tra sistemi informativi delle funzioni di rete e delle funzioni commerciali*".

La metodologia che Telecom Italia ha adottato, a partire dal 2002, e ispirata ai principi della norma BS7799 (successivamente divenuta ISO17799 / ISO27001 / ISO27002), definisce gli elementi di base della Certificazione tecnica e stabilisce le misure adottate in ottemperanza ai principi stabiliti dalla Delibera 152/02/CONS, articolo 2, comma 7.

Nell'ambito di tale metodologia si fa riferimento alle seguenti definizioni:

- ***Asset da proteggere***: "*insieme dei dati relativi alla clientela dell'OLO*"[1] da proteggere contro la possibilità di utilizzo in contrasto con le raccomandazioni della delibera 152/02/CONS;
- ***Area d'indagine***: perimetro, costituito da sistemi e funzioni utente, entro il quale devono essere applicate e rispettate le misure di riservatezza;
- ***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***[2]: 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.

[1] Estratto dalla Delibera 152/02/CONS art. 2, Comma 7.
[2] I principi di protezione indicati dalla ISO27002 sono: integrità, disponibilità e riservatezza. La Delibera indica come principio di protezione, sull'Asset definito, quello di riservatezza.

2.2 La certificazione 2011: tipologia di verifiche svolte

Obiettivo della certificazione tecnica è quello di verificare l'avvenuta "*separazione tra sistemi informativi delle funzioni di rete e delle funzioni commerciali*". Inoltre "*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*".

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.

La Certificazione tecnica valuta dunque i criteri secondo cui Telecom Italia autorizza e controlla l'accesso ai sistemi informativi contenenti dati riservati relativi all'OLO e/o della sua clientela, la loro rispondenza con le raccomandazioni di AGCOM contenute nella Delibera 152/02/CONS, articolo 2, comma 7, e l'attuazione di misure e procedure atte al continuo rispetto di tali criteri.

La certificazione tecnica 2011 è stata condotta seguendo la metodologia già adottata da Telecom Italia nelle precedenti certificazioni tecniche supportata, per l'esecuzione delle "sonde" sui sistemi dall'applicazione dei principali standard internazionali di riferimento in materia di sicurezza informatica (ISO27000) e di controllo IT (Cobit).

Le attività di certificazione hanno consentito di aggiornare l'Area d'Indagine 2011 composta da funzioni/sistemi relativi al mercato della telefonia fissa, in linea con il disposto della Delibera 152/02/CONS, articolo 2, comma 7.

In particolare, nell'ambito dell'Area d'Indagine, le attività di verifica svolte sono state le seguenti:

- interviste alle Funzioni aziendali (N°27);
- interviste ai responsabili di sistema (N°81);
- sonde a campione su 30 sistemi (campione rappresentativo dei sistemi appartenenti all'area d'indagine), di cui:
  - 30 sonde su accessi utente;
  - 12 sonde su accessi addetti IT;
- 9 site visit (campione rappresentativo delle strutture appartenenti all'area d'indagine).

Nell'ambito dell'attività di verifica sono stati, inoltre, analizzati:

- Il Codice di comportamento per la riservatezza dei dati relativi agli OLO e/o della sua clientela;
- Il Codice comportamentale derivante dagli impegni che TI ha assunto ed AGCOM ha approvato, con la Del 718/08/CONS;
- le 6 policy e linee guida che disciplinano le tematiche trattate dalla Delibera 152/02/CONS, Art. 2 comma 7;
- gli schemi dei profili/funzione e/o procedure di gestione degli accessi per tutti i sistemi appartenenti all'Area d'Indagine 2011;
- circa 60 file contenenti evidenze di processi autorizzativi e verifiche periodiche;

- circa 200 file contenenti i risultati dalle elaborazioni del sistema CATONE (sistema per l'analisi automatica dei.tracciamenti statici e dinamici);
- circa 90.000 record di tracciamento.

Inoltre nel corso delle "sonde" sono state coinvolte circa 70 utenze attive (utenti e addetti IT) e raccolte circa 500 schermate dei sistemi.

Nell'ambito delle verifiche è stato effettuato un controllo sulle abilitazioni e sulle verifiche periodiche per 844 utenze (288 Addetti IT e 556 Utenti).

2.3 Conclusioni

In base alle attività svolte riteniamo che Telecom Italia abbia adottato le misure di riservatezza, tecniche, organizzative e di sicurezza tali da garantire la parità di trattamento interna ed esterna ai fini della delibera 152/02/CONS, articolo 2 comma 7.

In particolare a valle di tutte le attività di certificazione tecnica eseguite per l'anno 2011 riportiamo le nostre conclusioni:

- ✓ i sistemi appartenenti all'area di indagine 2011 posseggono le misure di riservatezza necessarie e sufficiente a garantire la parità di trattamento interna ed esterna ai sensi della Delibera 152/02/CONS articolo 2, comma 7;

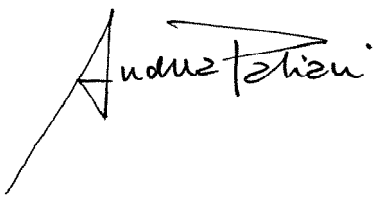
- ✓ sono state adottate idonee misure (cosiddette "non sui sistemi") atte a garantire il presidio e il continuo rispetto da parte del personale delle raccomandazioni previste dalla delibera 152/02/CONS, articolo 2, comma 7. A tal fine si è riscontrato, presso le strutture visitate, una piena consapevolezza degli obblighi in capo a Telecom Italia discendenti dalla delibera 152/02/CONS da parte del personale TI

Roma, 24 giugno 2011

ERNST&YOUNG FINANCIAL-BUSINESS ADVISORS S.P.A.

Andrea Paliani

(Socio)



3 Contesto di riferimento

3.1 Contesto regolamentare

Il principio della parità di trattamento e della non discriminazione è uno dei principi cardine della disciplina comunitaria nell'ambito della regolamentazione del settore delle Telecomunicazioni.

Al fine di assicurare il rispetto del principio di parità di trattamento e non discriminazione, l'Autorità ha l'obiettivo di garantire che l'operatore con significativo potere di mercato (di seguito SPM) non gestisca ed utilizzi informazioni e dati commerciali relativi agli operatori interconnessi per propri fini commerciali.

L'Autorità, mediante Delibera 152/02/CONS, ha stabilito che l'operatore SPM e quindi Telecom Italia, debba garantire che:

- le unità organizzative preposte alla gestione della rete siano sufficientemente separate da quelle preposte alla vendita dei servizi finali;
- i sistemi informativi e gestionali relativi ai dati degli operatori alternativi siano gestiti da personale differente da quello preposto alle attività commerciali verso i clienti finali;
- i sistemi e le relative informazioni non siano accessibili al personale delle unità organizzative commerciali che forniscono servizi ai clienti finali, tramite l'individuazione di apposite misure di sicurezza.

In particolare l'Autorità, con l'articolo 2, comma 7 della Delibera 152/02/CONS, stabilisce che:

- *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".*

La disposizione prevista in Delibera 152/02/CONS è tuttora valida in quanto è stata più volte confermata nel corso dell'emanazione delle delibere relative al nuovo quadro regolamentare definito a conclusione del secondo ciclo di analisi di mercato ed in particolare:

- Delibera n. 718/08/CONS;
- Delibera n. 731/09/CONS Art. 55, comma 8 - Art. 6 comma 2 - Art. 7 comma 6;
- Delibera n. 52/09/CIR Art. 2 comma 10;
- Delibera n. 179/10/CONS Art. 7 e Art. 15
- Delibera n. 180/10/CONS Art. 9 e Art. 16
- Delibera n. 2/10/CONS Art. 16.

3.2 Le misure di riservatezza adottate da Telecom Italia

Telecom Italia al fine di garantire la riservatezza dei dati gestiti e in attuazione di tale disposto, sin dal 2002 ha individuato e **implementato le misure** previste dal citato dettato normativo e ha **individuato una metodologia** per verificarle, al fine di presentare all'Autorità, in ottemperanza al comma 7 dell'art. 2 della Delibera 152/02/CONS, "una relazione annuale certificata da un soggetto terzo che comprovi la separazione tra sistemi informativi delle funzioni di rete e delle funzioni commerciali".

In particolare Telecom Italia ha adottato misure di riservatezza per garantire la ***separazione (fisica e logica) dei sistemi informativi*** delle funzioni di rete e delle funzioni commerciali e per impedire l'utilizzo dei dati della clientela degli OLO in possesso delle Funzioni di Rete e Wholesale da parte delle divisioni commerciali di Telecom Italia.

3.2.1 Separazione dei sistemi informativi

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

- **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.

3.2.2 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 (ove presente), procedure operative, procedure di esercizio e procedure di 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 organizzative**:
  - Codice di Comportamento per il rispetto della riservatezza dei dati riservati dell'OLO e/o sua clientela;
  - 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 152/02/CONS, articolo 2, comma.

4 La metodologia Telecom per la certificazione

4.1 La metodologia di verifica delle misure di sicurezza

La metodologia che Telecom Italia ha adottato a partire dal 2002, ispirata ai principi della norma BS7799 (successivamente divenuta ISO27001 / ISO27002), 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 si fa riferimento alle seguenti definizioni:

- ✓ **Asset da proteggere**: "*insieme dei dati relativi alla clientela dell'OLO*[3]" da proteggere contro la possibilità di utilizzo in contrasto con le raccomandazioni della delibera 152/02/CONS;
- ✓ **Area d'indagine**: il perimetro, costituito dai sistemi e funzioni utente, entro il quale devono essere applicate e rispettate le misure di riservatezza;
- ✓ **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**[4]: 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.

[3] Estratto dalla Delibera 152/02/CONS art. 2, Comma 7.
[4] I principi di protezione indicati dalla ISO27002 sono: integrità, disponibilità e riservatezza. La Delibera indica come principio di protezione, sull'Asset definito, quello di riservatezza.

4.1.1 Gli asset da proteggere

Al fine di assicurare la completezza e l'efficacia del lavoro di indagine e delle relative analisi/ interviste, i dati riservati dell'OLO e/o sua clientela che compongono l'Asset da proteggere sono stati censiti e "clusterizzati" nelle seguenti tipologie:

- ✓ Servizio OLO[5] associato a linea Cliente;
- ✓ Piani/Ordini di Lavoro relativi a servizi OLO (espletati o non espletati);
- ✓ Trouble Ticket di OLO su servizi erogati a sua Clientela;
- ✓ Cartellini di traffico (xDR) intergestore (voce e dati);
- ✓ Dati di fatturazione verso OLO;
- ✓ Contratti stipulati tra Telecom Italia (Funzione *National Wholesale Services*) ed OLO;
- ✓ Viste aggregate su dati riservati dell'OLO e/o sua Clientela in cui è presente l'indicazione OLO;
- ✓ Documentazione contenente dati riservati dell'OLO e/o sua clientela.

4.1.2 L'area di indagine

L'Area d'Indagine definisce il perimetro (sistemi e funzioni utente) entro il quale devono essere applicate e rispettate le misure di riservatezza.

L'Area d'Indagine è composta da:

- ✓ Sistemi informativi che contengono dati dell'Asset da proteggere;
- ✓ Utenti che hanno necessità di utilizzo/visibilità dei dati riservati dell'OLO e/o sua clientela, presenti in tali sistemi, per lo svolgimento delle proprie mansioni operative.

I driver per l'individuazione dei sistemi sono:

- ✓ I servizi OLO ed i relativi processi gestionali (es. processi di provisioning ed assurance);
- ✓ Le interfacce, dei sistemi individuati, verso altri sistemi o linee utente.

I driver per l'individuazione delle funzioni utente sono:

- ✓ I processi e le responsabilità di gestione dei servizi OLO;
- ✓ Gli eventi gestionali retail per i quali è necessario conoscere/intervenire sui dati dell'OLO e/o sua clientela.

4.1.3 Le categorie di sistema

L'analisi dei sistemi di Telecom Italia ha permesso l'identificazione delle seguenti categorie di sistemi:

- ✓ ***Sistemi Dedicati Retail***
  - o Sistemi appartenenti all'area Commerciale retail acceduti dal solo personale dell'area Commerciale retail
- ✓ ***Sistemi Condivisi Retail***

[5] Per Servizio OLO si intendono tutti i servizi che Telecom Italia come operatore notificato, offre agli OLO quali ad esempio: Carrier Preselection, Number Portability, ULL, Bitstream, WLR, Canale Virtuale Permanente, Servizi di traffico di interconnessione, etc.

- Sistemi appartenenti all'area Commerciale retail acceduti sia da personale dell'area Commerciale retail che da personale dell'area Rete/Wholesale

✓ ***Sistemi Frodi, Info12 ed Integrity Billing***
- Sistemi appartenenti all'area Commerciale retail ma che non sono a supporto diretto delle attività di commercializzazione e vendita servizi retail

✓ ***Sistemi di Datawarehouse Commerciali retail***
- Sistemi di Datawarehouse per l'area Commerciale retail

✓ ***Sistemi Dedicati Wholesale***
- Sistemi appartenenti all'area Wholesale e dedicati alle attività svolte dalla funzione National Wholesale Services

✓ ***Sistemi di Datawarehouse Rete***
- Sistemi di Datawarehouse per l'area Rete

✓ ***Sistemi di Rete***
- Sistemi appartenenti all'area Rete che dispongono dei dati riservati dell'OLO e/o sua clientela; tali sistemi dispongono di funzionalità di accesso ai dati riservati semplificato (interfaccia GUI e/o Web) e funzionalità utente di reporting ed estrazione dei suddetti dati riservati

✓ ***Sistemi Tecnici di Rete***
- Sistemi appartenenti all'area Rete ad uso del solo personale tecnico che non forniscono reportistica specifica sui dati dell'OLO e/o sua Clientela e non sono acceduti da personale dell'area Commerciale retail.

4.1.4 Le misure di riservatezza

Sono considerate 4 classi di misure di sicurezza a protezione della riservatezza dei dati riservati dell'OLO e/o sua clientela, nei confronti delle divisioni commerciali retail di Telecom Italia:

- Policy e procedure per il rispetto della riservatezza dei dati riservati dell'OLO e/o della sua clientela;
- Classificazione delle informazioni;
- Controllo degli accessi ai dati dell'Asset;
- Protezione dell'accesso al sistema operativo per le postazione utente.

4.1.4.1 Policy e procedure per il rispetto della riservatezza

Il rispetto della riservatezza dei dati riservati dell'OLO e/o sua clientela nei confronti delle divisioni dell'area Commerciale retail deve essere rafforzato da policy che forniscono chiare indicazioni e dimostrano supporto e ferma volontà, nel perseguimento degli obiettivi di riservatezza delle informazioni sensibili.

Le policy devono essere comunicate a tutta l'organizzazione in modo palese, accessibile e comprensibile per il personale cui sono rivolte. Devono essere previste sessioni specifiche di formazione per gli operatori di Customer Care 'supervisore autorizzato' e per tutto il personale delle funzioni delle aree Commerciale retail, Rete e Wholesale interessati alla tematica della Delibera 152/02/CONS.

Le policy devono vietare la diffusione non autorizzata delle informazioni riservate; devono inoltre indicare le azioni nei confronti dei trasgressori.

4.1.4.2 Classificazione delle informazioni

I dati riservati dell'OLO e/o della sua clientela sono riservati e classificabili come *Confidenziali* secondo quanto stabilito nelle linee guida comunicate dalla funzione corporate di Telecom Italia per la sicurezza sui sistemi informativi.

I sistemi contenenti dati riservati devono prevedere, ad ogni accesso con profilo abilitato a gestire e/o visualizzare dati riservati dell'OLO e/o della sua clientela, la presentazione di una nota informativa[6] sulla riservatezza dei dati contenuti nel sistema come reminder alla policy di Telecom Italia.

Inoltre tutte le comunicazioni e la documentazione che contengono i suddetti dati riservati, devono essere classificate come *Confidenziali*; i report riportare un'opportuna dicitura[7] che dichiari la riservatezza ai fini della Delibera 152/02/CONS.

Le modalità di trattamento sono quelle previste dalla normativa di sicurezza di Telecom Italia.

4.1.4.3 Controllo degli accessi ai dati dell'Asset

Per i sistemi appartenenti all'Area di Indagine, il livello di accesso ai dati dell'Asset deve essere coerente con le specifiche esigenze operative e con la funzione di appartenenza. Tale livello di accesso può essere:

- ✓ **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;
- ✓ **Nullo**: non è consentito alcun accesso ai dati dell'Asset.

Il livello di accesso si realizza attraverso:

- ✓ la configurazione a sistema di profili utente abilitati a funzionalità predefinite e l'assegnazione nominativa di tali profili;
- ✓ il tracciamento degli accessi e delle attività svolte
- ✓ le procedure che definiscono ruoli ed attività per l'attribuzione degli accessi.

[6] Si riporta la "*nota informativa*" di riferimento: "Attenzione: i dati contenuti nel sistema sono classificati Telecom Italia – Confidenziale e sono soggetti ai vincoli imposti dalla Delibera 152/02/CONS. Net trattare i dati l'operatore deve attenersi alle disposizioni contenute nel "Codice di Comportamento per la riservatezza de dati relativi alla clientela dell'OLO", nonché a tutte le normative di sicurezza vigenti in Azienda"

[7] Si riporta a seguite la dicitura di riferimento: "Telecom Italia – Confidenziale – informazioni soggette ai vincoli imposti dalla Delibera 152/02/CONS come da disposizioni contenute nel "Codice di Comportamento per la riservatezza dei dati relativi alla clientela dell'OLO"

Vengono di seguito rappresentati i livelli di accesso ed i requisiti per la realizzazione dello stesso:

Livello di accesso	Requisito di sistema			Requisito Organizzativo
	Profilo *ad hoc*	Tracciamento accesso	Tracciamento attività	Procedure
Completo		⊗		⊗
Parziale	⊗	⊗	⊗	⊗
Nullo	⊗			

Il livello di accesso ai sistemi informativi dell'area Rete/Wholesale

Per i sistemi informativi dell'area rete Rete/Wholesale si deve prevedere un livello di accesso **completo**, da assegnare al personale dell'area Rete/Wholesale che ne ha bisogno per lo svolgimento delle attività di propria competenza. Il personale delle divisioni dell'area commerciale retail non deve accedere ai dati riservati contenuti nei sistemi dell'area rete/wholesale.

Le misure da prevedere per il controllo degli accessi a tali sistemi sono:

- ✓ una procedura di abilitazione degli accessi. La procedura indica:
  - chi e come può richiedere l'autorizzazione o la revoca;
  - chi autorizza l'accesso a sistemi dell'area Rete/Wholesale;
  - chi espleta la richiesta e come comunica userid e password;
  - chi è responsabile di verificare periodicamente che la procedura sia rispettata mediante la verifica delle utenze abilitate;
  - a chi è stata diffusa la procedura;
- ✓ una procedura di esercizio;
- ✓ il registro delle abilitazioni all'accesso ai sistemi dell'area rete/wholesale;
- ✓ il tracciamento degli accessi ai sistemi dell'area rete/wholesale che consente di verificare che solo il personale autorizzato ha accesso ai dati dell'asset presenti i tali sistemi;
- ✓ una procedura di accesso diretto.

Il livello di accesso ai sistemi informativi dell'area Commerciale Retail

Per i sistemi informativi dell'area rete Commerciale Retail si deve prevedere tre livelli di accesso:

- ✓ ***Completo*** per il personale dell'area Rete/Wholesale che deve gestire ordinativi di lavoro relativi a Servizi OLO (es ULL, WLR, etc);
- ✓ ***Parziale*** per il personale commerciale retail autorizzato che deve gestire particolari e limitati eventi di business *censiti e autorizzati* la cui lavorazione, richiede, in taluni casi, la conoscenza della consistenza completa (che può includere anche dati riservati dell'OLO) dei servizi attivi sulla linea del Cliente stesso;
- ✓ ***Nullo*** per il personale retail non autorizzato.

Le misure da prevedere per il controllo degli accessi ai sistemi retail che contengono dati riservati dell'asset sono:

- ✓ Una procedura di abilitazione degli accessi. La procedura
  - chi e come può richiedere l'autorizzazione o la revoca;
  - chi autorizza l'accesso a sistemi dell'area Commerciale retail;
  - chi espleta la richiesta e come comunica userid e password;
  - chi è responsabile di verificare periodicamente che la procedura sia rispettata mediante la verifica delle utenze abilitate;
  - a chi è stata diffusa la procedura;
- ✓ una procedura di esercizio;
- ✓ il registro delle abilitazioni all'accesso ai sistemi informativi retail che contengono dati riservati dell'asset per i profili "completo" o "parziale";
- ✓ il tracciamento degli accessi ai dati riservati presenti nei sistemi retail che consente di verificare che il personale dell'area commerciale retail non autorizzato non acceda a dati riservati presenti in tali sistemi;
- ✓ il tracciamento dinamico delle attività per verificare che il personale dell'area commerciale retail autorizzato svolga unicamente le attività gestionali censite;
- ✓ una procedura di accesso diretto

La tabella successiva riporta le misure tecniche di riservatezza attese sui sistemi, per ciascuna delle categorie dei sistemi definite.

Misure Attese								
Categoria Sistemi	**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**
Dedicati Retail	Nullo	-	Y	-	-	-	-	Y
Condivisi Retail	Completo Parziale Nullo	Y	Y	Y	Y	Y	Y	Y
Frodi,Info 12, Integrity Billing	Completo Nullo	Y	Y	Y	Y	-	Y	Y
DWH Commerciali retail	-	-	-	-	-	-	-	-
DWH Rete	Completo Nullo	Y	Y	Y	Y	-	Y	Y
Rete	Completo Nullo	Y	Y	Y	Y	-	Y	Y
Tecnici di Rete	Completo Nullo	Y	Y	Y	-	-	Y	Y
Dedicati Wholesale	Completo	Y	Y	Y	Y	-	Y	Y

Legenda:

'Y' Misura attesa

'-' Misura non applicabile

4.1.4.4 Protezione dell'accesso al sistema operativo per le postazioni utente

Le misure di protezione dell'accesso per le postazioni utente risultano utili a ridurre i rischi legati ai terminali lasciati occasionalmente incustoditi e da cui si potrebbe accedere a dati riservati presenti sui sistemi. Il sistema operativo di ogni postazione su cui risiedono dati riservati dell'OLO e/o sua clientela deve essere protetto al logon.

L'accesso al sistema operativo deve prevedere l'esistenza di un account per ogni operatore autorizzato all'accesso ai dati riservati. Tale account di accesso deve essere strettamente personale. Gli operatori autorizzati all'accesso ai dati riservati devono obbligatoriamente utilizzare l'account personale assegnatogli per l'accesso al sistema operativo.

Inoltre l'inattività della postazione per più di x minuti (periodo predefinito di time-out) deve prevedere un logout dal sistema o, in alternativa, un meccanismo di blocco (lock) del terminale. In entrambi i casi un successivo accesso al sistema operativo deve essere subordinato alla fornitura delle credenziali utente (login e password).

4.2 L'ambito di intervento

L'ambito di 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, linee guida e procedure.

4.3 La modalità di indagine

La metodologia prevede l'impiego delle seguenti modalità operative, strumentali per l'acquisizione delle diverse tipologie di informazioni oggetto di verifica:

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
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 Verificare la conoscenza delle procedure operative e degli obblighi derivanti dalla normativa (consapevolezza) da parte del personale Telecom Italia .
Questionari relativi a sistemi già presenti nella certificazione 2010	Aggiornare e raccogliere informazioni relative rispettivamente ai sistemi già in esercizio durante la precedente certificazione e a quelli entrati in esercizio successivamente ad essa
Questionari relativi a sistemi non presenti nella certificazione 2010	
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)	

5 La certificazione tecnica 2011

La certificazione tecnica 2011 è stata condotta seguendo la metodologia adottata da Telecom Italia e già impiegata nelle precedenti certificazioni tecniche.

La metodologia Telecom è stata supportata dall'approccio strutturato e sistematico che Ernst & Young adotta nella gestione dei progetti volti alla verifica della conformità di processi e soluzioni IT rispetto alle normative di riferimento e dall'applicazione dei principali standard internazionali di riferimento in materia di sicurezza informatica **(ISO27000)** e di controllo IT **(Cobit).**

L'applicazione di tali framework permette di:

- verificare gli aspetti di governance dei sistemi informativi, che si rendono necessari per assicurare che le policy, le quali mirano a recepire i requisiti di compliance esterni (nello specifico i requisiti richiesti dalla delibera), siano declinate in specifiche procedure e norme operative;
- garantire che il sistema di controllo sia nel suo complesso governato e gestito secondo le principali "best practice" di riferimento, in particolare con riferimento agli ambiti di interesse per la delibera (classificazione dei dati, gestione e controllo degli accessi, protezione delle postazioni, ecc.).

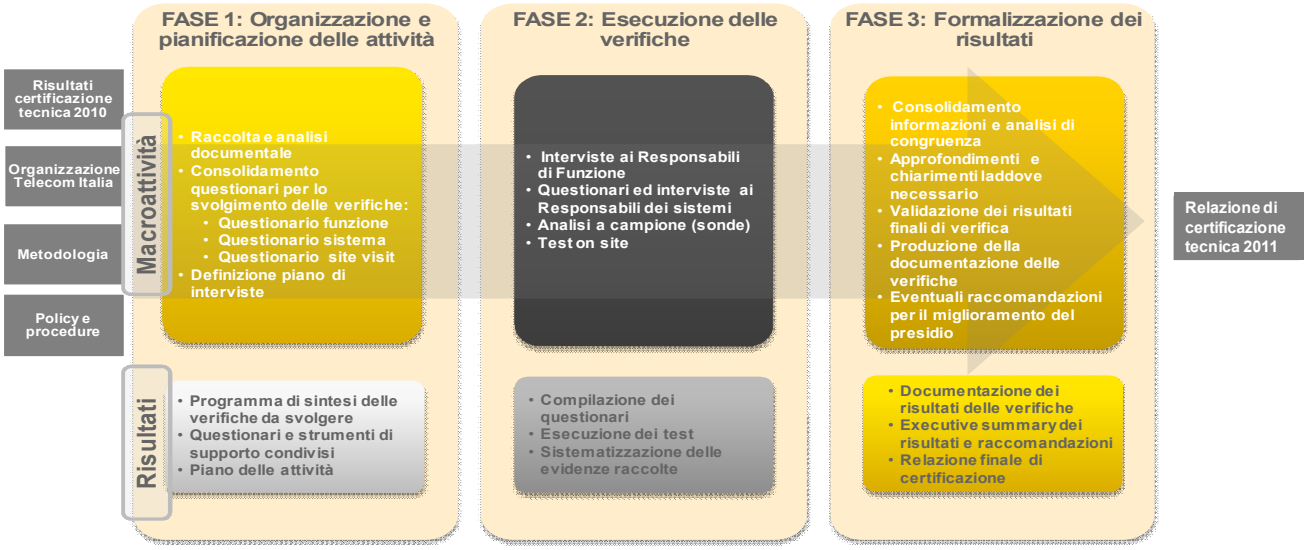
Al fine di avere completo accesso alle persone ed alle informazioni necessarie al progetto, il Gruppo di Lavoro E&Y ha interfacciato direttamente la struttura Equivalence & Regulatory Affairs – Regolamentazione Nazionale. Tale struttura, infatti, oltre a costituire il process owner dell'attività di certificazione tecnica, è inserita nell'organigramma a diretto riporto del Presidente e quindi in posizione di indipendenza rispetto alle strutture delle aree Commerciale Retail, Rete e Wholesale.

In particolare tutte le comunicazioni formali tra Telecom Italia e il Gruppo di Lavoro E&Y responsabile dell'attività di certificazione sono avvenute per il tramite della struttura stessa.

5.1 Piano delle attività

Il processo di certificazione tecnica 2011 è stato caratterizzato dalle seguenti fasi progettuali:

- ✓ **Fase 1**: organizzazione e pianificazione delle attività;
- ✓ **Fase 2**: esecuzione delle verifiche;
- ✓ **Fase 3**: formalizzazione dei risultati.



La prima fase del processo di verifica(*Organizzazione e pianificazione delle attività*) ha avuto come scopo la raccolta ed analisi del materiale propedeutico all'avvio delle attività di Certificazione tecnica 2011 con riferimento alla metodologia/linee guida definite.

In particolare sono state effettuate:

- ✓ L'analisi delle indicazioni della Certificazione tecnica 2010 e l'analisi della nuova struttura organizzativa di Telecom Italia;
- ✓ La definizione dell'Area di Indagine 2011 attraverso il censimento dei sistemi contenenti dati riservati dell'OLO e/o della sua clientela e delle funzioni aziendali che hanno necessità di utilizzo/visibilità di tali dati per lo svolgimento delle proprie mansioni operative e Funzioni aziendali che non devono avere accesso a 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 di dettaglio delle attività di indagine.

La seconda fase dell'attività di verifica (*esecuzione delle verifiche*) ha avuto come scopo la conduzione di attività, al fine di raccogliere le informazioni necessarie alla produzione della Certificazione tecnica. In particolare:

- ✓ Interviste ai responsabili delle funzioni aziendali coinvolte nell'utilizzo/trattamento di dati riservati dell'OLO e/o della sua clientela;
- ✓ Interviste ai responsabili dei sistemi contenenti dati riservati dell'OLO e/o della sua clientela;
- ✓ Sonde utente e/o addetti IT (accesso diretto) su un campione di sistemi appartenenti all'area di indagine;

- ✓ Verifiche a campione sul territorio mediante *site visit* alle strutture coinvolte nella gestione dei dati riservati dell'OLO e/o della sua clientela.

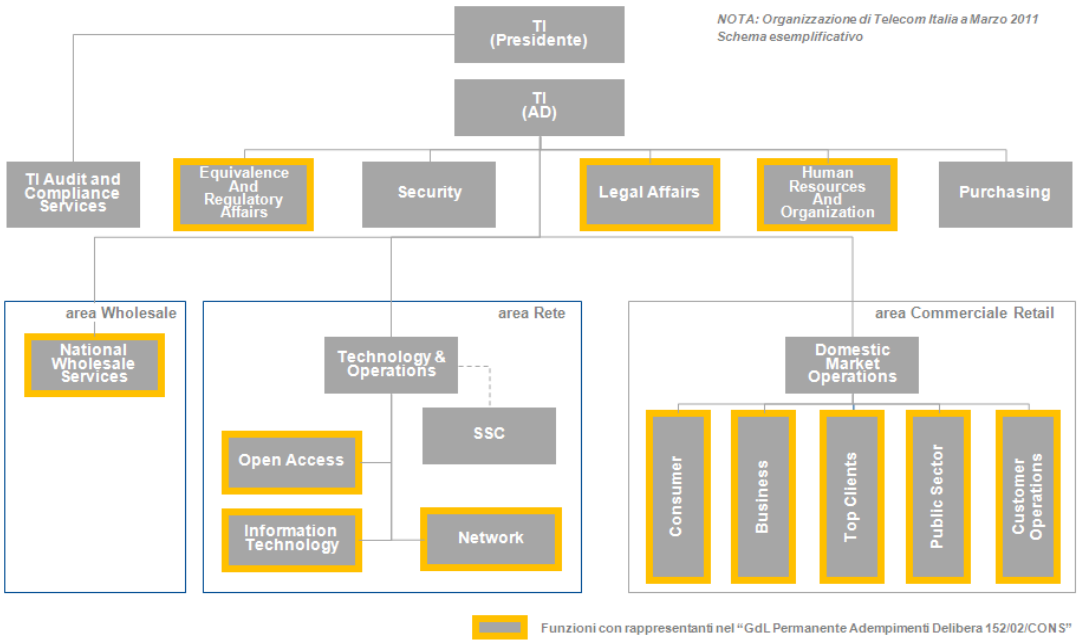
La terza fase dell'attività di verifica (*formalizzazione dei risultati*) ha avuto come scopo l'elaborazione della relazione di "*Certificazione tecnica 2011*" ai sensi della delibera 152/02/CONS, art. 2, comma 7.

5.2 L' Area di indagine

L' Area di indagine identificata per la certificazione tecnica 2011, stabilita in seguito alle analisi svolte in fase di avvio delle attività, è illustrata nei seguenti paragrafi.

5.2.1 Funzioni Aziendali

L'insieme delle funzioni interessate dall'attività di certificazione tecnica 2011 è rappresentato nello schema organizzativo riportato in forma semplificata nella Figura seguente



L'ambito d'intervento è stato tracciato tenendo in considerazione il modello organizzativo consolidato alla data del 30 Marzo 2011, data convenzionalmente assunta come data inizio formale delle attività.

Al fine di mantenere la coerenza nella nomenclatura rispetto alle precedenti relazioni e rispetto al disposto dalla Delibera 152/02/CONS, in questo schema e nel seguito di questa relazione 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 intende la direzione Domestic Market Operations articolata in:
  - Consumer;
  - Business;
  - Top Client;
  - Customer Operations;
  - Public Sector.

- ✓ con **area Corporate** si indica l'insieme delle seguenti funzioni:
  - TI Audit and Compliance Services;
  - Equivalence & Regulatory Affairs;
  - Legal Affairs;
  - Human Resources & Organization;
  - Purchasing.

Di seguito si riporta il dettaglio delle 27 funzioni identificate, suddivise per marco-area di appartenenza.

5.3 Dettaglio delle attività svolte

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

- ✓ sistemi Telecom Italia appartenenti all'area di indagine 2011;
- ✓ 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 delle attività sono state svolte:

- ✓ 27 interviste ai responsabili di funzione, di cui:
  - 18 dell'area Commerciale Retail;
  - 5 dell'area Rete;
  - 4 dell'area Wholesale.
- ✓ 13 interviste ai responsabili di sistema (effettuate per i nuovi sistemi dell'Area di indagine 2011)
- ✓ 42 sonde a campione, di cui:
  - 30 sonde su accessi utente
    - 5 su sistemi dell'area Commerciale retail;
    - 19 su sistemi dell'area Rete;
    - 6 su sistemi dell'area Wholesale.
  - 12 sonde su accessi addetti IT
    - 4 su sistemi dell'area Commerciale retail;
    - 7 su sistemi dell'area Rete;
    - 1 su sistemi dell'area Wholesale.
- ✓ 9 site visit, di cui:
  - 4 in ambito Technology & Operations;
  - 4 in ambito Domestic Market Operations;
  - 1 in ambito National Wholesale Services.
- ✓ 1 intervista conclusiva:

- Equivalence & Regulatory Affairs.

Inoltre sono stati acquisiti ed analizzati:

- ✓ 81 questionari a sistema, di cui:
  - 68 relativi a sistemi già presenti nel perimetro 2010;
  - 13 relativi a sistemi di nuova introduzione nel perimetro 2011.
- ✓ 2 Codici di comportamento;
- ✓ 6 policy e linee guida;
- ✓ Schemi dei profili/funzione e/o procedure di gestione degli accessi per tutti i sistemi appartenenti all'Area d'Indagine 2011;
- ✓ Circa 60 file contenenti evidenze dei processi autorizzativi e verifiche periodiche;
- ✓ Circa 200 file di tracciamento statici e dinamici (prodotti dal Sistema Catone);
- ✓ 90.215 record di tracciamento, di cui:
  - 68.855 tracciamenti utente;
  - 21.360 tracciamenti addetti IT.

Nel corso delle sonde sono state coinvolte circa 70 utenze attive (utenti e addetti IT) e raccolte circa 500 schermate dei sistemi.

Nell'ambito delle verifiche è stato effettuato un controllo sulle abilitazioni e sulle verifiche periodiche su 844 utenze (288 Addetti IT e 556 Utenti).

Le utenze oggetto di verifica sono state identificate tramite la metodologia standard di campionamento di Ernst & Young. In particolare tale metodologia viene utilizzata nelle attività di audit e consente di effettuare le verifiche tramite la selezione di un campione da una popolazione sulla base della teoria del "*test dei 25*".

Tale approccio è basato sull'analisi della popolazione totale oggetto di campionamento e individua una numerosità adeguata in relazione alla dimensione del campione, assumendo un margine di errore statisticamente accettabile.

Tali attività hanno consentito di:

- ✓ Consolidare l'Area di Indagine 2011 costituita dai sistemi che contengono dati riservati dell'OLO e/o della sua clientela;
- ✓ Verificare che per i sistemi già oggetto della certificazione tecnica 2010 le misure di sicurezza siano state mantenute;
- ✓ Verificare che per i nuovi sistemi le misure di sicurezza siano state introdotte.

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

6 Esiti delle attività

Di seguito sono riportati gli esiti puntuali delle attività di verifica svolte nell'ambito della certificazione tecnica per l'anno 2011.

6.1 Verifiche sui sistemi oggetto di indagine

Le attività di verifica condotte sui sistemi di 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 tramite 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 della 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 (ULL, WLR, CPS e NP, etc) 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 della 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 un ruolo specifico ruolo (es. supervisore);
  - Tale personale autorizzato, al pari di tutto il rimanente personale Telecom Italia, è tenuto al rispetto di quanto stabilito dal "Codice di comportamento" e da un'apposita procedura operativa che regola il "trattamento dei dati riservati dell'OLO e/o della sua clientela da parte del personale autorizzato di Customer Operations";
  - Gli eventi censiti ed autorizzati che richiedono la visualizzazione dei dati riservati dell'OLO e/o della sua clientela si riferiscono alle attività di:
    - Gestione reclamo;
    - Gestione prodotti su linea ceduta ad altro Operatore;
    - Scorporo fattura;
    - Gestione frodi;
    - Integrity billing;
    - Gestione degli scarti sui Dati Elenco Abbonati;
    - Gestione dei rientri in Telecom Italia.
- ✓ Le attività del personale che dispone di accesso ai dati riservati dell'OLO e/o della sua clientela sono regolate da appositi policy e linee guida.

6.2 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 Delibera 152/02/CONS.

6.2.1 Diffusione del codice di comportamento

E' prevista (entro il 30 giugno 2011) una nuova diffusione via posta elettronica del codice comportamentale relativo alla delibera 152/02/CONS e la contestuale diffusione del codice di comportamento conseguente agli impegni assunti da Telecom Italia ed approvati con la delibera 718/08/CONS.

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

Inoltre nel corso dell'ultimo anno è stata erogata formazione specifica relativamente ai temi della delibera 152/02/CONS per le risorse neo assunte nelle Funzioni di Open Access e National Wholesale Service che ha interessato complessivamente circa 980 risorse.

6.2.2 Copertura della clausole contrattuali

E' quasi completa l'integrazione dell'apposita clausola contrattuale a tutela della riservatezza dei dati degli OLO nei contratti già in essere e nei nuovi contratti con società terze[8] che sono interessate dalla tematica della Delibera 152/02/CONS, articolo 2, comma 7. Si evidenzia un'unica eccezione per la quale l'inserimento della clausola contrattuale è in corso di formalizzazione.

6.2.3 Gestione e controllo automatizzato delle abilitazioni utenze

E' in corso l'integrazione dei sistemi dell'area d'indagine con sistemi automatici di gestione delle abilitazioni all'accesso.

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

- ✓ dei 59 sistemi gestiti da Technology & Operations - Information Technology, 58 (95%) risultano integrati con sistemi automatici, solo un sistema (in dismissione) prevede l'utilizzo di un *workflow* autorizzativo manuale;
- ✓ i 2 sistemi gestiti da National Wholesale Service non risultano integrati con sistemi automatici e prevede l'utilizzo di un *workflow* autorizzativo manuale;
- ✓ dei 12 sistemi gestiti a livello dipartimentale, è utilizzato un *workflow* autorizzativo manuale che consente di effettuare un controllo delle abilitazioni degli utenti secondo quanto richiesto dalla normativa;
- ✓ i restanti 8 sistemi non posseggono interfaccia utente e quindi non richiedono l'integrazione con sistemi automatici.

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

- ✓ dei 71 sistemi gestiti da Technology & Operation - Information Technology, tutti (il 100%) risultano integrati con sistemi automatici;
- ✓ dei rimanenti 10 sistemi, è utilizzato un *workflow* autorizzativo manuale che consente di monitorare e tracciare l'abilitazione degli addetti IT.

[8] Si intendono tutte quelle società che stipulano un contratto con Telecom Italia che prevede l'utilizzo di dati riservati dell'OLO e/o della sua clientela.

7 Conclusioni della certificazione tecnica

7.1 Valutazione dei sistemi oggetto di 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 della sua clientela, **posseggono misure di riservatezza** che non consentono alle divisioni dell'area Commerciale retail l'utilizzo non autorizzato ai suddetti dati;
- ✓ **i sistemi informativi dell'area Rete e Wholesale posseggono misure di riservatezza** che non consentono alle divisione dell'area Commerciale retail l'utilizzo dei dati riservati dell'OLO e/o della sua clientela

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

Misure Riscontrate									
Categoria Sistemi	**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**	**Esito dell'indagine**
Dedicati Retail	Parziale Nullo	-	√	-	-	-	-	√	OK
Condivisi Retail	Completo Parziale Nullo	√	√	√	√	√	√	√	OK
Frodi,Info 12, Integrity Billing	Completo Nullo	√	√	√	√	-	√	√	OK
DWH Commerciali retail	-	-	-	-	-	-	-	-	-
DWH Rete	Completo Nullo	√	√	√	√	-	√	√	OK
Rete	Completo Nullo	√	√	√	√	-	√	√	OK
Tecnici di Rete	Completo Nullo	√	√	√	√	-	√	√	OK
Dedicati Wholesale	Completo	√	√	√	√	-	√	√	OK

Legenda:

'√' Misura attesa

'-' Misura non applicabile

7.2 Valutazioni delle azioni "non sui sistemi"

Oltre alle azioni previste sui sistemi appartenenti all'area di indagine 2011, Telecom Italia ha attuato una serie di ulteriori azioni (cosiddette "non sui sistemi") atta a garantire il rispetto, da parte del personale, delle raccomandazioni della delibera 152/02/CONS, articolo 2, comma 7.

In particolare si evidenzia che:

- ✓ E' prevista (entro il 30 giugno 2011) una nuova emissione tramite posta elettronica del Codice di comportamento previsto dalla Delibera 152/02/CONS; assieme ad esso è stato diffuso anche il Codice di comportamento conseguente agli impegni assunti da Telecom Italia ed approvati con la delibera 718/08/CONS. Così facendo Telecom Italia si impegna continuativamente a tutelare la confidenzialità dei dati riservati dell'OLO e/o della sua clientela nei confronti del personale dell'area commerciale retail, e a rafforzare la responsabilità di ogni dipendente verso il continuo rispetto della riservatezza dei dati riservati dell'OLO e/o della sua clientela e della parità di trattamento in generale;

- ✓ è stata aggiornata la composizione del "Gruppo di lavoro permanente – Adempimenti delibera 152" in coerenza con la variazioni dell'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 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 riservati dell'OLO.

Inoltre è stata riscontrata, presso le funzioni oggetto di site visit, una diffusa conoscenza della problematica connessa alla gestione dei dati riservati dell'OLO ed una profonda sensibilità del personale nei confronti degli obblighi derivanti dalla delibera 152/02/CONS.

7.3 Valutazione conclusiva

A valle di tutte le attività di certificazione tecnica eseguite per l'anno 2011 riportiamo le nostre conclusioni:

- ✓ i sistemi appartenenti all'area di indagine 2011 posseggono le misure di riservatezza necessarie e sufficiente a garantire la parità di trattamento interna ed esterna ai sensi della Delibera 152/02/CONS articolo 2, comma 7;

- ✓ sono state adottate idonee misure (cosiddette "non sui sistemi") atte a garantire il presidio e il continuo rispetto da parte del personale delle raccomandazioni previste dalla delibera 152/02/CONS, articolo 2, comma 7. A tal fine si è riscontrato, presso le strutture visitate, una piena consapevolezza degli obblighi in capo a Telecom Italia discendenti dalla delibera 152/02/CONS da parte del personale di TI.