UNOFFICIAL TRANSLATION

The following is an unofficial English translation of a report prepared in Italian by the Internal Control and Corporate Governance Committee of the Board of Directors of Telecom Italia S.p.A. for the Board of Directors. In the event of conflict or inconsistency between the terms used in the Italian version of the report and the English translation, the Italian version shall prevail, as the official document is the Italian version.

Milan, February 16, 2007

REPORT OF THE INTERNAL CONTROL AND CORPORATE GOVERNANCE COMMITTEE TO THE BOARD OF DIRECTORS

1. Introduction

1.1. This report has been prepared by the INTERNAL CONTROL AND CORPORATE GOVERNANCE COMMITTEE and sets forth the outcome of the activities performed and the investigations undertaken by the COMMITTEE during 2006 and through the middle of February of the current year with reference to the following matters:
- events related to the ex Head of the Security Function, Giuliano Tavaroli;
- network security and services to the Judicial Authorities;
- traffic data, privacy and collection of information on employees.

1.2. It should be noted that, pursuant to art. 12 of the Self-Regulatory Code of the Company, the COMMITTEE acts as advisor and makes proposals to the Board of Directors. In particular (and insofar as the goals of this report are concerned) the COMMITTEE assists the Board in the execution of its responsibilities for the internal control system, evaluates the work plan prepared by the staff responsible for internal control, receives periodic reports from such staff and reports to the Board at least every six months on its activity and on the adequacy of the internal control system.

1.3. The COMMITTEE is composed entirely of independent Directors (Guido Ferrarini, Francesco Denozza, Domenico De Sole and Marco Onado). The Chairman of the Board of Auditors, or another auditor as designated by him, attends the meetings of the COMMITTEE. When deemed appropriate, depending on the topics to be dealt with, the COMMITTEE and the Board of Auditors meet in joint session.

1.4. It should also be noted that, pursuant to art. 11 of the Self-Regulatory Code of the Company, the Board of Directors is responsible for designing the internal control system and monitors its proper functioning with respect to the management of business risks. The Director delegated for that purpose (currently the Executive Vice Chairman, Carlo Buora) defines the tools and methods for implementing the system of internal control, in execution of the policies established by the Board of Directors, ensures the overall adequacy and effectiveness of the system and its adaptation to changes in the operating conditions and in the legislative and regulatory environment.

1.5. To monitor the correct functioning of the internal control system, the Board of Directors also has access, in addition to the COMMITTEE, to an independent appointee that is endowed with the necessary resources to perform such task. Such appointee, currently the consortium company TELECOM ITALIA AUDIT & COMPLIANCE SERVICES, which for this

purpose appointed its Chairman, Armando Focaroli, reports on its work to the Executive Vice Chairman, the COMMITTEE and the Board of Auditors.

1.6. The Executive Vice Chairman implements the changes to the internal control system that are prompted by the checks carried out, appointing one or more persons for the purpose of implementing such changes. To improve implementation of the internal control system, the role of Group Compliance Officer was created in 2005. To ensure that risk management is coordinated at a senior level a Risk Management Committee was also created in 2006, chaired by Carlo Buora and made up of the managers of the Central Functions involved; in addition, within TELECOM ITALIA AUDIT & COMPLIANCE SERVICES, the office of Group Risk Officer was established.

1.7. The principles of the system of internal control are set forth in art. 11, subsection 6 of the Self-Regulatory Code and also specified in the Organisational Model 231. This Model, adopted pursuant to Italian legislative decree no. 231/2001 (which deals with the liabilities of a company for certain crimes, when committed by its directors, managers or employees in the company's interest or to the company's benefit), consists of "principles of behaviour with Government bodies" and "internal control schemes" in which the principal phases of each process are listed, highlighting corresponding risks, in terms of possible criminal behaviour in connection with the relevant process, and setting out measures designed to avoid such risks. Organisational Model 231 is subject to periodic revision as a result of experience in its application and of the extension of the relevant regulations to new events. A specific "Organismo di Vigilanza", or Supervisory Board, consisting of a Statutory Auditor (Ferdinando Superti Furga, who acts as Chairman), an independent Director (Guido Ferrarini) and the Head of internal audit (Armando Focaroli), monitors – with the support of a specific work group called the 231 Support Group – compliance with the Model and – in collaboration with a Steering Committee consisting of the Senior Executives responsible for the functions involved – proposes any necessary modifications thereof.

1.8. The element of the internal control system that is concerned with financial reporting also relates to the application of the Sarbanes-Oxley Act, which requires certification of the relevant internal controls over financial reporting by the CEO and the CFO, and attestation by the auditors about the adequacy of the controls on this matter, pursuant to Section 404. The Company is currently engaged in an important project designed to ensure the full and correct application of these regulations and thus to improve the internal controls over financial reporting (404 Project). The auditors' attestation will be issued, for the first time, on the financial statements for 2006.

2. The activities performed by the COMMITTEE

2.1. Initially, the investigations with respect to the Security issue involved only the Internal Audit function and the Supervisory Board (see 3.1, below). However, in the Committee's meeting held on May 4, 2005, as part of the quarterly Report of internal audit, the COMMITTEE was provided initial general information on the internal audit addressing the Security function; a confidential report on the notice of investigation issued to Giuliano Tavaroli was also provided.

On July 15, 2005, the COMMITTEE received a report on Giuliano Tavaroli's decision to voluntarily relinquish his managerial activities as the Head of the Security function as

from May 4, 2005 and on the Company's intention to appoint him as a consultant on antiterrorism. .
The Board of Directors received a similar report on July 26, 2005, when it was also informed of the appointment of Giovanni Penna as interim manager of the Security Function.

2.2. The COMMITTEE directly addressed the three topics that are the subject of this report from 2006 onwards, in the meetings specified below:

2.2.1. Meeting on March 30, 2006: examination of press coverage of alleged irregular phone tapping and improper use of customer traffic data, with respect to the Tavaroli issue; notification by the Head of internal audit of (i) the audit operation carried out in February/March 2005, (ii) the acquisition of the results of such audit by the Judicial Authorities, and (iii) the subsequent organisational changes which had been put in place and declared to be suitable. These issues were reported to the Board of Directors on May 8, 2006;

2.2.2. Meeting (together with the Board of Statutory Auditors) on June 12, 2006: examination of compliance issues (network, IT systems, services for the Judicial Authorities), with respect to the Tavaroli issues; the COMMITTEE was informed that a memorandum had been filed with the Judicial Authorities; all of this was reported to the Board of Directors on July 5, 2006, when a document concerning the matters discussed in this Report was also examined;

2.2.3. Meeting (together with the Board of Statutory Auditors) on September 29, 2006: analysis of the arrest warrant issued by the Magistrate responsible for the preliminary investigations by the Milan Court against Giuliano Tavaroli (a warrant that became public knowledge following its publication on the Internet at www.ilvelino.it; hereinafter "the Warrant"); examination of the alleged violations of privacy rules in handling traffic data and the activities performed by the Company to comply with an Order issued by the Privacy Authority on June 1, 2006;

2.2.4. Meeting (together with the Board of Statutory Auditors) on October 3, 2006: continuing examination of the aforementioned privacy issues;

2.2.5. Meeting (together with the Board of Statutory Auditors) on October 12, 2006: presentations by the Executive Vice Chairman, representatives of KPMG Advisory, representatives of Reconta Ernst & Young (who described the additional audit activities to be performed concerning the Security issue) and by Davis Polk & Wardwell, the Company's U.S. legal advisors with respect to the applicable issues to be considered from the perspective of United States law (applicable to the company since it is listed on the NYSE); report on the legal opinions sought from external legal advisors on various aspects of Italian law relating to the object of this Report;

2.2.6. Meeting (together with the Board of Statutory Auditors) on October 24, 2006: review of the legal opinion by Professor Mucciarelli on the relevant issues with respect to the Tavaroli matter, in the light of Italian legislative decree no. 231/2001 (see paragraph 3.5 below); meeting with KPMG Advisory and with senior management for an update on the topics that are the subject of this report;

2.2.7. Meeting (together with the Board of Statutory Auditors) on October 31, 2006: presentation by the Executive Vice Chairman on the actions of the Risk Management Committee he chairs, and on the coordination of the work of the Risk Management Committee and the COMMITTEE for better management of risks in general, and for an adequate response to the recent events reviewed in the meetings described above in particular, as well as on the present organisation of the Security function and other organisational issues involved in such events.

2.2.8. Meeting (together with the Board of Statutory Auditors) on December 12, 2006: check on the progress of IT compliance initiatives, and update on the Tavaroli matter.

2.2.9. Meeting (together with the Board of Statutory Auditors) on January 31, 2007: receipt of the first results of the additional audit activities performed by the audit firm Reconta Ernst & Young with regard to the Security issue, discussion with the Executive Vice Chairman of the events relating to Fabio Ghioni (a former employee of Telecom Italia) and the so-called "Tiger Team" (the office within the Security function of Telecom Italia in charge of technical security issues, acting under the responsibility of the aforementioned Ghioni);

2.2.10. Meeting on February 16, 2007: update on the Company's activities regarding IT compliance, communications by the audit firm Reconta Ernst & Young on the continuation of its work programme relating to the abovementioned additional audit activities; clarifications on methods and timeliness of the Company in addressing the requests by the Judicial Authorities with reference to the unauthorized access to the computer network of RCS (one of the most important Italian publishing companies, with a presence both in Italy and abroad) widely commented upon by the Italian press.

3. Information received and activities performed by the COMMITTEE

During the meetings listed above, representatives from the applicable offices of the Company have informed the COMMITTEE of the facts of, and expressed their opinions on, the matters at stake.

3.1. *The Security issue*

3.1.1. *Audit and reorganisation*

3.1.1.1. A review by internal audit of expenses for professional and consultancy services rendered to the Security Function – Intelligence department was carried out in February/March 2005. The purpose of the audit (not included in the 2005 Audit Plan, but performed at the request of CEO Carlo Buora, in part as a result of the increase in the expenses of this Function) was to evaluate the relevant internal control system through remote (computerised) access to documentation and subsequent interviews with the head of the office.

3.1.1.2. The final report did not identify specific concerns, although it highlighted that the internal control system of the Security function allowed regular recourse to purchases of professional and consultancy services outside the ordinary procedure (so-called purchases "in derogation" accounted for 60% of the overall amount of this kind of services) and the head of the Security function to determine the choice of supplier, to approve the service provided, and to authorise invoices for payment.

In the introduction to the executive summary, it was emphasised that the period under consideration was "characterised by intense activity to counteract threats by third parties which certainly influenced the modus operandi of the entire structure" (with implied reference to the well known events in Brazil). The conclusions of this report acknowledged the "objective difficulties (involved in) creating a 'traditional' control system given the sensitivity of the activities concerned" .

The Head of internal audit, Armando Focaroli, informed the senior management of the Company of the outcome of the audit, and also informed the members of the Supervisory Board, on an informal basis. The latter agreed that the control system of the Security function needed strengthening.

The Supervisory Board formally considered the issue in a meeting on May 31, 2005, when Armando Focaroli presented a summary of the result of the audit over professional services and consultancy procurement by the Security Function. The Supervisory Board agreed upon the need for a control system based on the separation of operational and supervisory roles, and requested that they be kept constantly updated.

3.1.1.3. In the meantime, on May 3, 2005, Giuliano Tavaroli received a notice of investigation indicating that investigations were pending against him for violation of official secrecy and conspiracy. His office in Telecom Italia was searched, and the Polizia Giudiziaria (Criminal Police) acquired the report of the aforementioned audit of the Security Function.

On May 12, 2006 the Judicial Authorities requested that the Company provide invoices issued by some suppliers to the Security Function.

A task force including representatives of various departments within the Company was established for the purpose of verifying, for payment purposes, the invoices received from the suppliers indicated. The commissioning of services from these suppliers ceased.

3.1.1.4. As soon as Tavaroli received the notice of investigation, he asked to be relieved of his work responsibilities with immediate effect for a period of three months. On July 5, 2005 the employment relationship with Tavaroli was terminated, with effect from July 31, with customary financial settlement.

Giovanni Penna was appointed as interim manager of the Security Function with effect from August 1, 2005.

On July 19, after the terrorist attack in London, and with the agreement of the governmental authorities, Tavaroli was appointed as a consultant on antiterrorism issues on a one year contract at a fee of 50,000 Euros (as reported by the Chairman of the Board, Mr. Tronchetti Provera, in the meeting of the Board of Directors on July 26, 2005 and by Mr. Chiappetta, General Counsel of the Company, in the meeting of the COMMITTEE on July 15, 2005). On September 23, 2005 a power of attorney was conferred on Tavaroli in relation to the aforementioned appointment, but it excluded the authority to make purchases. The appointment as a consultant – subsequently extended to business continuity issues, without change of fees or duration – was terminated in March 2006, and the power of attorney was cancelled on June 19, 2006.

3.1.1.5. The reorganisation of the Security Function as indicated above continued.

Initially the creation of a consortium company similar to TELECOM ITALIA AUDIT & COMPLIANCE SERVICES was considered; instead the Company opted for restructuring the Function internally, by separating operational and control roles.
After the changes, the Head of the Security Function (identified as Gustavo Bracco, the Director of the Human Resources and Organisation Function, in January 2006) does not have a direct operational function, but supervises and directs; he is supported by a staff for planning and control, which ensures correct application of administrative procedures, documentary support for operations, and that expenses are pertinent to the objectives attained.
The reorganisation was reported to the Supervisory Board on February 28, 2006. Mr. Focaroli declared that the need to strengthen the internal control system in the intelligence sector of the Security Function had been satisfied by the actions taken. The same meeting approved the report of the Supervisory Board for 2005, containing information on the results of the audit and on the organisational remedies for the shortcomings encountered.
Similarly, in the meeting of the COMMITTEE on March 30, 2006 Mr. Focaroli explained that – as previously reported to the Supervisory Board in April/May 2005 (see 3.1.1.2 above) – "early in 2005 TI Audit reviewed the consultancy and professional services expenses of the structure (Security), in the light of a significant and rapid rise in expenditure, for which there were also objective reasons. The audit highlighted some critical aspects, not in terms of irregularities, but because of inadequacies in the control system resulting from the number of tasks directly performed by the head of the office. […] The comments of the internal auditor were followed by organisational changes, without affecting the special aspects of the specific type of services".

3.1.1.6. The issue raised by the internal audit report was presented by management as principally organisational in nature, and the Company took action to provide a suitable response in organisational terms.
It was not considered necessary to take further action, given:

a. the special nature of the sector (and the very sensitive situation in terms of international, in addition to Company, security). This gave credibility to avoiding the storage on Company premises of documents and other results of investigations for certain sensitive activities;
b. the excellent results achieved by Tavaroli in recent events (such as the Kroll business in Brazil, in which a formal apology letter was actually presented to Telecom Italia); and
c. the fact that the amounts in question were not material in terms of their possible impacts on the company financial statements, and on the overall assessment of the Company's internal controls.

3.1.2. *Emergence of new information*

3.1.2.1. The issue assumed a different character at the end of 2005, when the defence counsel of Emanuele Cipriani (one of the most significant providers of outside services to the Security Function – Intelligence department of both Telecom Italia and Pirelli) forwarded a request (to be specific, only to Pirelli) that raised doubts about whether or not the services invoiced to Telecom Italia had actually been provided. The Company (just as Pirelli) engaged an outside attorney as legal advisor to investigate the invoices paid in the past to companies linked with Cipriani.

3.1.2.2. In the previously mentioned meeting of the COMMITTEE on March 30, 2006, director Francesco Denozza "demanded clarification of the news that had appeared in the daily press about alleged irregular payments made by the Security function". Management affirmed that, in the light of the investigations undertaken so far and still underway at that time, the payments made by the Company appeared justified by the services actually rendered.

3.1.2.3. The investigation by the outside legal advisor was completed on April 21, 2006, and emphasised that in many cases it had not been possible to reconstruct the purpose of the services rendered. However, the sums involved (an estimated 8.5 million Euros for the period between May 30, 2002 and November 3, 2004) were not such as to reach a negative conclusion about the quality of internal controls (and certainly did not constitute a material weakness under US criteria), and in any event the issue had been tackled through the procedural changes made over a year earlier. The Company gave a detailed account of this matter in the memorandum filed with the Judicial Authorities on June 8, 2006.

3.1.2.4. In its meeting of October 3, 2006, the COMMITTEE requested that Mr. Focaroli question the top management of the Company in place at the time of the events under consideration (Tronchetti Provera, Buora and Ruggiero) and their direct reports (a total of 17 senior managers) to check if services had been commissioned to Tavaroli between March 2003 and May 2005, and, if that was the case, what they were, how they were assigned, and how the results were obtained.
Of the 20 people to whom the request was made, 10 responded affirmatively, and supplied information about content of the tasks, how they were assigned, and how the results were obtained; such information did not provide any problematic evidence.

3.1.2.5. From the Warrant, the COMMITTEE learnt that certain administrative documents had been destroyed by employees of Pirelli and Telecom Italia. The Board of Statutory Auditors requested internal audit to investigate whether possible further similar episodes might have occurred in the Company. The outcome of this investigation was negative.

3.1.2.6. Ad hoc audit procedures are being carried out by the audit firm Reconta Ernst & Young, in relation to the acquisition of services provided to the Security function during the period 2001-2006, with the primary objective of evaluating possible impacts on the financial statements of Telecom Italia. In the meetings of January 31 and February 16, 2007 the COMMITTEE was updated on the progress of the work programme which, as agreed with the Company, was conducted according to the applicable auditing standards and Consob guidelines. The review completed to date, which covered all the suppliers cited in the aforementioned Warrant, do not evidence a "material" impact on the balance sheet.

3.1.2.7. The Company has cooperated with the Judicial Authorities, presenting further memoranda on October 19, December 6 and December 14, 2006.

3.1.2.8. The "maintenance" work on Organisational Model 231 has continued, and has in fact been accelerated by the matters examined here.
In particular:

- The Group 231 Steering Committee approved an addition to the control scheme for “Agents and Intermediaries”: the change (which is included in the corresponding standard contract form) prohibits the agent or intermediary from transferring a credit and/or giving mandate for payment, so as to ensure that only the agent or intermediary can be the actual recipient of the payment. Any derogations from this provision are to be highlighted in the quarterly information flows to the Supervisory Board, and payments made somewhere other than the residence/domicile/registered offices of the agent or intermediary are also to be highlighted.
- This amendment was extended to other control schemes within the Organizational Model with the approval of a similar modification to the control schemes relating to “Consultancy and Professional Services”, “Sponsorships” and “Acquisitions of goods and services”.
- With respect to “Consultancy and professional services”, the Company is checking, at the specific request of the Board of Statutory Auditors, the efficacy and efficiency of the current procedure, paying particular attention to operations performed “in derogation”. Previously, on this same matter, the Executive Vice Chairman issued an order stating that recourse to derogations of the procedures envisaged in the Organisational Model 231 and, more general, in the internal control system, were prohibited – unless explicitly authorised by the Executive Vice Chairman himself. Subsequently, in January 2007, a special procedure for the management and payment of “non-system” invoices became operative, which provides for invoices relating to amounts exceeding a determined threshold, and in any cases where is deemed appropriate, regardless of the amount of the invoice, requiring the authorization by the Executive Vice Chairman. In addition a specific report is to be issued periodically checking and monitoring this issue.

3.1.2.9. As referred to in the COMMITTEE meeting of February 16, 2007, the re-organisation of the Security function has continued with the transfer of the IT Security technical activities to the technical auditing unit of TELECOM ITALIA AUDIT & COMPLIANCE SERVICES, concentrating the activities of Security on security and management of information (such as defining policies with respect to protection of information, identification of the owner of the process/system, etc.).
Revision of the qualification system for suppliers of “Investigation Services” is under way, and a corresponding review is under way for the qualification system of suppliers of “Executive Protection”, while the definition of a vendor rating procedure is under consideration, with the goal of evaluating the services of suppliers. Monitoring will be carried out in accordance with criteria established in the general procedures used by the Company in other areas, and will be based on the evaluations of technical, administrative and commercial quality.

3.2. *Network security and services to the Judicial Authorities*

“Judicial systems” are a combination of systems designed to deliver services to the Judicial Authorities pursuant to statutory provisions applying to all telecommunications operators. It should be noted that tapping activities pursuant to an order by Judicial Authorities take place outside of Company premises. The Company does not participate in tenders for the organization of monitoring centres, and only fulfils its legal obligations, imposed on all operators, to route the lines that competent Judicial Authorities have arranged to be monitored, to the pre-selected numbers indicated by the same Judicial Authorities.

3.2.1. The COMMITTEE examined this subject several times during 2006. In particular, during the meetings of March 30 and June 12, 2006, reference was made that:

a. the Company, after a significant reorganization in 2003, carried out a series of changes to its organisational structure in 2005 so as to offer a united, centralised interface with the Judicial Authorities, and to improve quality and timeliness of the service;
b. the relevant organization was rationalised with the creation of the JUDICIAL AUTHORITIES SERVICES Office (Funzione SERVIZI AUTORITÀ GIUDIZIARIA - otherwise named SAG), through the integration in a unique centre of certain offices of the Company (already operating in the NATIONAL JUDICIAL AUTHORITY CENTRE, CENTRO NAZIONALE AUTORITÀ GIUDIZIARIA - CNAG, within the Security function) and TIM (Telecom Italia's subsidiary focused on mobile services, which had been merged with and into Telecom Italia), dedicated to mandatory services for Judicial Authorities. SAG's responsibility was placed under the responsibility of the Legal Affairs Manager (organisational measures of November 25, 2005);
c. the adopted procedures protect Telecom Italia, as the actual tapping takes place in premises controlled by the Judicial Authorities. In particular, management confirmed that "the tapping issue is fully under control, and does not represent a problem" (COMMITTEE meeting of June 12, 2006);
d. the support systems for the activity of intercepting mobile lines were granted certification by the company CSQ, applying standards defined by the BSI - British Standard Institute (standard ex BS7799, equivalent to ISO 27001).

3.2.2. In conclusion, the "tapping" issue, in the strictest sense, has never been a critical problem according to the information supplied to the COMMITTEE.

3.2.3. There is a more general problem of protection of privacy with reference to the treatment of judicial data and the management of the flow of information relating to mandatory services supplied to the Judicial Authorities; on December 15, 2005 the Privacy Authority addressed a specific ruling to all operators, and prescribed the adoption, within 180 days, of specific measures designed to guarantee and increase protection of managed data. The requirements (concerning organisational aspects; the security of the flow of information to and from the Judicial Authorities; and the protection of data used for judicial purposes) relate to the form and authenticity of the Judicial Decrees to commence activities, the methods of transmission of the corresponding documentation, the management of the authorisation profiles and the attribution of access rights to the IT resources. Issues which, at least with respect to the first two topics, require cooperation with the Judicial Administration.

On June 20, 2006 Telecom Italia responded to the ruling of December 15, 2005, submitting a report on compliance with the requirements (which were only partially met, as some of them required, for their implementation, the Judicial Authorities' offices also to meet suitable technical requirements).

On September 20, 2006 the Privacy Authority issued a new ruling regarding services provided to the Judicial Authorities, ordering all telephone operators to complete the implementation, within 90 days, of the directions under the aforementioned ruling of December 15, 2005, and aimed at safeguarding data and flow of information relating to activities connected with the services supplied to the Judicial Authorities.

3.2.4. The Company requested the advice of KPMG Advisory on services to the Judicial Authorities. In the meeting of October 31, 2006 KPMG Advisory reported their findings to the COMMITTEE:

a. the lack of an overall plan, complete and updated, of the IT applications within the area of SAG;
b. that the Circe system (i.e. the software for the execution of mandatory services to be supplied to the Judiciary in the mobile sector) evidenced some weaknesses, which could cause potential security risks, as well as difficulty in the ex-post verification of consistency of activities carried out with the competent authorities' requests;
c. there was a lack of continuity in the integration process between the systems for wired network and those applying to the mobile services.

However, in the meeting of February 16, 2007, management reported to the COMMITTEE the results of the review that had been carried out since October 31, 2006. Based on the assessment performed to date, 23 systems were identified that are used exclusively to comply with Judicial Authorities' requests, and 14 systems were identified that support the supply of mandatory services to the Judicial Authorities on a non exclusive basis. In the meantime, the project aimed at compliance with the ruling by the Privacy Authority of September 20, 2006 was substantially concluded within the prescribed deadline. Such compliance was confirmed to the Authority in a special document filed on December 22, 2006. Such report indicated that the correct operation of the implemented solutions depends on the adoption by the Judicial Authorities' offices of suitable equipment for the reception and sending of communications in accordance with the secure protocols that have been defined.

3.2.5. In addition, assessment activities over the medium term continue in order to rationalise and integrate the various current structures and procedures. Both the systems used for mandatory services and the support systems are undergoing analysis and evaluation of the IT applications used and the relative processes that are managed, in order to determine, with the advice of KPMG Advisory, possible risks and areas for improvement.

3.3. *Traffic data, privacy and information on employees*

3.3.1. This subject came to the attention of the COMMITTEE at the beginning of 2006, when an increase of improper dissemination of clients' personal data (traffic data) by disloyal employees occurred. A new case, in particular, presented a significant difference to past cases. Until that time, each time these events occurred, the person responsible was quickly identified and subjected to disciplinary actions, including dismissal. In the new case, however, the Company was unable to identify the person responsible.

Taking this into account, in March 2006 the CEO, Carlo Buora, held a managerial work team on the subject of security and protection of traffic data. The analyses by this group concluded that, in particular, the planning of the systems that manage the traffic data was incomplete, with consequential unavailability of information on the number of individuals authorised to access such data.

3.3.2. During the COMMITTEE meeting of June 12, 2006 management indicated its confidence in the quality of the relevant controls. (As pointed out in the memo distributed during the meeting, "It is, however, important to highlight how the control systems are correct in the sense that, in retrospect, the extracted log files have allowed for the certain identification of the perpetrators of offences, both in the cases

of violations carried out by personnel from offices servicing the Judicial Authorities, and in the cases of personnel from other offices").

3.3.3. However during the aforementioned meeting, the COMMITTEE was informed that, during inspections by officers of the Privacy Authority, it emerged that an existing system (Radar) did not comply with company security standards, nor to legal requirements. The Company, however, had immediately arranged to block the Radar system from further use and reported the occurrence to the Judicial Authorities.

3.3.4. On June 1, 2006, after an appeal by a client, the Privacy Authority ordered the Company to adopt, within 120 days, a set of protective measures for traffic data, in the absence of which the Company should stop handling the data.

3.3.5. The Company's response, with respect to a situation that proved to be different and more worrisome than had been previously understood, took the form of:

a. a mandate to KPMG Advisory for the independent audit and analysis of the security of the processes and the IT systems of the Company, with particular reference to traffic data;
b. the definition of a project with a more general scope, addressing the entire company organisation, dealing with the three levels of strategy, coordination and operation, which focused on 132 company applications. According to technological suppliers, Telecom Italia's initiative was likely to be unprecedented on a worldwide basis, and certainly it was a first for Italy, as far as dealing with these kinds of issues in a large scale operational context;
c. an undertaking (already carried out) representing Company internal resources of 2 million man/hours, with an estimated investment of over 30 million Euros for 2006 (7 million Euros for the years 2007-08).

On September 29, 2006 a document was filed with the Privacy Authority, describing the activities completed, the initiatives that were on-going and relevant technical problems (due in part to Italian legal requirements with respect to digital signatures that are particularly burdensome). On October 30, 2006 an update document was likewise submitted describing the activities carried out to date.

In the COMMITTEE meeting of December 12, 2006, Management reported that the activities completed to date to address compliance with the Authority ruling dated June 1, 2006 had made the applicable systems fully compliant with relevant privacy requirements which - according to management's evaluation - were relevant to allow the Company to continue the effective operation of its business.

3.3.6. At the COMMITTEE meeting of December 12, both KPMG Advisory and the Company's IT Governance manager presented a further update on the actions taken since October 31, 2006, and on the timing of those still in progress.

3.3.7. With a measure dated December 7, 2006 the Privacy Authority resolved to extend, until March 31, 2007, the deadline for completing the requirements set forth in the order of June 1, 2006. The corrective work carried out by the Company has thus been positively appreciated.

3.3.8. In the meeting of February 16, 2007, with reference to systems which deal with traffic data, the COMMITTEE was informed that, with respect to the 35 applications that were still critical at September 30, 2006, required remedies have now been carried out for 31 applications. The correction of the remaining 4 applications

(systems that supply added-value services, that are complex but of low importance) will be completed well before the deadline provided by the extension order of December 7, 2006. As required by the above-mentioned extension order, an update document on the status of these activities was submitted to the Authority on January 31, 2007.

3.3.9 The COMMITTEE, on reading the Warrant, also learned about collection of information on employees. In particular, according to the Warrant (which contains very harsh words in this respect), the Security department had collected information on a certain number of employees during the period February – August 2004.

3.3.10 The enquiry carried out by the Human Resources Management showed that:

a. the controls were arranged at the initiative of Tavaroli, who asked the Wireline Human Resources Department for lists of candidates for employment in order to allegedly counter the risk of terrorist infiltration.
b. in two cases indication of non-suitability were notified to the Wireline Human Resources Department (verbally). The two candidates were not hired;
c. Human Resources Management declared it ignored the enquiry methods used by Tavaroli.

3.3.11 In the report by Gustavo Bracco, Head of the Group's Human Resources function, it was specified that "there is no policy on the subject, nor any instruction was given to this end by those in charge of human resources management".

3.4. Recently, the press reported some criticism regarding the way the Company met requests from the Judicial Authorities with reference to the episode of unauthorized access to the RCS computer network: the enquiries carried out by the management concluded that there have not been delays, but evidenced that some of the responses to the Judicial Authorities were provided by Mr. Ghioni, who is currently under arrest for alleged crimes committed in relation to the unauthorized access to RCS's computer network.

3.5 Professor Avv. Francesco Mucciarelli, an expert in criminal law, expressed his opinion on the possibility of Telecom Italia being held responsible under Italian Legislative Decree 231/01 for the facts under the Warrant.
Professor Avv. Mucciarelli gave a negative reply to this question.
As among the alleged offences in the Warrant, only the episodes of corruption are covered by Legislative Decree 231/01, and Mr. Tavaroli, sole ex-employee of Telecom Italia under investigation for corruption, is to be considered (by way of a conservative interpretation) a top manager ("apical subject" as per Legislative Decree 231), the alleged corruption, according to current knowledge, only refers to the giving of a sum of money to public officials by Mr. Cipriani, through Italian and foreign companies reporting to him, for the acquisition of information not legitimately available to third parties.
Professor Mucciarelli observed that no notification has been given to Telecom Italia under d.lgs. 231/01, in that the illegal actions performed appear to have been committed to the detriment of the Company and not to its advantage or in its interests; in this consideration it is apparent that the illegal conduct has occurred without the knowledge of the company management.
On the other hand, the offences alleged, and in particular the offence of association and fraud, conflict with the interests of the Company, and would give basis to the hypothesis that they were carried out through methods aimed at concealing their true nature. This latter consideration seems to Professor Mucciarelli particularly significant, in that one of the requirements for

exclusion of direct responsibility of the corporation, when the deed is committed by a top manager, consists in the fraudulent evasion of existing organisational models.
Obviously the opinion of the Professor is based on publicly available information and certain Judicial Authority's evaluations of the relevant facts and their qualification as criminal acts, which have yet to be declared final and proven in court.

4. Proposals

4.1. The COMMITTEE, on the basis of the information received from Management and advisors, as well as considering the measures taken by the Judicial Authority and the Privacy Authority, believes it necessary that the actions already in progress be integrated and strengthened in order to ensure confidence in the organization and the correctness of the Company's behaviour.
In this respect it is necessary to start and/or finalize the following initiatives as soon as practicable:

4.1.1. full compliance with the Privacy Authority's requirements under the measure of June 1, 2006 (deadline extended to March 31, 2007), by performing the plan of actions already initiated;

4.1.2. immediate implementation of the measures identified by the management with the support of KPMG Advisory, as per their advisory report on the state of Company IT procedures and systems with respect to security (under §3.3.6);

4.1.3. ascertaining the reasons that prevented suitable perception of the risks connected to compliance with privacy regulation, and proposal for subsequent measures;

4.1.4. completion of the enquiry by Reconta Ernst & Young on how (if at all) the findings in the Security sector affect the Company's financial statements;

4.1.5. assessment of the organization of the Security function being adequate, taking into account the remedies already implemented, with particular attention to the respect of operational correctness and the efficiency of controls;

4.1.6. evaluation of the efficiency level of the solutions set forth by the Organizational Model 231 on the subject of consultancy;

4.1.7. determination if the Tavaroli issue may still affect the Company. And in particular: (i) understand the references in the Warrant to Tavaroli's position after May 2005 ("according to documents, it results that for a certain period, even after his distancing from the management of the Security sector, he maintained an active role in Telecom, operating, in particular, from Romania") [page 337]", and (ii) verify if, subsequent to May 2005, Company employees or officials have, no matter what the responsibilities of Tavaroli as a consultant were, allowed Tavaroli to access company data; and

4.1.8. determination if any office or any individual employee / consultant of the Company in any way facilitated the acquisition and treatment of confidential data, or data however unrelated to the professional aptitude, of perspective employees; adoption of procedures to ensure respect of applicable security regulations.