UNIVERSITY
OF TRENTO

DEPARTMENT OF INFORMATION AND COMMUNICATION TECHNOLOGY

38050 Povo – Trento (Italy), Via Sommarive 14
http://www.dit.unitn.it

USING A SECURITY REQUIREMENTS ENGINEERING METHODOLOGY IN PRACTICE: THE COMPLIANCE WITH THE ITALIAN DATA PROTECTION LEGISLATION

Fabio Massacci, Marco Prest and Nicola Zannone

November 2004

Technical Report # DIT-04-103

Using a Security Requirements Engineering Methodology in Practice: The compliance with the Italian Data Protection Legislation[*]

Fabio Massacci
Dip. di Informatica e Telecomunicazioni
University of Trento
fabio.massacci@unitn.it

Marco Prest
Direzione Amministrativa IT
University of Trento
marco.prest@unitn.it

Nicola Zannone
Dip. di Informatica e Telecomunicazioni
University of Trento
zannone@dit.unitn.it

Abstract

Extending Requirements Engineering modelling and formal analysis methodologies to cope with Security Requirements has been a major effort in the past decade. Yet, only few works describe complex case studies that show the ability of the informal and formal approaches to cope with the level complexity required by compliance with ISO-17799 security management requirements.

In this paper we present a comprehensive case study of the application of the Secure Tropos RE methodology for the compliance to the Italian legislation on Privacy and Data Protection by the University of Trento, leading to the definition and analysis of a ISO-17799-like security management scheme.

1 Introduction

The last years have seen a major interest in the development of requirements engineering (RE) methodologies which are able to capture security requirements. This has been marked by some workshops (SREIS, SAPS, REHAS, et al.) and many papers and books [3, 17, 13, 19, 20, 22, 15, 21].

Some works have focused on modelling security and privacy concepts within existing RE frameworks. For example Liu et al. [17] have used Tropos/i*, while Anton et al. [3] have proposed a taxonomy of privacy requirements based on a goal oriented methodology. Others have modified the RE constructs to account for special constructs for privacy & security. The most notable proposal is Jürjens's UMLsec [15] where security tags are added to UML constructs. McDermott and Fox introduce abuse cases [19]. An abuse case is an interaction between a system and one or more actors, where the results are harmful to the system, or one of the stakeholders of the system. Sindre and Opdahl [20] define the concept of a misuse case, the inverse of a use case, which describes a

[*] This is a revised and extended version of [18]

function that the system should not allow. An analogous proposal has been put forward by van Lamsweerde et al. [22] that introduce the notion of anti-goals, i.e., goals of the attacker that can be refined. Giorgini et al. [13] present a framework extending Tropos in which security is considered during the whole process of requirements analysis, and trust and delegation relationships are used to model the interactions among actors involved in the system. Many of those proposals are backed up by a number of formal analysis tools that can be used to support the requirement engineer in the validation and verification of the analysis. For sake of example Jurien's work [15] is based on the AutoFOCUS case tool, van Lamsweerde's approach is based on the KAOS, modal logic based, reasoning tool [22], and Giorgini et al. work is based on Datalog [13].

Yet, what seems missing is the proof-of-concept ability to support the enterprise in the definition of complex security policies as dictated by ISO security standards (e.g. ISO-17799 [14]) or complex national Data Protection Legislation. Indeed, it should be possible to use the RE methodology to derive the policy itself using its refinement mechanism and verify and validate the same policy using the analysis tools available with the framework. In contrast, many papers presents the methodology and supply some (toy) examples but only a handful describe complex case studies [4, 7, 11, 10] which really copes with the complexity required by an ISO-17799 compliance.

In this paper we present a major case study of the application of the Secure Tropos requirements engineering modelling and formal analysis methodology [13, 12] for the compliance to the Italian legislation on Privacy and Data Protection by the University of Trento. In this report, we focus on the key modelling aspects of the case study and refer to [13] for the introduction of the general formal framework based on Datalog.

In the next section we briefly sketch the Italian and EU Data Protection Legislation and its requirements (§2) and the information about the Univ. of Trento that is relevant to the law (§3). Then we present the Secure Tropos RE methodology (§4) and we dig into the details of the case study showing some examples of modelling actors (§5), modelling dependency and delegation (§6), and refining one's specification (§7). Finally we point out to a number of issues that have been discovered by the analysis (§8), discuss related case studies and conclude (§9).

2 The Italian Data Protection Legislation

Many countries have recently promulgated a new privacy legislation spurred by increased concerns over data protection. Table 1 gives a brief history of European and Italian legislation about protection of personal data and privacy.

In Italy, data protection legislation is less than a decade old. Transposing the EC Directive 1995/46 into Italian law, the Italian Data Protection Act decreed that personal data are to be processed "by respecting the rights, fundamental freedoms and dignity of natural persons, in particular with regard to privacy and personal identity". This goal was achieved by imposing to every data controller a set of obligations:

- identification of all entities involved in data processing with their roles and responsibilities;
- assurance that the purpose of data processing is fair, lawful and legitimate;
- implementation of minimal precautionary security measures to reduce risks on data disclosure were clearly defined with a later regulation enacted by Decree on July 28th, 1999.

Table 1: Brief history of European and Italian data protection legislation

European Legislation
Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector ("Directive on privacy and electronic communications").
Directive 2002/22/EC of the European Parliament and the Council of 7 March 2002 on universal service and users rights relating to electronic communications networks and services ("Universal Service Directive").
Directive 2002/21/EC of the European Parliament and the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services ("Framework Directive").
Regulation No 45/2001 of the European Parliament and the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.
Directive 2000/31/EC of the European Parliament and the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce").
Directive 1997/66/EC of the European Parliament and the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector (It has been repealed and replaced by Directive 2002/58/EC).
Directive 1995/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Italian Legislation
Legislative Decree No 196 of 30 June 2003 Italian Personal Data Protection Code.
Directive of Innovation and Technologies Department of 16 January 2002 on computer and telecommunications security in Public Administration.
Legislative Decree No 467 of 28 December 2001 concerning corrective and additional provisions with regard to the protection of personal data in accordance with Act No 127 of 24 March 2001.
Act No 325 of 3 November 2000 on provisions concerning the adoption of minimum security measures for personal data processing in accordance with Act No 675 of 31 December 1996.
Legislative Decree No 281 of 30 July 1999 concerning provisions with regard to personal data processing for historical, statistical and scientific research purposes.
Presidential Decree No 318 of 28 July 1999 Regulation on minimum security measures for personal data processing in accordance with Act No 675 of 31 December 1996 (It has been repealed and replaced by Legislative Decree No. 196/2003).
Act No 675 of 31 December 1996 on protection of individuals and other subjects with regard to the processing of personal data (It has been repealed and replaced by Legislative Decree No. 196/2003).

Innovation and Technologies Department enacted the Directive on Computer and Telecommunications Security in Public Administration on January 16th, 2002. It was the first Directive of Italian Government that forces the entire public administration process to assess the security of their information systems and the start of the necessary activities to ensure their compliance to a minimal security basis. This minimal security base is defined by six main features: security policy, organization (roles and responsibilities), procedures, management and control, risk analysis and staff training. It required the adoption of a procedure for computer security incidents management and the creation of Computer Emergency Response Team (CERT). The requirements were close but not identical to the ISO standard 17799.

Later EU and Italian legislation systematized the norms on privacy and data protection. It confirmed and integrated:

- the definitions of personal data, sensitive data, and data processing,
- the definitions of all entities involved in data processing, their roles and responsibilities (controller, processor, operator, subject),
- the obligations relating to public and private data controllers with specific reference to the legitimate purpose of data processing and the adoption of minimal precautionary security measures to minimize the risks on data.

Skipping over specific ruling penalties and procedures, the law included a technical annex that regulates the implementation of minimal precautionary security measures as authentication and authorization system, antivirus, data backup and restore, and structure.

These measures had to be detailed into a "Documento Programmatico sulla Sicurezza" (DPS). The DPS is a security policy document for the management of all aspects of security concerning

- organization, technology and procedures - explicitly imposed as an obligation to data controllers by the Data Protection Code. Every organization was supposed to draw up, update yearly and obviously deploy a DPS. Table 3 shows an item-by-item comparison of the DPS enacted by the University of Trento and ISO-17799.

3 University of Trento: Information System & Organization

Personal data are processed within University for institutional purposes: education and research. The University has enforced the Data Protection Act through a Privacy Internal Regulation on January 14th, 2002 that transposed general regulations into its internal organization: it sets the responsibility line relating to personal data processing from data controller, the Chancellor, through data processors identified with Faculty Deans, Heads of Department and Central Directorate Managers down to data processing operators. Every data processor is responsible on behalf of the controller to accomplish the obligations relating to personal data processed within its own organization, supported by the ICT Directorate with regard to the adoption of the minimal precautionary security measures for electronic data processing.

Central Administrative Directorates (where the bulk of data processing is done) manage and coordinate all activities to support education and research. The Data Controller is identified with the Chancellor and all administrative executive directors are Data Processor within their own Directorate. Within the University, we have 10 Directorates: Chancellorship, General, Governance Relations, HR, Budget and Finance, Student Affairs and University Relations, ICT, Facilities Services, Library, Rovereto Administrative[1].

The Chief Executive Officer (CEO) has a special coordinating role within University on behalf of the Chancellor to accomplish all obligations related to personal data processing. The Chief Information Officer (CIO) is responsible for the adoption of the minimal and suitable precautionary security measures for electronic personal data processing.

The ICT Directorate manages the IT systems. The substructures in charge of Information Systems and Network, manage all central information services and network infrastructure whereas the local systems and services are managed by ICT local garrisons. Based on the University Privacy Internal Regulation, the CIO is responsible to draw up and to update the DPS and to implement the minimal and suitable security measures. Furthermore, he designates Database Security Operators and Network Security Operators within central structure and local garrisons.

Williams [23] proposes a maturity model to establish rankings for security in an organization (Table 2). Matched against this scale, the University of Trento can be ranked between 3 and 4. In particular 4(a) is not yet enforced whereas 4(b) and 4(c) are (almost entirely) enforced[2].

4 Security-Aware Tropos

Tropos [8] is an agent-oriented software development methodology, tailored to describe both the organization and the system. In Tropos, one can capture not only the *what* or the *how*, but also the *why* a piece of software is developed. This allows a more refined analysis of the system's functional requirements, and also of the non-functional requirements such as security.

[1] The University has a subsidiary in another city.

[2] Security awareness briefings are restricted to technical staff whereas non-technical staff only receive notifications in occasion of major virus and worm attacks. Intrusion testing is still amateurish.

Table 2: Maturity of information risk management

Maturity Level	Description
0	**Non-Existent: management processes are not applied at all**
	(a) No risk assessment of processes or business decisions. The organization does not consider the business impact associated with security vulnerabilities. Risk management has not been identified as relevant to IT solutions and services;
	(b) The organization does not recognize the need for IT security. Responsibilities and accountabilities for security are not assigned. Measures supporting the management of IT security are not implemented. There is no IT security reporting or response process for IT security breaches. No recognizable security administration processes exist;
	(c) No understanding of the risks, vulnerabilities and threats to IT operations or service continuity by management.
1	**Initial/Ad-Hoc: processes are ad-hoc and disorganized**
	(a) The organization considers IT risks in an ad-hoc manner, without following defined processes or policies. Informal project based risk assessment is used;
	(b) The organization recognizes the need for IT security, but security awareness depends on the individual. IT security is reactive and not measured. IT security breaches invoke "finger pointing" responses if detected, because responsibilities are unclear. Responses to IT security breaches are unpredictable;
	(c) Responsibilities for continuous service are informal, with limited authority. Management is becoming aware of the risks related to and the need for continuous service.
2	**Repeatable but intuitive: processes follows a regular pattern**
	(a) There is an emerging understanding that IT risks are important and need to be considered. Some approach to risk assessment exists, but the process is still immature and developing;
	(b) Responsibilities and accountabilities for IT security are assigned to an IT security coordinator with no management authority. Security awareness is fragmented and limited. Security information is generated, but is not analyzed. Security tends to respond reactively to incidents and by adopting third-party offerings, without addressing the specific needs of the organization. Security policies are being developed, but inadequate skills and tools are still being used. IT security reporting is incomplete or misleading;
	(c) Responsibility for continuous service is assigned. Fragmented approach to continuous service. Reporting on system availability is incomplete and does not take business impact into account.
3	**Defined Process: processes are documented and communicated**
	(a) An organization-wide risk management policy defines when and how to conduct risk assessments. Risk assessment follows a defined process that is documented and available to all staff;
	(b) Security awareness exists and is promoted by management through formalized briefings. IT security procedures are defined and fit into a structure for security policies and procedures. Responsibilities for IT security are assigned, but not consistently enforced. An IT security plan exists, driving risk analysis and security solutions. IT security reporting is IT focused, rather than business focused. Ad-hoc intrusion testing is performed.
	(c) Management communicates consistently the need for continuous service. High-availability components and system redundancy are being applied piecemeal. An inventory of critical systems and components is rigorously maintained.
4	**Managed and Measurable: processes are monitored and measured**
	(a) The assessment of risk is a standard procedure and exceptions would be noticed by IT management. It is likely that IT risk management is a defined management function with senior level responsibility. Senior management and IT management have determined the levels of risk that the organization will tolerate and have standard measures for risk/return ratios;
	(b) Responsibilities for IT security are clearly assigned, managed and enforced. IT security risk and impact analysis is consistently performed. Security policies and practices are completed with specific security baselines. Security awareness briefings, user identification, authentication and authorization have become mandatory and standardized. Intrusion testing is standardized and leads to improvements. Cost/benefit analysis, is increasingly used. Security processes are coordinated with the overall organization security function and reporting is linked to business objectives;
	(c) Responsibilities and standards for continuous service are enforced. System redundancy practices, including use of high-availability components, are being consistently deployed.
5	**Optimized-best practices are followed and automated**
	(a) Risk assessment has developed to the stage where a structured, organization- wide process is enforced, followed regularly and well managed;
	(b) IT security is a joint responsibility of business and IT management and integrated with corporate business objectives. Security requirements are clearly defined, optimized and included in a verified security plan. Functions are integrated with applications at the design stage and end users are increasingly accountable for managing security. IT security reporting provides early warning of changing and emerging risk, using automated active monitoring approaches for critical systems. Incidents are promptly addressed with formalized incident response procedures supported by automated tools. Periodic security assessments evaluate the effectiveness of implementation of the security plan. Information on new threats and vulnerabilities is systematically collected and analyzed, and adequate mitigating controls are promptly communicated and implemented. Intrusion testing, root cause analysis of security incidents and proactive identification of risk is the basis for continuous improvements. Security processes and technologies integrated organization wide.
	(c) Continuous service plans and business continuity plans are integrated, aligned and routinely maintained. Buy-in for continuous service needs is secured from vendors and major suppliers.

Here we use Security-Enhanced Tropos [13]. We have the concepts of actor, goal, soft goal, task, resource and social relationships for defining the obligations of actors to other actors. Actors have strategic goals and intentions within the system or the organization. A goal represents the strategic interests of an actor. A task specifies a particular course of action that produces a desired effect, and can be executed in order to satisfy a goal. A resource represents a physical or an informational entity. The relationships we have considered so far are functional dependency, ownership, provisioning, trust, and delegation of permission. A functional dependency between two actors means that the dependee will take responsibility for fulfilling the functional goal of a depender. The owner of a service has full authority concerning access and usage of his services, and he can also delegate this authority to other actors. Delegation marks a formal passage between the actors. In contrast, trust marks simply a social relationship that is not formalized by a "contract" between the actors: such as a digital credential or a signed piece of paper attributing permission.

Various activities contribute to the acquisition of a first requirement model, to its refinement into subsequent models:

Actor modeling, which consists of identifying and analyzing both the actors of the environment and the system's actors and agents;

Dependency modeling, which consists of identifying actors which depend on one another for goal be achieved, plans to be performed, and resources to be furnished, and actors which are able to provide goal, plans, and resources.

Trust modeling, which consists of identifying actors which trust other actor for goal, plans, and resources, and actors which own goal, plans, and resources.

Delegation modeling, which consists of identifying actors which delegate to other actors the permission on goals, plans, and resources.

Goal refinement, which consists of refining requirements and eliciting new relations. This is standard in Goal-Oriented Methodologies [8].

A graphical representation of the model obtained following the first four modeling activities is given through three different kinds of *actor diagrams*: *functional dependency model*, *trust model*, and *trust management implementation*. In these diagrams, actors are represented as circles; goals, tasks and resources are respectively represented as ovals, hexagons and rectangles.

Once the stakeholders and their goals and social relations have been identified, the analysis tries to enrich the model with more details. Goal refinement aims to analyze any goals of each actor, and is conducted from the perspective of the actor itself by using AND/OR decomposition. A graphical representation of goal refinement is given through *goal diagrams*. The outcome of this phase is a set of social relations among actors, defined incrementally by performing goal refinement on each goal, until all goals have been refined. Goal refinement builds goal hierarchies where lower goals are more specific and are motivated by goals higher in the hierarchy.

5 Modelling Actors

The first activity in the early requirements phase is actors' modeling. This phase consists of identifying and analyzing the application domain stakeholders and their intentions as social actor which want to achieve goals.

In our example we can start by informally listing some of them. The following definitions[3] apply and shall be used in this paper:

[3] See Article 2 "Definitions" of EU Directive 95/46/EC.

Data Controller is the natural or legal person which determines the purposes and means of the processing of personal data. In the University, the data controller is identified with Chancellor (as the post-holder is also the legal representative of the University).

Data Processor is a natural or legal person which monitors personal data processing on behalf of the controller. In the University, based on the enacted regulations, data processors are identified with:

- Faculty Deans;
- Heads of Department;
- Central Directorate Managers, and in particular with:
  - Chief Executive Officer (CEO);
  - Chief Information Officer (CIO).

Data Processing Operator is the human appointed by the data controller or processor to perform the operations related to the data processing or to manage and maintain the information systems and services. At University of Trento, these are identified with:

- Personal Data Processing Operator;
- Database Security Operator;
- Network Security Operator.

Data Subject is the natural or legal person to whom the personal data are related. In the Secure Tropos terminology, this is the legitimate owner of the data.

CERT (Computer Emergency Response Team) is composed by:

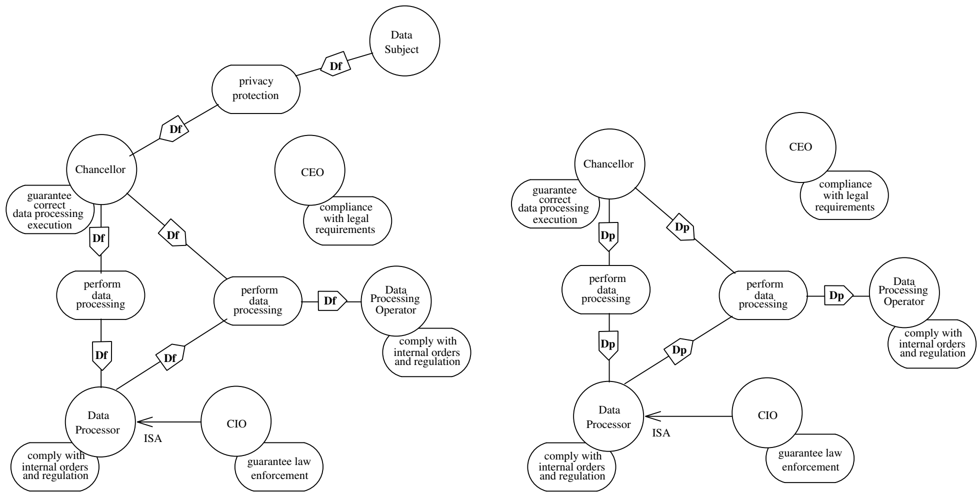
- the staff of ATI Network that manages the network infrastructure and services of the University;
- the Information Security Office Manager;
- the CIO.

To be more precise CERT includes a member in charge of security issues for every major ICT service center in the University.

In the underlying formal model based on datalog instances of actors are represented as constants satisfying atomic predicates for actors' types (e.g. being Chancellor) and binary predicates are used to link agents and goals.

6 Modelling Dependencies and Delegation

The analysis proceeds introducing the functional dependencies and the delegation of permission between actors and the consequent integrated security and functional requirements. Figure 1(a) and Figure 1(b) show the functional dependency model and the trust management implementation. We use delegation of permission (**Dp**) to model the actual transfer of rights in some form (e.g. a digital certificate, a signed paper, etc.), and **Df** for functional dependency.


Data Subject
Df
privacy protection
Df
Chancellor
guarantee correct data processing execution
CEO
compliance with legal requirements
Df
Df
perform data processing
perform data processing
Df
Data Processing Operator
comply with internal orders and regulation
Df
Df
Data Processor
ISA
CIO
comply with internal orders and regulation
guarantee law enforcement
Chancellor
CEO
compliance with legal requirements
guarantee correct data processing execution
Dp
Dp
perform data processing
perform data processing
Dp
Data Processing Operator
comply with internal orders and regulation
Dp
Dp
Data Processor
ISA
CIO
comply with internal orders and regulation
guarantee law enforcement

(a) Functional Dependency Model (b) Trust Management Implementation

Figure 1: Actor Diagrams

In the functional dependency model, *Chancellor* is associated with a single relevant goal: *guarantee correct data processing execution*, while *CEO* has an associated goal *compliance with legal requirements*. Along similar lines, *Data Processor* and *Data Processing Operator* want to *comply with internal orders and regulation*, while *CIO*, wants to *guarantee law enforcement*. Finally, the diagram includes some functional dependencies: *Data Subject* depends on *Chancellor* for *privacy protection* goal; *Chancellor* depends on *Data Processor* and *Data Processing Operator* to *perform data processing*; and, in turn, *Data Processor* depends on *Data Processing Operator* for it.

In the trust management implementation, following the current practice *Chancellor* delegates permissions to *perform data processing* to *Data Processor* and *Data Processing Operator*. In turn, *Data Processor* delegates permissions to *perform data processing* to *Data Processing Operator*.

At this stage, the analysis already reveals a number of pitfalls in the actual document template provided by the ministry's agency. The most notable one is the absolute absence of functional dependencies between the Chancellor and the CEO, who is actually the one who runs the administration. Such functional dependency is present in the Universities statutes, but not here (an apparently unrelated document).

Another missing part in the trust management implementation is the delegation of permission from the data subject. This can be also automatically spotted with the techniques developed in [13]. Somehow paradoxically (for a document template enacted in fulfillment of a Data Protection Act) the process of acquisition of data (and the relative authorization) is neither mentioned nor forseen. In practice this gap is solved by the University by a blanket authorization: in all the paper or electronic data collection steps a signature is required to authorize the processing of data in compliance with the privacy legislation.

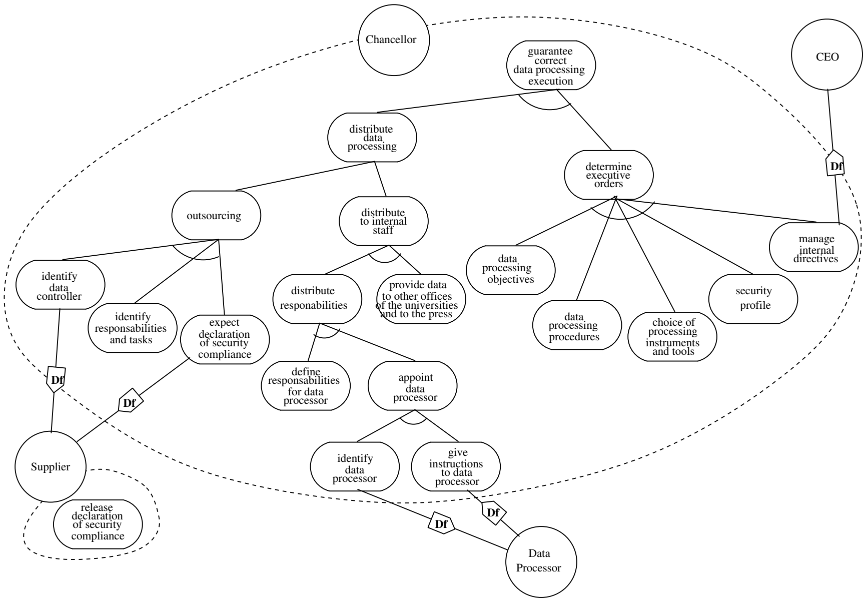

Chancellor
guarantee correct data processing execution
CEO
distribute data processing
determine executive orders
Df
outsourcing
distribute to internal staff
manage internal directives
data processing objectives
identify data controller
distribute responabilities
provide data to other offices of the universities and to the press
security profile
identify responsabilities and tasks
expect declaration of security compliance
data processing procedures
choice of processing instruments and tools
Df
define responsabilities for data processor
appoint data processor
Df
Supplier
identify data processor
give instructions to data processor
release declaration of security compliance
Df
Df
Data Processor

Figure 2: Functional Dependency Model for Chancellor

7 Goal Refinement

A first example of the goal refinement is given by the goal diagram depicted in Figure 2 for the *Chancellor*. The goal *guarantee correct data processing execution* is decomposed into *distribute data processing* and *determine executive orders*. We call this a "AND-decomposition". The goal *distribute data processing* is decomposed (OR-decomposition) into two subgoals: *outsourcing* and *distribute to internal staff*.

The security requirements of an organization outsourcing the management and control of all or some of its information system is addressed in a contract agreed between the parties. For example, the contract should address: how the legal requirements are to be met, e.g. data protection legislation; what arrangements will be in place to ensure that all parties involved in the outsourcer, including subcontractors, are aware of their security responsibilities; how the integrity and confidentiality of the organization's business assets are to be maintained and tested; etc. In a nutshell the contract should say that the goal *guarantee correct data processing execution* is also fulfilled by the service supplier. The contract should allow the security requirements and procedures to be expanded in a security management plan to be agreed between the two parties. Following these requirements, the goal *outsourcing* is AND-decomposed into *identify data controller*, *identify responsibilities and tasks*, and *expect declaration of security compliance*.

The other hand, the goal *distribute to internal staff* is decomposed into *distribute responsibilities* and *provide data to other offices of the university and to press. Distribute responsibilities* consists into *define responsibilities for data processor* and *appoint data processor*. Since security roles and responsibilities should include implementing or maintaining security policy as well as any specific responsibilities for the protection of particular assets, or for the execution of particular security processes or activities, the goal *determine executive orders* is AND-decomposed into five subgoals: *data processing objectives*, *data processing procedures*, *choice of processing instruments and tools*, *security profile*, and *manage internal directives* for which *Chancellor* depends on *CEO*. Note here

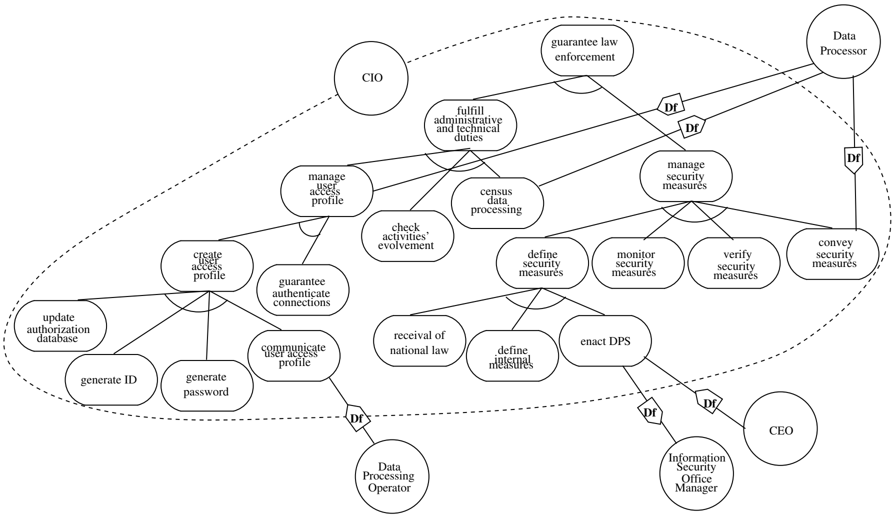

CIO
guarantee law enforcement
Data Processor
fulfill administrative and technical duties
Df
Df
Df
manage user access profile
census data processing
manage security measures
check activities' evolvement
create user access profile
guarantee authenticate connections
define security measures
monitor security measures
verify security measures
convey security measures
update authorization database
generate ID
generate password
communicate user access profile
receival of national law
define internal measures
enact DPS
Df
Df
Df
CEO
Data Processing Operator
Information Security Office Manager

Figure 3: Functional Dependency Model for CIO

the gap: everything is “formally” decided by *Chancellor* and only the final executive regulations are delegated to the *CEO*. Only in theory objectives, procedures, processing instruments and security profile are defined by *Chancellor*, whereas they are just enacted by him.

A second example, in Figure 3, shows the goal analysis for CIO, relative to the goal *guarantee law enforcement*. This goal is decomposed into *fulfill administrative and technical duties* and *manage security measures*. The goal *fulfill administrative and technical duties* is decomposed into three goals: *manage user access profile* for which *Data Processor* depends on *CIO*, *check activities' evolvement*, and *census data processing* for which *CIO* depends on *Data Processor*. The goal *manage user access profile* is decomposed into *create user access profile* and *guarantee authenticate connections*. The goal *create user access profile* is decomposed into *update authorization database*, *generate ID*, *generate and retrieve password*,[4] and *communicate user access profile* for which *Data Processing Operator* depends on *CIO*. The goal *manage security measures* is decomposed into *define security measures*, *monitor security measures*, *verify security measures*, and *convey security measures* for which *Data Processor* depends on *CIO*. Essentially this map the formal requirements that a policy document should be approved by management, published and communicated, as appropriate, to all employees.

The goal diagram in Figure 4 shows the trust management implementation for *Chancellor* with respect to goal *guarantee correct data processing execution*. In particular, it points out that *Supplier* delegates a signed *declaration of security compliance* to *Chancellor* where *Supplier* engages in honoring and enforcing the undertaken responsibilities. This map the formal requirements that the University has security policies that requires adherence to several necessary precautions in order to maintain *privacy protection* in behalf of *Data Subject*. Further, *Chancellor* delegates *mail within instructions* to *Data Processor* and *executive orders list* to *CEO*.

Figure 5 shows the trust management implementation for *CIO*. The diagram displays that *Data Processor* delegates *data processing list* to *CIO* for census. Further, *CIO* delegates *ID*, *password* and *user access profile* to *Data Processing Operator*.

[4] The procedure also includes some fuzzy steps on something that is a security anathema (helping users who forgot their password) but a fairly frequent problem.

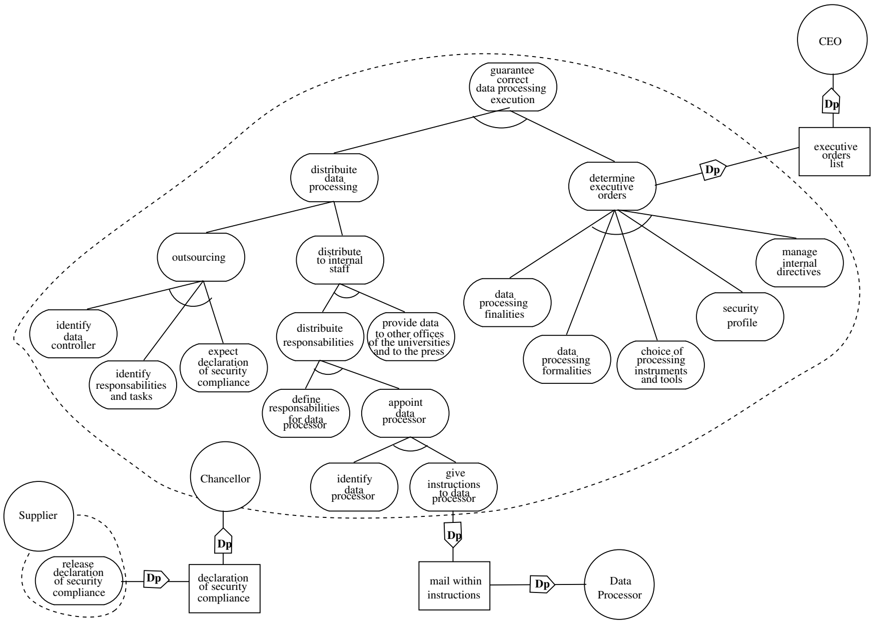

CEO
Dp
executive orders list
guarantee correct data processing execution
distribuite data processing
determine executive orders
Dp
outsourcing
distribute to internal staff
manage internal directives
data processing finalities
security profile
identify data controller
expect declaration of security compliance
identify responsabilities and tasks
distribuite responsabilities
provide data to other offices of the universities and to the press
data processing formalities
choice of processing instruments and tools
define responsabilities for data processor
appoint data processor
identify data processor
give instructions to data processor
Chancellor
Supplier
Dp
Dp
release declaration of security compliance
Dp
declaration of security compliance
mail within instructions
Dp
Data Processor

Figure 4: Trust Management Implementation for Chancellor

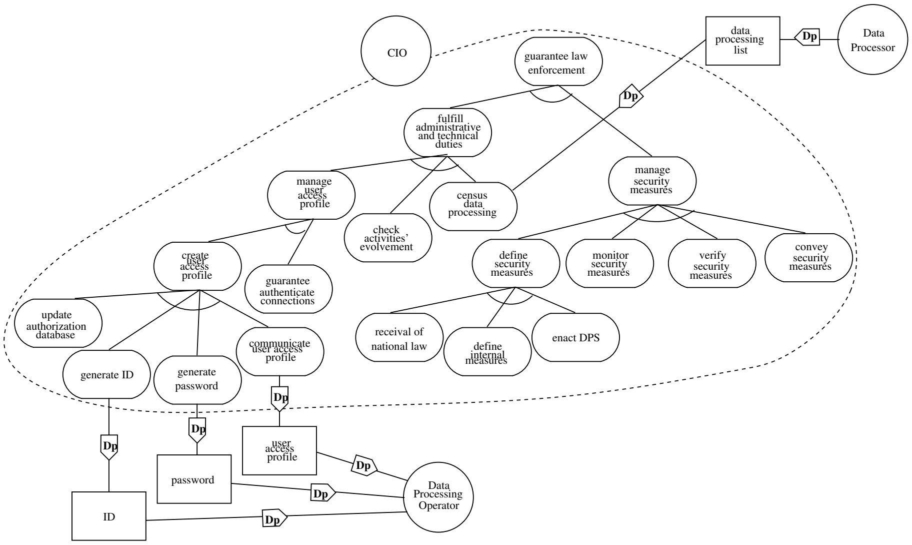


Figure 5: Trust Management Implementation for CIO

The model has been further refined down to the the various offices and members of staff until it could be matched one-one with the actual DPS. Next, we present other diagrams for the some actors involved in the system. Figures 6 and 7 show, respectively, functional dependency model and trust management implementation for Data Processor relative to the goal *comply with internal orders and regulation*. Figures 8 and 9 show, respectively, the goal refinement of the functional dependency model and the trust management implementation for Data Processing Operator, relative to the goal *comply with internal orders and regulation*, and for Database Security Operator, relative to

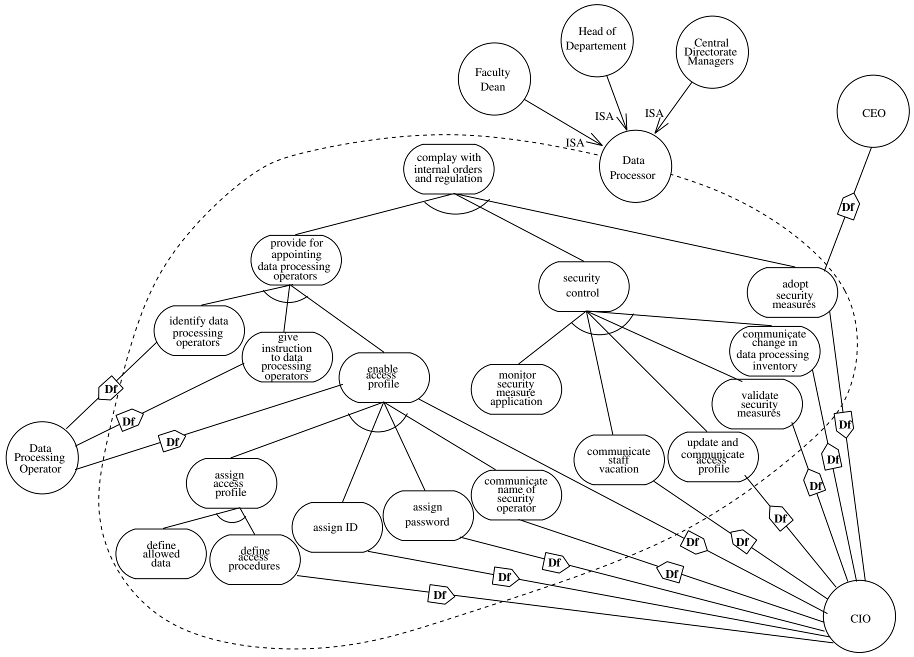

Head of Departement
Central Directorate Managers
Faculty Dean
ISA
ISA
ISA
CEO
Data Processor
complay with internal orders and regulation
Df
provide for appointing data processing operators
security control
adopt security measures
identify data processing operators
give instruction to data processing operators
enable access profile
monitor security measure application
communicate change in data processing inventory
validate security measures
Df
Df
Df
Df
Data Processing Operator
Df
communicate staff vacation
update and communicate access profile
Df
Df
assign access profile
communicate name of security operator
Df
assign ID
assign password
Df
Df
Df
define allowed data
define access procedures
Df
Df
Df
CIO

Figure 6: Functional Dependency Model for Data Processor

the goal *manage and maintain ICT instruments and tools*.

The goal diagrams in Figure 10(a) and 10(b) show, respectively, functional dependency model and trust management implementation for Data Subject. The functional dependency model reveals that *Data Subject* depends on *Chancellor* to *get informative*, and that *Chancellor* depends on *Data Subject* for the consensus needed for performing data processing. The trust implementation model displays that *Chancellor* delegate *informative* to *Data Subject*, and *Data Subject* delegate *consensus* to *Chancellor*.

Figure 11 shows the goal refinement for CEO, relative to the goal *compliance with legal requirements*. The goal diagrams in Figure 12 shows the functional dependency model for CERT, relative to the goal *co-ordinate response activities for security incidents*, and for Information Security Office Manager, relative to the goal *manage information security and privacy matters*. The trust implementation model for CEO and CERT is not shown since it is not defined in the DPS.

8 Adequacy and Analysis of the Model

The primitives suggested for Secure Tropos were sufficient to cope with the complexity of a real ISO-17799-like case study and the methodology allowed to pinpoint many issues.

For example, the first observation is that a trust model is not considered in the required procedures and documents. Trust relations are implicitly defined in the employment contract that actors draw up with the University. In absence of such model, some of the properties proposed in [13] cannot be verified since trust is at the base of such framework. Note also that, in according with the Code, data subjects own their personal data. In [13], we suggest to check if employees who are entitled to access to Personal data, have previously gotten the permission from data subjects for them. In above models, this is not verified since there is not delegation from data subjects to

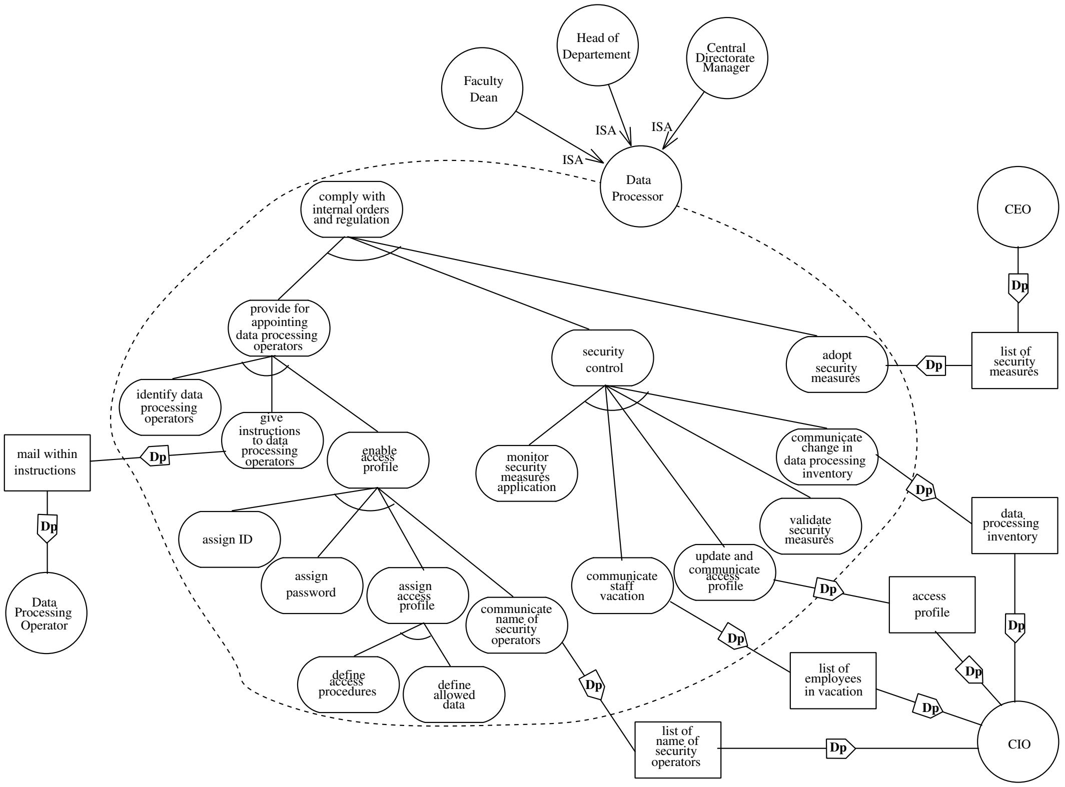

Head of Departement
Central Directorate Manager
Faculty Dean
ISA
ISA
ISA
Data Processor
CEO
comply with internal orders and regulation
Dp
provide for appointing data processing operators
security control
adopt security measures
Dp
list of security measures
identify data processing operators
give instructions to data processing operators
enable access profile
monitor security measures application
communicate change in data processing inventory
mail within instructions
Dp
Dp
Dp
data processing inventory
validate security measures
Dp
assign ID
assign password
assign access profile
communicate name of security operators
communicate staff vacation
update and communicate access profile
Dp
access profile
Dp
Data Processing Operator
Dp
list of employees in vacation
Dp
Dp
define access procedures
define allowed data
Dp
list of name of security operators
Dp
CIO

Figure 7: Trust Management Implementation for Data Processor

employees for personal data. Essentially we only have a blanket authorization.

Further, DPS defines only objectives and responsibilities for the entities involved into the organization, but does not identify who is really able to provide services. This entails that some relations among entities could miss. For example, looking at Figure 3 and 5, the CIO has the responsibilities to manage user access profile. In practice, he delegates the execution of this goal to an employee of the ICT Directorate that generates IDs and passwords, and then delegates them to data processing operators. Consequently, it is not possible capture requirements of availability unless an explicit model of the functional requirements is also given. For instance, we cannot verify whether data subjects delegate their personal data only to someone that is able to provide the requested service. This clashes with privacy principles and, specifically, with the notion of "limited collection": the collection of personal information should be limited to the minimum necessary for accomplishing the specified service.

Notice that this is not a problem of the University of Trento, but rather of the entire security assessment procedure in the state of the art: unless the ISO-17799 policy (or its equivalent DPS) is matched by a description of the functional goals of the organization it is not possible to conclude whether access is fair or respect least privileges principles. The same problem affects EPAL proposals [5, 6] and other privacy proposals in the literature [1, 2, 9, 16].

The most painful (and so far not formally analyzed part) is the treatment of manual non-ICT procedures. This difficulty steams from two main sources. The first one is that non-ICT procedures are often not completely formalized since there is no need for "programming" and "debugging" a

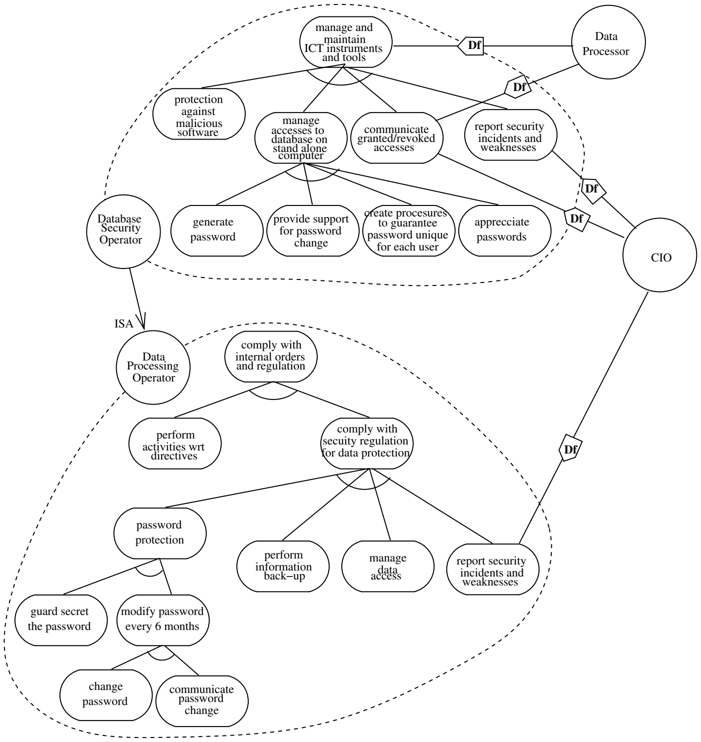

manage and maintain ICT instruments and tools
Df
Data Processor
protection against malicious software
Df
manage accesses to database on stand alone computer
communicate granted/revoked accesses
report security incidents and weaknesses
Df
Df
Database Security Operator
generate password
provide support for password change
create procesures to guarantee password unique for each user
apprecciate passwords
CIO
ISA
Data Processing Operator
comply with internal orders and regulation
perform activities wrt directives
comply with secuity regulation for data protection
Df
password protection
perform information back–up
manage data access
report security incidents and weaknesses
guard secret the password
modify password every 6 months
change password
communicate password change

Figure 8: Functional Dependency Model for Data Processing Operator

human. This does not means that offices do not follow standard procedures but rather that these procedures are somehow "embedded" in the organization or the "office distributed knowledge". In absence of fully formalized functional procedures it is difficult to define the corresponding authorization and trust management procedures.

9 Related Case Studies and Conclusions

The last years have seen an increasing awareness that security and privacy play a key role in system development and deployment. This awareness has been matched by a number of research proposals on incorporating security and privacy considerations into the mainstream requirement and software engineering methodologies. Yet, only few papers describe complex case studies.

Becker et al. [7] use Cassandra to model and analyze an access control policy for a national electronic health record system. The background of this case study is the British National Health Service's current plan to develop an electronic data spine that will contain medical data for all patients in England. The proposed policies contain a total of 310 rules and define 58 parameterized roles.

In [3], Antòn et al. introduces a privacy goal taxonomy and reports the analysis of 23 Internet privacy policies for companies in three health care industries: pharmaceutical, health insurance and on-line drugstores. The identified goals are used to discover inner internal conflicts within privacy policies and conflicts with the corresponding websites and their manner of manage customers' personal data.

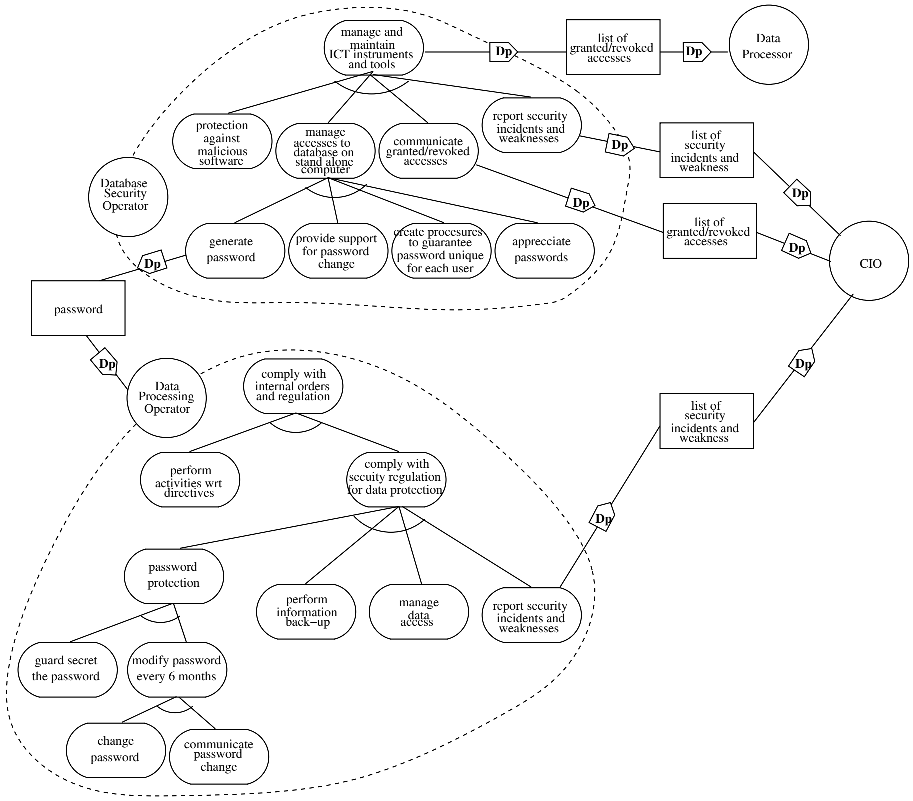
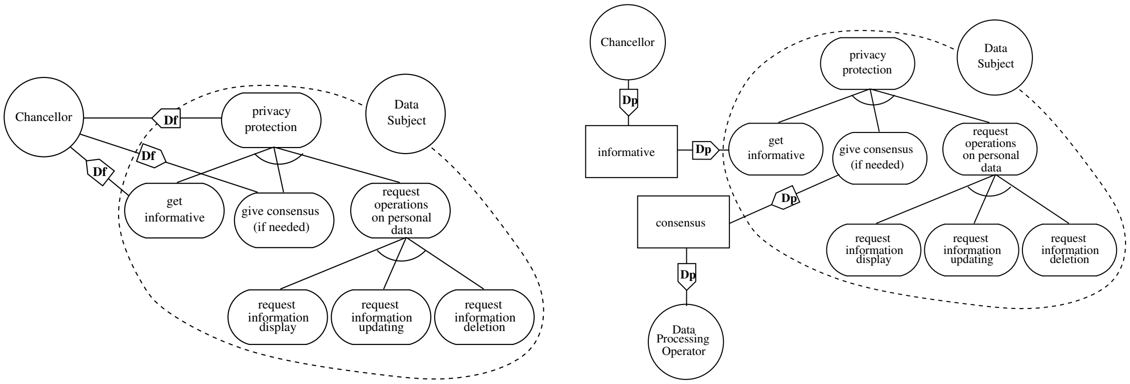

manage and maintain ICT instruments and tools
Dp
list of granted/revoked accesses
Dp
Data Processor
protection against malicious software
manage accesses to database on stand alone computer
communicate granted/revoked accesses
report security incidents and weaknesses
Dp
list of security incidents and weakness
Dp
Database Security Operator
Dp
list of granted/revoked accesses
Dp
CIO
generate password
provide support for password change
create procesures to guarantee password unique for each user
apprecciate passwords
Dp
password
Dp
Data Processing Operator
comply with internal orders and regulation
Dp
list of security incidents and weakness
perform activities wrt directives
comply with secuity regulation for data protection
Dp
password protection
perform information back−up
manage data access
report security incidents and weaknesses
guard secret the password
modify password every 6 months
change password
communicate password change

Figure 9: Trust Management Implementation for Data Processing Operator


Chancellor
Df
privacy protection
Data Subject
Df
Df
get informative
give consensus (if needed)
request operations on personal data
request information display
request information updating
request information deletion
Chancellor
Dp
privacy protection
Data Subject
informative
Dp
get informative
give consensus (if needed)
request operations on personal data
consensus
Dp
request information display
request information updating
request information deletion
Dp
Data Processing Operator

(a) Functional Dependency Model

(b) Trust Management Implementation

Figure 10: Diagrams for Data Subject

A study of the certification of information security management systems based on specifications promulgated by Taiwan's Ministry of Economic Affairs is proposed in [11]. In particular, this work shows the ability of Taiwan's information security management systems to meet the requirements proposed in international standards. In [10], authors analyze the knowledge and skills required

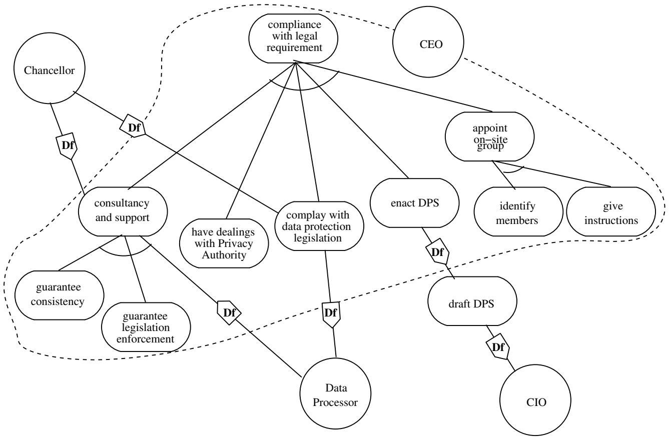


Figure 11: Functional Dependency Model for CEO

for auditing the certification procedures for asset, threat, and vulnerability. They recognize that reducing risks is the target of information security management system protection mechanism. Thus, risk assessment is need to analyze the threats to and vulnerabilities of information systems and the potential impact of harm that the loss of confidentiality, integrity, or availability would have on an agency's operations and assets.

In this paper we have shown the Secure Tropos methodology at work on a real-life comprehensive case study encompassing on ISO-17799 security management policy. The proposed constructs and methodology were up the challenge and revealed a number of pitfalls, especially when the formal analysis techniques were applied.

Future work is in the full automated analysis of the policy at the level of individual staff members processing data.

References

[1] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu. Hippocratic Databases. In *Proceedings of the 28th International Conference on Very Large Data Bases (VLDB'02)*, pages 143–154, 2002.

[2] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu. An Implementation of P3P Using Database Technology. In *Proceedings of the 9th International Conference on Extending Database Technology*, volume 2992 of *Lecture Notes in Computer Science*, pages 845–847. Springer-Verlag, 2004.

[3] A. I. Antòn and J. B. Earp. A requirements taxonomy for reducing Web site privacy vulnerabilities. *Requirements Engineering*, 9(3):169–185, 2004.

[4] A. I. Antòn, J. B. Earp, and A. Reese. Analyzing Website privacy requirements using a privacy goal taxonomy. In *Proceedings of the 10th IEEE International Requirements Engineering Conference (RE'02)*, pages 23– 31. IEEE Computer Society Press, 2002.

[5] M. Backes, G. Karjoth, W. Bagga, and M. Schunter. Efficient comparison of enterprise privacy policies. In *Proceedings of the 2004 ACM Symposium on Applied Computing*, 2004.

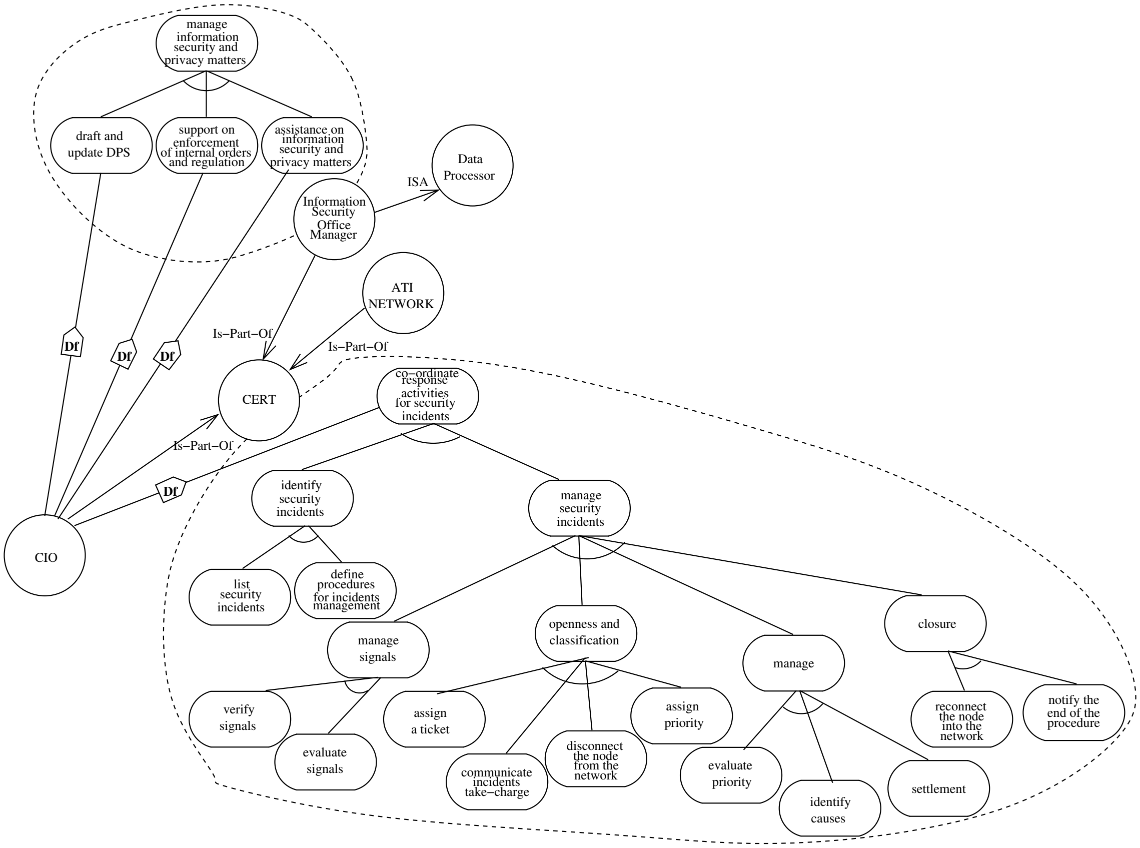

manage information security and privacy matters
draft and update DPS
support on enforcement of internal orders and regulation
assistance on information security and privacy matters
Data Processor
ISA
Information Security Office Manager
ATI NETWORK
Is–Part–Of
Is–Part–Of
Df
Df
Df
CERT
co–ordinate response activities for security incidents
Is–Part–Of
Df
identify security incidents
manage security incidents
CIO
list security incidents
define procedures for incidents management
closure
openness and classification
manage signals
manage
verify signals
evaluate signals
assign a ticket
assign priority
reconnect the node into the network
notify the end of the procedure
communicate incidents take–charge
disconnect the node from the network
evaluate priority
identify causes
settlement

Figure 12: Functional Dependency Model for CERT

[6] M. Backes, B. Pfitzmann, and M. Schunter. A Toolkit for Managing Enterprise Privacy Policies. In *Proceedings of the 8th European Symposium on Research in Computer Security*, volume 2808 of *Lecture Notes in Computer Science*, pages 162–180. Springer-Verlag, 2003.

[7] M. Y. Becker and P. Sewell. Cassandra: flexible trust management, applied to electronic health records. In *Proceedings of the 17th IEEE Computer Society Security Foundations Workshop*, pages 139–154. IEEE Computer Society Press, 2004.

[8] P. Bresciani, P. Giorgini, F. Giunchiglia, J. Mylopoulos, and A. Perini. TROPOS: An Agent-Oriented Software Development Methodology. *Journal of Autonomous Agents and Multi-Agent Systems*, 8(3):203–236, 2004.

[9] L. Cranor, M. Langheinrich, M. Marchiori, and J. Reagle. The Platform for Privacy Preferences 1.0 (P3P1.0) Specification. W3C Recommendation, Apr. 2002.

[10] K.-J. Farn, S.-K. Lin, and A. R.-W. Fung. A study on information security management system evaluationassets, threat and vulnerability. *Computer Standards and Interfaces*, 26(6):501–513, 2004.

[11] A. R.-W. Fung, K.-J. Farn, and A. C. Lin. Paper: a study on the certification of the information security management systems. *Computer Standards and Interfaces*, 25(5):447–461, 2003.

[12] P. Giorgini, F. Massacci, J. Mylopoulous, and N. Zannone. Filling the gap between Requirements Engineering and Public Key/Trust Management Infrastructures. In *Proceedings of the 1st European PKI Workshop: Research and Applications*, volume 3093 of *Lecture Notes in Computer Science*, pages 98–111. Springer-Verlag, 2004.

[13] P. Giorgini, F. Massacci, J. Mylopoulous, and N. Zannone. Requirements Engineering meets Trust Management: Model, Methodology, and Reasoning. In *Proceedings of the Second International Conference on Trust Management*, volume 2995 of *Lecture Notes in Computer Science*, pages 176–190. Springer-Verlag, 2004.

[14] ISO/IEC. Information technology – Code of practice for information security management. ISO/IEC 17799, 2000.

[15] J. Jürjens. *Secure Systems Development with UML*. Springer-Verlag, 2004.

[16] G. Karjoth, M. Schunter, and M. Waidner. Platform for Enterprise Privacy Practices: Privacy-enabled Management of Customer Data. In *Proceedings of the 2nd Workshop on Privacy Enhancing Technologies*, Lecture Notes in Computer Science. Springer-Verlag, 2002.

[17] L. Liu, E. S. K. Yu, and J. Mylopoulos. Security and Privacy Requirements Analysis within a Social Setting. In *Proceedings of the 11th IEEE International Requirements Engineering Conference (RE'03)*, pages 151–161. IEEE Computer Society Press, 2003.

[18] F. Massacci, M. Prest, and N. Zannone. Using a Security Requirements Engineering Methodology in Practice: The compliance with the Italian Data Protection Legislation. *Computer Standards & Interfaces*, 2004. To appear.

[19] J. McDermott and C. Fox. Using Abuse Case Models for Security Requirements Analysis. In *Proceedings of 15th Annual Computer Security Applications Conference*, pages 55–66. IEEE Computer Society Press, 1999.

[20] G. Sindre and A. L. Opdahl. Eliciting Security Requirements by Misuse Cases. In *Proceedings of TOOLS Pacific 2000*, pages 120–131. IEEE Computer Society Press, 2000.

[21] A. Toval, A. Olmos, and M. Piattini. Legal requirements reuse: a critical success factor for requirements quality and personal data protection. In *Proceedings of the 10th IEEE International Requirements Engineering Conference (RE'02)*, pages 95 –103. IEEE Computer Society Press, 2002.

[22] A. van Lamsweerde, S. Brohez, R. De Landtsheer, and D. Janssens. From System Goals to Intruder Anti-Goals: Attack Generation and Resolution for Security Requirements Engineering. In *Proceedings of International Workshop on Requirements for High Assurance Systems (RHAS 2003)*, pages 49–56, 2003.

[23] P. Williams. Information Security Governance. *Information Security Technical Report*, 6(3):60–70, 2001.

A Comparing ISO-17799 and DPS 3.0

Table 3: Comparing ISO-17799 and DPS 3.0

ISO/IEC 17799 2000 **“Code of Practice for Information Security Management”**	**DPS 3.0** according Italian D.Lgs n.196/2003 **“Programmatic Security Document”**
INTRODUCTION what is information security?, why information security is needed, how to establish security requirements, assessing security risks, selecting controls, information security starting point, critical success factors, developing your own guidelines	**1 INTRODUCTION**
1 SCOPE	**3 SCOPE**
2 REFERENCES	**2 REFERENCES**
3 TERMS AND DEFINITIONS	Not implemented
4 SECURITY POLICY	**4 INFORMATION SECURITY POLICY**
4.1 INFORMATION SECURITY POLICY 4.1.1 Information security policy document 4.1.2 Review and evaluation	
5 ORGANIZATIONAL SECURITY	6.3 ORGANIZATIONAL SECURITY 6.3.1 Actors provided for law 6.3.2 ICT Directorate Limited to privacy
5.1 INFORMATION SECURITY INFRASTRUCTURE 5.1.1 Management information security forum 5.1.2 Information security co-ordination 5.1.3 Allocation of information security responsibilities 5.1.4 Authorization process for information processing facilities 5.1.5 Specialist information security advice 5.1.6 Co-operation between organizations 5.1.7 Independent review of information security	
5.2 SECURITY OF THIRD PARTY ACCESS 5.2.1 Identification of risks from third party access 5.2.2 Security requirements in third party contracts	6.3.8 Security requirements in outsourcing contracts
5.3 OUTSOURCING 5.3.1 Security requirements in outsourcing contracts	
6 ASSET CLASSIFICATION AND CONTROL	**5 ASSET CLASSIFICATION AND CONTROL** - Annex 1 Facsimile for inventory of Server Systems - Annex 2 Facsimile for inventory of Software Systems - Annex 3 Facsimile for inventory of data processing - Annex 4 Data processing census (D.Lgsn.196/2003) - Annex 5 Asset classification and control
6.1 ACCOUNTABILITY FOR ASSETS 6.1.1 Inventory of assets	
6.2 INFORMATION CLASSIFICATION 6.2.1 Classification guidelines 6.2.2 Information labeling and handling	
7 PERSONNEL SECURITY	6.3 ORGANIZATIONAL SECURITY 6.3.1 Actors defined by law 6.3.2 ICT Directorate Limited to privacy
7.1 SECURITY IN JOB DEFINITION AND RESOURCING 7.1.1 Including security in job responsibilities 7.1.2 Personnel screening and policy 7.1.3 Confidentiality agreements 7.1.4 Terms and conditions of employment	
7.2 USER TRAINING 7.2.1 Information security education and training	**8 USER TRAINING**
7.3 SECURITY INCIDENTS AND MALFUNCTIONS 7.3.1 Reporting security incidents 7.3.2 Reporting security weaknesses 7.3.3 Reporting software malfunctions 7.3.4 Learning from incidents 7.3.5 Disciplinary process	6.3 ORGANIZATIONAL SECURITY 6.3.3 CERT@Unitn.it 6.3.4 Management of security incidents and malfunctions
8 PHYSICAL AND ENVIRONMENTAL SECURITY	6.1 PHYSICAL AND ENVIRONMENTAL SECURITY 6.1.1 Secure areas 6.1.2 Equipment security
8.1 SECURE AREAS 8.1.1 Physical security perimeter 8.1.2 Physical entry controls 8.1.3 Securing offices, rooms and facilities 8.1.4 Working in secure areas 8.1.5 Isolated delivery and loading areas	
8.2 EQUIPMENT SECURITY 8.2.1 Equipment siting and protection 8.2.2 Power supplies 8.2.3 Cabling security 8.2.4 Equipment maintenance 8.2.5 Security of equipment off-premises 8.2.6 Secure disposal or re-use of equipment	
8.3 GENERAL CONTROLS 8.3.1 Clear desk and clear screen policy 8.3.2 Removal of property	

Table 3: Comparing ISO-17799 and DPS 3.0

9 COMMUNICATIONS AND OPERATIONS MANAGEMENT	6.2 OPERATIONAL SECURITY 6.3 ORGANIZATIONAL SECURITY
9.1 OPERATIONAL PROCEDURES AND RESPONSIBILITIES 9.1.1 Documented operating procedures 9.1.2 Operational change control 9.1.3 Incident management procedures 9.1.4 Segregation of duties 9.1.5 Separation of development and operational facilities 9.1.6 External facilities management	
9.2 SYSTEM PLANNING AND ACCEPTANCE 9.2.1 Capacity planning 9.2.2 System acceptance	Not implemented
9.3 PROTECTION AGAINST MALICIOUS SOFTWARE 9.3.1 Controls against malicious software	6.2.3 Controls against malicious software
9.4 HOUSEKEEPING 9.4.1 Information back-up 9.4.2 Operator logs 9.4.3 Fault logging	6.2.4 Information back-up and recovery 6.3.6 Procedures for information back-up and recovery
9.5 NETWORK MANAGEMENT 9.5.1 Network controls	6.2.2 Network controls
9.6 MEDIA HANDLING AND SECURITY 9.6.1 Management of removable computer media 9.6.2 Disposal of media 9.6.3 Information handling procedures 9.6.4 Security of system documentation	6.1.3 Management of removable computer media and system documentation
9.7 EXCHANGES OF INFORMATION 9.7.1 Exchange policy 9.7.2 Exchange agreements 9.7.3 Physical media in transit 9.7.4 Electronic commerce 9.7.5 Electronic communications 9.7.6 On-Line Transactions 9.7.7 Office information systems 9.7.8 Publicly available systems	Not implemented
10 ACCESS CONTROL	6.2 OPERATIONAL SECURITY 6.3 ORGANIZATIONAL SECURITY 6.2.1 Access control (Authentication and Authorization) 6.3.5 User access management (Authentication and Authorization)
10.1 BUSINESS REQUIREMENT FOR ACCESS CONTROL 10.1.1 Access control policy	
10.2 USER ACCESS MANAGEMENT 10.2.1 User registration 10.2.2 Privilege management 10.2.3 User password management 10.2.4 Review of user access rights	
10.3 USER RESPONSIBILITIES 10.3.1 Password use 10.3.2 Unattended user equipment	
10.4 NETWORK ACCESS CONTROL 10.4.1 Policy on use of network services 10.4.2 Enforced path 10.4.3 User authentication for external connections 10.4.4 Node authentication 10.4.5 Remote diagnostic port protection 10.4.6 Segregation in networks 10.4.7 Network connection control 10.4.8 Network routing control 10.4.9 Security of network services	
10.5 OPERATING SYSTEM ACCESS CONTROL 10.5.1 Automatic terminal identification 10.5.2 Terminal log-on procedures 10.5.3 User identification and authentication 10.5.4 Password management system 10.5.5 Use of system utilities 10.5.6 Duress alarm to safeguard users 10.5.7 Terminal time-out 10.5.8 Limitation of connection time	
10.6 APPLICATION ACCESS CONTROL 10.6.1 Information access restriction 10.6.2 Sensitive system isolation	
10.7 MONITORING SYSTEM ACCESS AND USE 10.7.1 Event logging 10.7.2 Monitoring system use 10.7.3 Clock synchronization	Not structured (though individual logs are taken)
10.8 MOBILE COMPUTING AND TELEWORKING 10.8.1 Mobile computing 10.8.2 Teleworking	Not implemented

Table 3: Comparing ISO-17799 and DPS 3.0

11 SYSTEMS DEVELOPMENT AND MAINTENANCE	6.2 OPERATIONAL SECURITY 6.3 ORGANIZATIONAL SECURITY 6.2.5 Software controls (non-repudiation services will be implemented in the near future!)
11.1 SECURITY REQUIREMENTS OF SYSTEMS 11.1.1 Security requirements analysis and specification	
11.2 SECURITY IN APPLICATION SYSTEMS 11.2.1 Input data validation 11.2.2 Control of internal processing 11.2.3 Message authentication 11.2.4 Output data validation	
11.3 CRYPTOGRAPHIC CONTROLS 11.3.1 Policy on the use of cryptographic controls 11.3.2 Encryption 11.3.3 Digital signatures 11.3.4 Non-repudiation services 11.3.5 Key management	
11.4 SECURITY OF SYSTEM FILES 11.4.1 Control of operational software 11.4.2 Protection of system test data 11.4.3 Access control to program source library	
11.5 SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES 11.5.1 Change control procedures 11.5.2 Technical review of operating system changes 11.5.3 Restrictions on changes to software packages 11.5.4 Covert channels and Trojan code 11.5.5 Outsourced software development	
12 BUSINESS CONTINUITY MANAGEMENT	6.3 ORGANIZATIONAL SECURITY 6.2.4 Information back-up and recovery 6.3.6 Procedures for information back-up and recovery
12.1 ASPECTS OF BUSINESS CONTINUITY MANAGEMENT 12.1.1 Business continuity management process 12.1.2 Business continuity and impact analysis 12.1.3 Writing and implementing continuity plans 12.1.4 Business continuity planning framework 12.1.5 Testing, maintaining and re-assessing business continuity plans	
13 COMPLIANCE	- Annex 7 Description of security policy and technical compliance (D.Lgs. N.196/2003) - Annex 8 Description of security policy and technical compliance (D.P.R.N.318/1999) Receival of national law, limited to privacy: - privacy - cryptography - digital signatures - copyright - illegal activities and disciplinary action - collection of evidence
13.1 COMPLIANCE WITH LEGAL REQUIREMENTS 13.1.1 Identification of applicable legislation 13.1.2 Intellectual property rights (IPR) 13.1.3 Safeguarding of organizational records 13.1.4 Data protection and privacy of personal information 13.1.5 Prevention of misuse of information processing facilities 13.1.6 Regulation of cryptographic controls 13.1.7 Collection of evidence	
13.2 REVIEWS OF SECURITY POLICY AND TECHNICAL COMPLIANCE 13.2.1 Compliance with security policy 13.2.2 Technical compliance checking	**7. REVIEWS OF SECURITY POLICY AND TECHNICAL COMPLIANCE** - Annex 6 Facsimile for reviews of security policy and technical compliance
13.3 SYSTEM AUDIT CONSIDERATIONS 13.3.1 System audit controls 13.3.2 Protection of system audit tools	