UNIVERSITY OF PIRAEUS

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

School of Information and Communication Technologies

Department of Digital Systems
Systems Security Laboratory

Systems Security
Laboratory

Ph.D. Thesis

Security Policies for Cloud Computing

A dissertation submitted for the degree of
Doctor of Philosophy
in
Computer Science
By

Dimitra A. Georgiou

PIRAEUS 2017

Advisory Committee

Costas Lambrinoudakis,
Professor (Supervisor)
University of Piraeus

Sokratis Katsikas,
Professor
University of Piraeus

Christos Xenakis,
Associate Professor
University of Piraeus

UNIVERSITY OF PIRAEUS

2017

Examination Committee

Costas Lambrinoudakis, Professor
University of Piraeus

Sokratis Katsikas, Professor
University of Piraeus

Christos Xenakis, Associate Professor
University of Piraeus

Stefanos Gritzalis, Professor
University of the Aegean (Member)

Spyros Kokolakis, Associate Professor
University of the Aegean (Member)

Aggeliki Tsohou, Assistant Professor
Ioanian University (Member)

Christos Kalloniatis, Associate Professor
University of the Aegean (Member)

UNIVERSITY OF PIRAEUS

PIRAEUS 2017

The views and conclusions contained in this document reflect the author and should not be interpreted as representing the official positions of University Piraeus.

Οι απόψεις και τα συμπεράσματα που περιέχονται στο παρόν έγγραφο εκφράζουν τον συγγραφέα και δεν πρέπει να ερμηνευθεί ότι αντιπροσωπεύουν τις επίσημες θέσεις του Πανεπιστημίου Πειραιώς.

Abstract

The massive technological developments in world trade and the need for personal information to cross international borders highlighted the need to define security policies and propose specific regulations to enhance the protection of citizens' personal data. A technological breakthrough, which creates challenges to the protection of personal data, is Cloud Computing. The main feature of Cloud Computing is that it allows on-demand network access to computing resources with minimal management effort or service provider interaction. This new era gives new dimensions to international transfers of personal data and for this reason it has become necessary to establish a Security Policy for Cloud Computing services. For the new era of Cloud Computing, the purpose of a Security Policy is to protect people and information, set rules for expected behavior by users, minimize risks and help to track compliance with regulation.

This thesis proposes a Methodology that can be adopted for the development of a Cloud Security Policy, in respect to data security. Specifically focused on the model of Software-as-a-Service (SaaS), this thesis is intended to serve as a Framework for organizations, users, Cloud Providers and provide a baseline for the Security Policy of Cloud Computing. We address the security requirements that are specific to Cloud Environment, highlight how these requirements link to our Cloud Security Policy and recommend, the measures and the corresponding security policies. Furthermore, it proposes a method that can be adopted by Cloud Providers for auditing the security of their systems as, security is one of the core competencies of the Cloud Provider.

Dimitra Georgiou
Department of Digital Systems
UNIVERSITY OF PIRAEUS
© 2017

Περίληψη

Οι μαζικές τεχνολογικές εξελίξεις του παγκόσμιου εμπορίου και η ανάγκη διασυνοριακής κίνησης των προσωπικών πληροφοριών, δημιουργούν την ανάγκη να καθοριστούν πολιτικές ασφαλείας και να προταθούν ειδικοί κανονισμοί για την ενίσχυση της προστασίας των προσωπικών δεδομένων των πολιτών. Ένα τέτοιο τεχνολογικό επίτευγμα, το οποίο δημιουργεί προκλήσεις στην προστασία των προσωπικών δεδομένων, είναι το Νέφος Υπολογιστών (Cloud Computing). Το κύριο χαρακτηριστικό του είναι ότι επιτρέπει εύκολη και κατά απαίτηση πρόσβαση στο δίκτυο σε υπολογιστικούς πόρους, ανεξάρτητα από το πού βρίσκονται τα δεδομένα, η οποία μπορεί να τροφοδοτηθεί γρήγορα και να υπάρξει με την ελάχιστη προσπάθεια διαχείρισης ή αλληλεπίδραση παροχής υπηρεσιών.

Η κατάσταση αυτή δίνει νέες διαστάσεις στη διασυνοριακή κίνηση των προσωπικών δεδομένων και για το λόγο αυτό έχει γίνει αναγκαίος ο καθορισμός της πολιτικής ασφαλείας των υπηρεσιών του Νέφους. Για την νέα εποχή του Νέφους, ο σκοπός της πολιτικής ασφάλειας είναι να προστατεύσει τους ανθρώπους και τις πληροφορίες, να θέσει κανόνες για την αναμενόμενη συμπεριφορά των χρηστών, να ελαχιστοποιήσει τους κινδύνους και να βοηθήσει στην παρακολούθηση των συμμορφώσεων με τους κανονισμούς.

Αυτή η διατριβή προτείνει μια μεθοδολογία που μπορεί να υιοθετηθεί για την ανάπτυξη μιας γενικότερης πολιτικής ασφαλείας συστήματος Νέφους Υπολογιστών, με στόχο πάντα την ασφάλεια των δεδομένων. Πιο συγκεκριμένα, επικεντρώνεται ειδικά στο μοντέλο υπηρεσιών του Software-as-a-Service (SaaS). Στην ακόλουθη έρευνα, παρατίθενται οι απειλές και οι απαιτήσεις ασφαλείας που ισχύουν μόνο για τα Περιβάλλοντα Νέφους Υπολογιστών, και προτείνονται μέτρα και αντίστοιχες πολιτικές ασφαλείας για την αποφυγή τους. Επιπλέον, προτείνεται μια μέθοδος που θα μπορούσε να υιοθετηθεί από τους Παρόχους υπηρεσιών Νέφους για τον έλεγχο της ασφάλειας των συστημάτων τους, αφού η ασφάλεια είναι έναν από τα βασικότερα προβλήματα τους.

Δήμητρα Γεωργίου
Τμήμα Ψηφιακών Συστημάτων
Πανεπιστήμιο Πειραιώς
© 2017

Αφιερώσεις

Στους γονείς μου...

Φανή και Θανάση

Γεωργίου

Δήμητρα Γεωργίου
Τμήμα Ψηφιακών Συστημάτων
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
©2017

Dedications

To my parents…

Fani and Thanasis

Georgiou

Dimitra Georgiou
Department of Digital Systems
UNIVERSITY OF PIRAEUS
© 2017

«Δεν υπάρχουν ιδέες, υπάρχουν μονάχα άνθρωποι που κουβαλούν τις ιδέες, κι αυτές παίρνουν το μπόι του ανθρώπου που τις κουβαλάει»

Ν.Καζαντάκης

Ευχαριστίες

«Η ζωή για τον καθένα μας είναι σαν παραμύθι…»

(Χανς Κρίστιαν Άντερσεν)

Επιλέγουμε τους ανθρώπους που θαυμάζουμε και εκτιμούμε

και μαζί τους βαδίζουμε στα μονοπάτια της ζωής…

Στο δικό μου «*παραμύθι*», είχα την τύχη και την τιμή να έχω στο πλευρό μου αξιόλογους ανθρώπους, επιστήμονες, συνεργάτες και φίλους που με καθοδήγησαν, με εμψύχωσαν, με στήριξαν και με γέμισαν με σοφία και πείρα, για το υπόλοιπο της ζωής μου.

Αρχικά, θα ήθελα να εκφράσω ένα πάρα πολύ μεγάλο ευχαριστώ, στον επιβλέποντα καθηγητή μου και μέντορά μου, όπως τον αποκαλώ, κ.Κωνσταντίνο Λαμπρινουδάκη, για την καθοδήγησή του και για την αμέριστη επιστημονική και ηθική υποστήριξη που μου προσέφερε κατά τη διάρκεια αυτής της διατριβής. Οι πολύτιμες συμβουλές του δεν ήταν μόνο εμπνευσμένες, αλλά και καθοριστικές σε αυτή την έρευνα. Από την αρχή της γνωριμίας μας, μέχρι και σήμερα, μου προσέφερε απλόχερα και ανιδιοτελώς επιστημονική, πνευματική και ηθική καθοδήγηση, αφιερώνοντάς μου αρκετό από τον πολύτιμό του χρόνο. Τον ευχαριστώ μέσα από τα βάθη της καρδιάς μου, για την εμπιστοσύνη που μου έδειξε και δείχνει μέχρι σήμερα, καθώς και το ότι με τίμησε με τη συνεργασία του. Αποτελεί πρότυπο για τη μελλοντική μου πορεία ως επιστήμονας, αλλά και ως άνθρωπος γενικότερα και ευελπιστώ η συνεργασία μας να συνεχιστεί και στο μέλλον, προάγοντας με τον δικό μας πάντα τρόπο την επιστήμη.

Ιδιαίτερες ευχαριστίες, θα ήθελα να απευθύνω στον καθηγητή και μέλος της Τριμελής Συμβουλευτικής μου Επιτροπής κ. Σωκράτη Κάτσικα, για την εμπιστοσύνη που έδειξε προς το πρόσωπό μου και για τη δυνατότητα που μου έδωσε, με το να με εντάξει από την αρχή της ακαδημαϊκής μου πορείας ως Ερευνήτρια στην ομάδα του Εργαστηρίου της Ασφάλειας Συστημάτων του Τμήματος Ψηφιακών Συστημάτων – Πανεπιστημίου Πειραιώς και να με οδηγήσει σε μονοπάτια γνώσης και εμπειρίας. Όλη τη διάρκεια της διατριβής μου, με τις πολύτιμες συμβουλές του, το γνήσιο ενδιαφέρον του και την εποικοδομητική του κριτική, συνέβαλε τα μέγιστα, τόσο στην επιστημονική εξέλιξή μου, όσο και στην ολοκλήρωση της παρούσας διατριβής. Αισθάνομαι, πολύ τυχερή που τον γνώρισα από την αρχή της πορείας μου και καθημερινά λαμβάνω αληθινά μαθήματα ανθρώπινης και ακαδημαϊκής συμπεριφοράς.

Επίσης, θα ήθελα να ευχαριστήσω τον Αναπληρωτή Καθηγητή κ. Χρήστο Ξενάκη και μέλος της Τριμελής μου Συμβουλευτικής Επιτροπής για την καθοδήγηση και τις πολύτιμες συμβουλές που μου παρείχε, καθώς με την εμπειρία του και την γνώση που μου προσέφερε, συνετέλεσε στην ολοκλήρωση αυτής της διατριβής.

Θερμές ευχαριστίες για την συμμετοχή τους ως Μέλη στην Επταμελή Συμβουλευτική Επιτροπή της διατριβής μου, οφείλω επίσης στους Καθηγητές: κ. Στέφανο Γκρίτζαλη – Καθηγητή Πανεπιστημίου Αιγαίου , κ. Σπυρίδων Κοκολάκη - Αναπληρωτή Καθηγητή Πανεπιστημίου Αιγαίου, κα. Αγγελική Τσόχου - Επίκουρη Καθηγήτρια Ιονίου Πανεπιστημίου και κ. Χρήστο Καλλονιάτη – Αναπληρωτή Καθηγητή Πανεπιστημίου Αιγαίου. Τους ευχαριστώ θερμά και είναι τιμή μου που συμμετείχαν στην ολοκλήρωση αυτής της διατριβής. Το έργο τους και η ακαδημαϊκή τους πορεία αποτελούν πρότυπο για τη μελλοντική μου πορεία μου ως επιστήμονας.

Ιδιαίτερες ευχαριστίες θα ήθελα να εκφράσω, στον Δρ. Δημήτριο Γενειατάκη για την ανεκτίμητη βοήθεια και καθοδήγησή μου στα πρώτα μου βήματα ως υποψήφια διδάκτορας, στον συνεργάτη μας Δρ. Νικόλαο Βράκα και σε όλα τα μέλη του Εργαστηρίου της Ασφάλειας Ψηφιακών Συστημάτων, για το ότι μου προσέφεραν ένα ευχάριστο περιβάλλον γεμάτο ενδιαφέρουσες και εποικοδομητικές συζητήσεις. Εύχομαι να συνεχίσουν με την έρευνά τους σε κάθε επίπεδο με επιτυχία. Επίσης, θα ήθελα να ευχαριστήσω τον Αναπληρωτή Καθηγητή κ. Ηλία Μαγκλογιάννη, για την ανεκτίμητη βοήθεια που μου προσέφερε. Με τις πολύτιμες συμβουλές του, το γνήσιο ενδιαφέρον του και την εποικοδομητική του κριτική, συνέβαλε τόσο στην επιστημονική εξέλιξή μου, όσο και στην ολοκλήρωση της παρούσας διατριβής.

Ο καθένας από όλους όσους ανέφερα, έχει συμβάλει με το δικό του ξεχωριστό τρόπο στην ολοκλήρωση αυτής της διατριβής. Αλλά την πιο μεγάλη συμβολή και το πιο μεγάλο ευχαριστώ, το οφείλω στην οικογένειά μου: στους γονείς μου Φανή και Θανάση Γεωργίου και στην αδερφή μου Αθηνά, για την αμέριστη αγάπη, υποστήριξη και συμπαράσταση, καθώς και για τις θυσίες και παραχωρήσεις που έχουν κάνει για εμένα όλα αυτά τα χρόνια. Ευελπιστώ, με την παρούσα διατριβή να ικανοποιούνται οι προσδοκίες που έτρεφαν στο πρόσωπό μου και να είναι υπερήφανοι για εμένα.

Δήμητρα Α. Γεωργίου

Acknowledgements

"Life for everyone is like a fairy tale ..."

(Hans Christian Andersen)

We choose the people we admire and appreciate

And with them we walk on the paths of life ...

In my own "fairy tale" I was fortunate to have remarkable people, scientists, colleagues and friends who guided me, animated me, supported me and filled me with wisdom and experience for the rest of my life.

First of all, I would like to express my sincere thanks to my supervising professor and mentor, as I call him, Mr. Costas Lambrinoudakis, for his guidance and for the full scientific and moral support that he offered me during this dissertation. His valuable advice was not only inspired but also crucial in this research. From the beginning of our acquaintance, until this day, he offered me generously and unselfishly scientific, spiritual and moral guidance, dedicating me enough of his precious time. I thank him through the depths of my heart, for the trust that he has shown and shows to me until now, as well as for honouring me with his cooperation. He is a model for my future career as a scientist, but also as a person in general and I hope that our cooperation will continue in the future by promoting our science in our own way.

I would like to extend my special thanks to the professor and member of my Advisory Committee, Professor Sokratis Katsikas, for the confidence he has shown towards me by integrating me from the beginning of my academic career as a Researcher at the Laboratory of Digital Systems Security Laboratory of the Digital Systems Department - University of Piraeus. He has guided me to paths of knowledge and experience. Throughout my dissertation, with his valuable advice, his genuine interest and constructive criticism, he contributed greatly both to my scientific development and to the completion of this dissertation. I feel very lucky to know him from my early steps and I receive real lessons of human and academic behaviour every day.

I would also like to thank Christos Xenakis, Associate Professor and member of my Advisory Committee, for the guidance and valuable advice he has given to me in order to complete this dissertation.

Many thanks I have to offer to the professors of my Examination Committee: Stefanos Gritzalis - Professor of the University of the Aegean, Spyros Kokolakis - Associate Professor of the University of the Aegean, Aggeliki Tsochou - Assistant Professor of the Ionian University and Christos Kalloniatis – Associate Professor of the University of the Aegean. I would like to thank them warmly and it is my honour that they participated in the completion of this dissertation. Their work and their academic career are a model for my future as a scientist.

I would like to express my special thanks to Dr. Dimitrios Geneiatakis for his invaluable help and guidance in my first steps as a doctoral candidate, our colleague Dr. Nikolaos Vrakas and all members of the Digital Systems Security Laboratory, for offering me a pleasant environment full of interesting and constructive discussions. I wish to continue with their research, in their fields successfully. I would also like to thank Ilias Maglogiannis – Associate Professor of the University of Piraeus, who with his valuable advice, his genuine interest and constructive critique contributed both to my scientific development and to the completion of this thesis.

Everyone from all those mentioned, has contributed in its own special way to the completion of this thesis. But the biggest contribution and the greatest thank you, I owe it to my family - my parents Fani and Thanasis Georgiou and my sister Athina for their undivided love, support and assistance, as well as the sacrifices and concessions they have done for me all these years. I hope that this dissertation will meet their expectations and that they will be proud of me.

Dimitra A. Georgiou

(Signature)

.....

Dimitra Georgiou

Ph.D. Thesis, University of Piraeus, Department of Digital Systems

System Security Laboratory

© 2017 – All rights reserved

Table of Contents

Abstract..... 5

List of Figures.....16

List of Tables..... 17

Chapter 1: Introduction..... 18

1.1. Problem Identification..... 20

1.2. Goals and Contribution 24

Chapter 2: Security in Cloud Computing.....27

2.1. Literal review..... 27

2.2. Security Policy in Cloud Computing 33

2.3. The problem of non-existing Security Policy 35

Chapter 3: Security Policy in Cloud Computing.....38

3.1. Introduction..... 38

3.2. An Analysis of the Methodology of our Security Policy Framework – First idea..... 40

3.3. An Analysis of the Methodology of our Security Policy Framework – Final Ideal..... 53

Chapter 4: Auditing our Methodology.....58

4.1. Introduction..... 58

4.2. Cloud Specific Security Threats 59

4.3. General Recommendations for the Security Policy 62

4.4. Proposed Model-Methodology for Auditing..... 64

Chapter 5: Security Policy Rules and Required Procedures for two crucial Threats of Cloud Computing..... 70

5.1. Introduction..... 70

5.2. Literature Review 71

5.3. Evaluation of transferring a System to Cloud 74

5.4. Two types of threats in Cloud Computing – Case Studies 80

5.5. Case study of the 1st Threat - Proposed Security Policy Rules 82

5.6. Case study of the 2nd Threat - Proposed Security Policy Rules..... 93

Chapter 6: Security in e-Health System 97

6.1. Introduction..... 97

6.2. Information Privacy in Health Informatics..... 98

6.3. Case Study of e-Health System in Europe and EEA Members States 99

6.4. E-Health Cloud Computing Implementations Issues 101

6.5. Requirements: Cloud-Specific Security Aspects for E-Health Systems 103

Chapter 7: Conclusions and Future Work 136

7.1. Conclusions..... 136

7.2. Future Work 137

References.....138

List of Figures

Figure 1 The contribution of the proposed Methodology……24

Figure 2 The NIST Cloud Definition Framework……29

Figure 3 Visual Model of NIST Working Definition of Cloud Computing……34

Figure 4 The Processing of our Security Policy……38

Figure 5 Structure of the General Security Policy……39

Figure 6 Security Policy Structure for Cloud Providers……45

Figure 7 Security Policy Rules covering Threat 5……46

Figure 8 Security Threats in Cloud Computing……54

Figure 9 Methodology of Cloud Security Framework……56

Figure 10 Cloud Security Framework……67

Figure 11 Overall Methodology of Cloud Security Framework with the evaluation……80

Figure 12 E-health example Types……101

Figure 13 A Cloud Based e-Health System……102

Figure 14 Cloud Computing Requirements of E-health system……110

List of Tables

Table 1 Cloud Security Issues and Description……30

Table 2 Linking Threats with Category……55

Table 3 Security Threats in Cloud Computing……59

Table 4 A list of Nine Cloud-specific Security Threats (Cloud Security Alliance)……60

Table 5 New Specific Security Threats to Cloud Computing……61

Table 6 SaaS Security Recommendations……62

Table 7 Linking Threats with Category - Auditing Example……66

Table 8 Case Study – Data Loss Threat……68

Table 9 Contending definitions of Threats……73

Table 10 Control point of the Compliance……74

Table 11 Control point of Technical System Characteristics……75

Table 12 Control points of Requirements and Operating System features……76

Table 13 Steps for Risk Assessment and System Security Requirements……77

Table 14 Two Crucial Threats and their Categories……81

Table 15 Security Policy for the Threat1 "Lack of user control"……83

Table 16 Security Policy for Threat2 "Insufficient Knowledge"……93

Table 17 Cloud Computing Requirements of e-health system……108

Table 18 Security Policy Rules of E-Health Cloud System (for Category A)……111

Table 19 Security Policy Rules of E-Health Cloud System (for Category B)……121

Table 20 Security Policy Rules of E-Health Cloud System (for Category C)……125

Table 21 Security Policy Rules of E-Health Cloud System (for Category D)……128

Chapter 1: Introduction

Nowadays, in interconnected world every corporation needs a well thought out Security Policy. The rapid growth of the information age has significantly changed the nature of Computing and gives rise to a new set of security concerns and issues. According to the National Institute of Standards and Technology (NIST), Security Policy is defined as "Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information" [1].

For the technological achievement of Cloud Computing**,** the purpose of a Security Policy is to protect people and information, set rules for expected behavior by users, minimize risks and track compliances with regulations [2]. Considering the fact that in recent times anyone with an interest in information technology has come across the term Cloud Computing [3] it is really important to seriously consider the security issues in Cloud Computing: Are there any Security threats in Cloud Computing, that do not appear in non- Cloud Systems? Is the Cloud secure and safe for the users? As Cloud Computing is achieving popularity, we attempt to demystify the security and privacy risks that are introduced, because of its transformational nature [4]. The success of a Cloud Security Policy really depends on the way the security contents are addressed.

Like most technologies, Cloud Computing evolved from a need. The tremendous growth of the Web has given rise to a new class of "Web-scale" problems—challenges such as the increasingly amount of information available in internet or the creation of larger space storage in servers and the use of more cloud-based applications storage over long distances.

As a need firstly, we must mention the accurate definition of this technology. The most widely used definition of the Cloud Computing model is introduced by NIST, as "Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or Service Provider interaction".

This Cloud Model is composed of five essential characteristics, three Service Models, and four Deployment Models.

Its "**five essential characteristics**" are: **a)** *On-demand self-service,* **b)** *Broad network access,* **c)** *Resource pooling,* **d)** *Rapid elasticity,* **e)** *Measured service* [5].

Its three **Service Models** which are referenced to: Software-as-a-Service **(SaaS)**, Platform-as-a-Service **(PaaS),** Infrastructure-as-a-Service **(IaaS).** It is worthwhile to be mentioned, that each Service Delivery Model has different implementations, which complicates the Development of standard security model that can be adopted by others, as Cloud Computing Consumers or Providers or Cloud Services.

Its **four Deployment Models** that are divided into, three commonly-used models and an additional one which are:

The three commonly-used Cloud Deployment models:

a) **Private** Cloud: is a built and managed within a single organization,
b) **Public** Cloud: is a set of Computing resources provided by third-party organizations,
c) **Hybrid** Cloud: is a mix of computing resources provided by both private and public clouds.

And the **additional Model**, which is less-commonly used and it is the:

Community Cloud: shares computing resources across several organizations, and can be managed by either organizational IT resources or third-party Providers. [6][7][8][9][10][11][12]

Managing such heterogeneous Models, to meet security needs is a complex task, taking into account conflicts among the security requirements and among security controls at each layer of Cloud.

From the Cloud Providers' perspective, security requires a lot of expenditures (security solutions' licenses) and resources and is a difficult problem to achieve. So Cloud Providers have to understand consumers' concerns and seek out new security solutions that resolve such concerns. As Cloud Computing is achieving popularity, its multidisciplinary has raised questions in the research community about how novel

this new paradigm is because it includes almost everything that existing technologies already do [13].

The methodology, presented in this Thesis, uses the Threats related to the Software-as-a-Service Model and related to the Cloud Provider. We choose this one to investigate in our research, because it remains the dominant Cloud Model for the reason that it simplifies deployment and reduces customer acquisition costs. According to its characteristics, it is also accessible from any locations, its updates are being automated, it is compatible across multiple devices and its products can be easily adjusted to particular client's needs. The SaaS model has flourished in recent years because of the many benefits it offers, so we decided to secure this one.

The key objective of the proposed Methodology gives a solution to the security challenges of a SaaS Cloud Computing Model. If the Cloud Providers follow the proposed Model, they will succeed in having a professional Security Audit and thus a high level of security in their Cloud Computing environment, saving time and money.

1.1. Problem Identification

While the internet grew rapidly and Cloud Computing is expanding as a service used by a great number of many individuals and organizations internationally, policy issues related to Cloud Computing are not being widely discussed or considered. The rapid growth of internet during the last decade comprises a fact that even the most doubtful could foresee. The usability, accessibility, low cost and the high volume of available information related to the Cloud Computing raise a range of important policy issues, which include issues of privacy, security, anonymity, telecommunications capacity, government surveillance, reliability, and liability, among others.

Conventional Security Policies designed for other technologies do not map well to the Cloud Computing environment. Cloud architecture is fundamentally different from other systems, the Cloud environment is by nature multitenant with shared resources, and the location of the data and the local privacy requirements

will not be controlled by the user. It is important to have in our mind that Cloud is enabled by virtualization technologies.

Although Cloud Computing has been researched earlier, the recent increased use of Cloud Services requires up-to-date insights into necessary security requirements and its solutions.

The Problem of Cloud Computing security is very important and can prevent the rapid growth. But what is the problem exactly? And why do we need a Security Policy for the Cloud Computing? We analyze the problem of security in Cloud and its strategy in accordance with the concepts and characteristics of Cloud Computing.

After our in-depth, risk analysis of Cloud Computing Model and our experience in other conventional systems occurred that, to have a safe operation of the Cloud Computing, we should consider the following areas: the architecture of Cloud Computing, governance, portability and interoperability, the traditional security, business continuity and disaster recovery, data in business center, the incident response, notification and remediation, application security, encryption and key management, identity and access management.

Many of the security issues that need to address the Cloud Computing are already known in other systems. But the Cloud Computing system has certain characteristics and attributes that create new security concerns.

Firstly, the Cloud environment has a much more complex architecture compared to other systems. It combines a number of Computing concepts and technologies such as Service Oriented Architecture (SOA), Web 2.0, virtualization and other technologies with reliance on the Internet, providing common business applications online through web browsers to satisfy the Computing needs of users, while their software and data are stored on the servers. The resource pooled nature of the Cloud, due to the centralization of data and universal architecture enables Cloud Providers to focus all their security resources on securing the Cloud architecture.

Furthermore, the lack of standardization is a very important problem associated with the Cloud Computing, since no proper standards exist, it becomes extremely difficult for a company to secure the services that it offers or uses through

a Cloud VMware white paper [14] supports that: Cloud architectures must have well-defined Security Policies and procedures in place. Realizing full interoperability with existing dedicated security controls is unlikely; there has to be some degree of compatibility between the newer security protections specifically designed for Cloud environments and traditional security controls.

Multi-tenancy (shared resources): Cloud Computing is based on a business model in which resources are shared (i.e. multiple users use the same resources) at the network level, host level and application level. Cloud Computing services exist in many variations, including data storage sites, video sites, personal health record websites and many others. The entire contents of a user's storage device may be stored with a single Cloud Provider or with many Cloud Providers. Multi-tenancy implies sharing of computational resources, storage, services, and applications with other tenants. In the multitenant Cloud environment the location of the data and the local privacy requirements are not be controlled by the user. This characteristic focuses on resource utilization, cost and service availability. In such a situation, data of various users will reside at the same location. Intrusion of data of one user by another becomes possible in this environment. Security Alliance says: about Multi-tenancy in Cloud Service Models, that implies a need for policy-driven enforcement, segmentation, isolation, governance, service levels and chargeback/billing models for different consumer constituencies. This attribute of multi-tenancy may lead to security issues.

Massive scalability: Although organizations might have hundreds or thousands of systems, Cloud Computing provides the ability to scale to tens of thousands of systems, as well as the ability to massively scale bandwidth and storage space. New nodes can be added or dropped from the network as can physical servers, with limited modifications to infrastructure set up and software. Cloud architecture can scale horizontally or vertically, according to demand. This attribute may lead to traffic overflow issues and how to manage such a huge amount of data.

Elasticity: Users can rapidly increase and decrease their Computing resources as needed, as well as, release recourses for other users when they are no longer required. Elasticity implies being able to scale up or down resources assigned to services based on the current demand. Scaling up and down of tenant's resources

gives the opportunity to other tenants to use the tenant previously assigned resources. This attribute may lead to confidentiality issues in Cloud Computing.

Pay as you go: Users pay for only the recourses they actually use and for only the time they require**.** Aside from the higher flexibility, a key benefit of this service is the usage-based payment scheme. This allows customers to pay as they grow. Another important issue is to buy and use the latest technology. On-demand, self-sustaining or self-healing, multi-tenant, customer segregation are the key requirements of IaaS. The Provider might give some control to the people to build applications on top of the platform. But any security below the application level such as host and network intrusion prevention will still be in the scope of the Provider and the Provider has to offer strong assurances that the data remains inaccessible between applications. For some types of information and some categories of Cloud Computing users, privacy and confidentiality rights, obligations and status may change when a user discloses information to a Cloud Provider. So, this attribute may lead to privacy and confidentiality issues.

Self-provisioning of resources: Users self-provision resources such as additional systems and network recourses. And **Concerns** that create questions as:

- *Who has access to the data?*
- *Do I have full visibility into information regarding these access-control policies?*
- *What are the access-control policies?*
- *Is data encrypted during transfer from the internal network to the public cloud?*
- *What is the disaster-recovery process?*
- *Does the Cloud Provider replicate data across multiple datacenters? Are these datacenters located in different geographical locations?*

All these questions need investigation and the Cloud Provider is the only source of information. Given that there are appropriate standards for the Cloud Computing, it is almost impossible for a company to ensure the quality of services provided.

Like other systems, so the Cloud Computing is not meant to have no risks, the truth remains that these risks are definitely manageable with some effort and we

will present this in our research that focuses on the **Creation of a single Security Policy**, after identifying the risks that threaten the Cloud Computing.

1.2. Goals and Contribution

Through the literature review, we have examined many aspects of Security Policies in Cloud Computing; the aim in our Ph.D. thesis was to propose a methodology that may be adopted for the development of a Cloud Security Policy, for the Cloud Providers, in respect to data security and thus contributing to the scientific community of Cloud Computing Security.

Specifically the **goals** were:

i. Detailed review of existing studies on the security issues of Cloud Computing.

ii. Review of all existing threats against Cloud Computing, focusing on those that are not applicable to conventional systems.

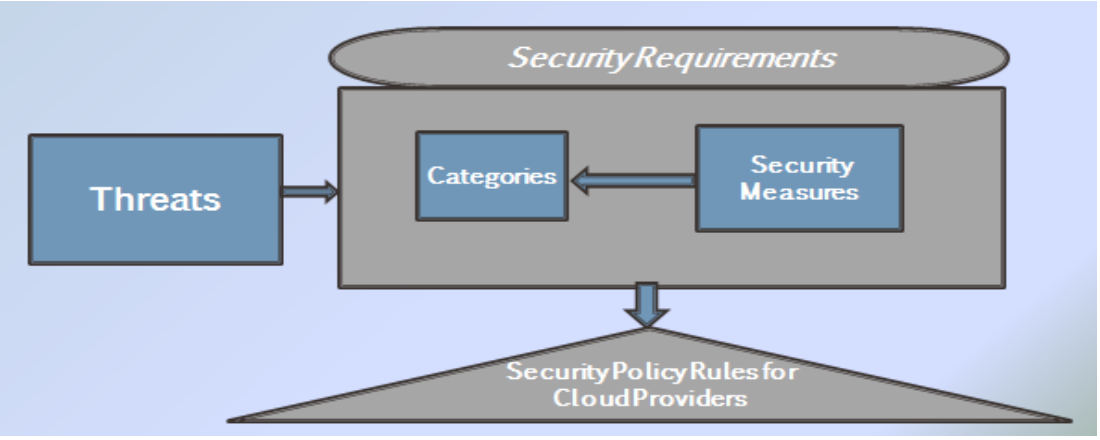
iii. Identification of Security Policy Rules and General Recommendations for SAAS Security Policies.

iv. Proposal of a Methodology for assessing threats in Cloud, in order to identify the new rules that should be incorporated in the Cloud Security Policy.

v. Application and evaluation of the proposed methodology in specific use cases.

To be specific in this Ph.D. thesis after reviewing all existing threats and their known solutions, the absence of a methodology for the development of a Security Policy was identified as one of the major problems in a Cloud Computing environment.

Figure 1 The contribution of the proposed Methodology



Existing research methodologies are not appropriate for Cloud Computing since threats in Cloud environments are different. Cloud architectures must have well-defined Security Policies and procedures in place.

Despite the research that has been carried out in the field of Cloud Computing security, it is necessary to assess the current state of research, practice and security policies, in order to provide practitioners with evidence that will enable them to focus on its further development. Something that we present with our detailed review of existing studies on the security issues in **(Goal I).**

Cloud Computing is not a new technology, is an evolution of Information Technology architecture from centralized computing to network dependent systems with distributed assets and distributed management responsibilities. While there are common definitions, the various different technologies models that comprise cloud computing reveal its complexity and amount of different threat**,** and that defining cloud computing is impractical for Policy purposes. So in our research**,** we made a review of all existing threats in Cloud, to succeed our **(Goal II).**

It is worthwhile to be mentioned that Cloud Computing raises a range of important Policy issues. A productive approach to begin analysis of the information Policy issues related to Cloud Computing is to consider user expectations. At a minimum, users will likely expect that a cloud will provide the following **a)** Reliability and liability, **b)** Security, privacy, and anonymity, **c)** Access and usage restrictions. In our research we present an implementation of Security Policy Rules and General Recommendations for SaaS Security Policies **(Goal iii),** so to fulfill users expectations and to guide Cloud Providers. To alleviate all the security concerns, a Cloud solution Provider must ensure that customers will continue to have the same security and privacy controls over their applications and services **(Goal I, ii, iii).** With the implementation of our new methodology we assessed the threats in order to identify the new rules that should be in incorporated in the Cloud Security Policy **(Goal IV).**

So, what is the contribution of this Thesis? While there are other policy issues beyond those mentioned above, we believe that the Security Policy Rules and considerations, presented in this Thesis, are vital for the successful development of a

General Security Policy for Cloud Computing, for the Software-as–a-Service Model. We provide evidence that the Cloud Computing Systems based in this Security Policy are achieving an adequate security protection level and that they can meet the provisions of the service-level agreement terms. Furthermore, we highlight Security Requirements and solutions, as best practices and the proposed Methodology of developing the Security Policy are performed through case studies **(Goal v).** In addition, it is worth mentioning that the Cloud Security Policy presented in this thesis considers the current Cloud Computing landscape with provisions on how this space is likely to evolve in the future. These principles, policies and the enterprise security plan constitute the enterprise security governance, risk management, and compliance model.

Chapter 2: Security in Cloud Computing

2.1. Literal review

Cloud computing is known as one of the big next things in information technology world [17]. Due to its architectural design and characteristics *(Flexibility/Elasticity, Scalability of infrastructure, Broad network access, Reliability, Sustainability*) imposes a number of security benefits which include centralization of security, redundancy, data segmentation and high availability [18][19].

Although there are many benefits from adopting Cloud Computing, there are also some significant barriers linked to/ pertaining to its adoption. The new concepts introduced by the Clouds, such as computation outsourcing, resource sharing and external data warehousing, increase the security and privacy concerns and create new security challenges. In addition to that, the large scale of the Clouds, the direct access to Cloud infrastructure and the proliferation of mobile access devices amplify Cloud vulnerabilities and threats. Thus, as Clouds' popularity grows progressively, more and more security concerns are raised, allowing them to become more attractive as attack targets due to the concentration of digital assets.

In general, Security is related to the important aspects of confidentiality, integrity and availability. In Cloud Computing, these important aspects of security, apply to the three categories of assets which are necessary to be secured: data, software and hardware resources.

Before we proceed with the presentation of the Cloud Security challenges proposed by the Cloud infrastructure, we should first clarify what Cloud Computing Security means as well as to analyze and understand what the security issues are. We also have to investigate the Cloud security attributes and to identify the security requirements including confidentiality, integrity, availability as well as transparency.

Security in Cloud Computing refers to the set of procedures, processes and standards designed to provide information security assurance in a Cloud Computing environment. It addresses both physical and logical security issues across all the different Service Models of Software, Platform and Infrastructure and it tackles also how these Services are delivered (Public, Private or Hybrid Delivery Model) [20].

Security issues are separated into **two categories,** according to different stakeholders: issues faced by **Cloud Providers** (organizations providing SaaS, PaaS or IaaS via the cloud) and issues faced by their **Customers** (companies or organizations who host applications or store data on the Cloud). Each one has its own requirements and capabilities delivered from one stakeholder to the other.

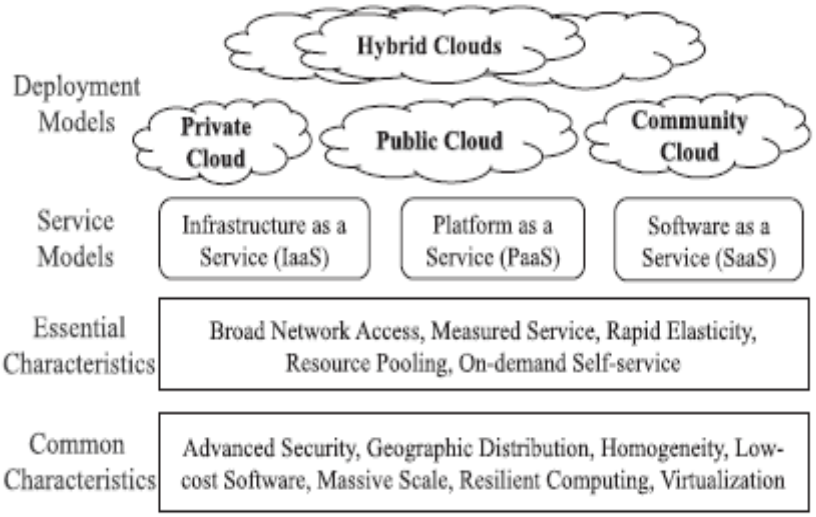
In all three models, the **Cloud Provider** manages and controls the infrastructures. The Provider is responsible for implementing and operating suitable infrastructure controls of fundamental importance, such as training, firewalls, physical security and others.

On the other hand, in all three models, the **Customers** have rights and responsibilities that will enable them to make more informed decisions before signing up with a Provider. Gartner presents below these seven rights and responsibilities that benefit both Service Providers and Service Customers [21].

1. The Right to Retain Ownership, Use and Control of one's own Data.
2. The Right to Service-Level Agreements that address Liabilities, Remediation and Business outcomes.
3. The Right to Notification and Choice about changes that affect the Service Consumer's business processes.
4. The Right to Understand the Technical Limitations or Requirements of the Service upfront.
5. The Right to Understand the Legal Requirements of Jurisdictions in which the Provider operates
6. The Right to Know what Security processes the Provider follows.
7. The Responsibility to Understand and to Adhere to Software License Requirements.

Providers and Consumers, these two stakeholders, need to negotiate and agree to the Security Properties in Cloud Computing. **(Figure 2)** shows the Cloud Deployment Models together with their infrastructure (IaaS, PaaS and SaaS). Cloud Deployment Models have similar internal infrastructure but vary in their Security Policies and user-access levels.

Figure 2 The NIST Cloud Definition Framework



Many researchers and practitioners discuss about Cloud Computing security challenges and issues. Plenty of them work on identifying attacks, vulnerabilities and threats and try to provide countermeasures, recommendations, frameworks, strategies and other security solutions (e.g.[22][23][24][25][26][27][28]).

Additionally efforts by some researchers present surveys on Cloud Security requirements such as confidentiality, integrity, transparency, availability, accountability, and assurance [29][30][31] .

While other researchers have addressed single attributes of Cloud Computing security such as data integrity, authentication vulnerabilities, auditing, *etc*. [32][33][34][35][36].

Researches by Organizations as ENISA list loss of control and governance as a top risk of cloud computing [37].The Cloud Security Alliance (CSA) lists data breaches and data loss as two of the top nine threats in Cloud Computing [38]. There are instead different aspects, with related issues, challenges and security controls that need to be considered and that can find application in different scenarios.

Cloud Computing is viewed as one of the most promising technologies in computing today, inherently able to address a number of issues. In the **Table 1** below, after the brief literature survey, we summarize, explain and describe the most popular security challenges in Cloud Computing

Table 1 Cloud Security Issues and Description

No. Issue	Cloud Security Issues Description – Questions
1. **Trust in remote execution:**	In a Cloud system, a customer must gain assurance that the base system executes his or her Cloud instance while protecting its integrity and secrecy, tantamount to running on the customer's own machine.
2. **Loss of governance:**	In a public Cloud deployment System, customers cede control to the Cloud Provider over a number of issues that may affect security.
3. **Data location:**	When you use a Cloud Computing Provider, your data travels over the Internet to and from one or more externally managed data centers. It may be in, or processed by, data centers in multiple locations around the world. Does the Cloud Vendor allow for any control over the location of data?
4. **Data availability:**	Can the Cloud Vendor move all their clients' data onto a different environment should the existing environment become compromised or unavailable?
5. **Responsibility ambiguity:**	Responsibility over aspects of security may be split between the Provider and the Customer, with the potential for vital parts of the defenses to be left unguarded if there is a failure to allocate responsibility clearly.
6. **Authentication & Authorization:**	The fact that sensitive Cloud resources are accessed from anywhere on the Internet heightens the need to establish with certainty the identity of a user. Strong authentication and authorization becomes a critical Concern.
7. **Isolation failure:**	Multi-tenancy and shared resources are defining characteristics of public cloud computing. This risk category covers the failure of mechanisms separating the usage of storage, memory, routing and even reputation between tenants.
8. **Compliance and legal risks:**	The Cloud customer's investment in achieving certification may be lost if the Cloud Provider cannot provide evidence of their own compliance with the relevant requirements, or does not permit audits by the Cloud Customer. The customer must check that the Cloud Provider has appropriate certifications in place. Which law applies to customers' data in the Cloud: The law where their data is located or the law where the data subject is located. International consensus on this issue has not yet been achieved.

9. Handling of security incidents:	The detection, reporting and subsequent management of security breaches may be delegated to the Cloud Provider but these incidents impact the customer. Notification rules need to be negotiated in the cloud service agreement so that customers are not caught unaware or informed with an unacceptable delay.
10. Management interface vulnerability:	Interfaces to manage public Cloud resources are usually accessible through the Internet. Since they allow access to larger sets of resources, they pose an increased risk, especially when combined with remote access and web browser vulnerabilities.
11. Application Protection:	Who is responsible for application security in the new world of Cloud Computing? Increasingly, we see Third-Party application Providers, who are not necessarily security vendors, being asked to verify the thoroughness and effectiveness of their security strategies. Nevertheless, the enterprise ultimately still bears most of the responsibility for assessing application security regardless of where the application resides. Application security is a critical component of any operational IT strategy and Web Applications are the Primary attack target for every Organization. Securing applications must be a Priority for Cloud Computing.
12. Data protection and Privacy:	It is the core issue in all challenges in this need to protect identity information policy component during integration and transaction histories.
13. Malicious behavior of insiders:	This damage in the cloud computing environment might occur within either or both the customer organization and the provider organization.
14. Auditing:	Is a report by an independent audit agency available for covering the Provider's Cloud services? Does the audit information conform to one of the accepted standards for security audit? Does the Provider have mechanisms to report to the customers both routine and exceptional behavior related to its services?
15. Privileged Access:	Who decides about the hiring and management of the administrator? Who decides about the access of the users in data?

When considering a move to Cloud Computing, customers must have a clear understanding of the potential security benefits and risks associated with Cloud Computing and set realistic expectations with their cloud provider. Failure to ensure

appropriate security protection when using Cloud Services could ultimately result in higher costs and potential loss of business, thus eliminating any of the potential benefits of Cloud Computing.

Cloud Computing could not be necessarily considered more or less secure than the current environment as it also create new risks, new threats, new challenges and new opportunities likewise any other new technology. However in the context of computing, although the terms security, privacy and trust are related they have different meanings. **Security** refers to a computing system's level of resistance to threats. **Privacy** most often concerns the digital collection, storage, and sharing of information and data, including the transparency of such practices. And finally **trust in the system,** is created when a Cloud Computing system is reliably secure and private for its users.

In addition, Cloud Computing technology itself is exposed to several problems with Security to be one of the major issues that could affect the adoption and the rapid development of Cloud Computing as it is the greatest challenge of Cloud Computing Systems [39] followed by issues regarding compliance, privacy and legal matters [41].

Many concerns are raised on the security issues since the Cloud Computing service is based on transferring data between the Service Provider and User. Until today, there have been numerous research efforts in the area of Cloud Computing security by various researchers. According to Kshetri, Almorsy et al., Lombardi and Di Pietro, Stinchcombe, Mansfield-Devine, Subashini and Kavitha, Abdul Nasir Khan et al. [41][42][42][44][45][46][47] the most important security issues in Cloud Computing are: trust, integrity, availability, authentication and authorization and confidentiality. Enisa [48] investigated the different security risks related to adopting Cloud Computing along with the affected assets, the risks likelihood, the impacts and the vulnerabilities in Cloud Computing that may lead to such risks. Bernd et al [49] discuss the security vulnerabilities existing in the Cloud platform. The authors presented the possible vulnerabilities into three categories related to technology, Cloud characteristics and security controls. The analysis done by David G. Rosado et al [50] examines the different existing approaches in the literature about migration processes to Cloud Computing while taking into account the security aspects that

have to be also moved to Cloud. Rebollo et al. [51] compare existing information security frameworks that have been specifically designed for the Cloud Computing environment using the clauses from the ISO/IEC 27002 standard as evaluation criteria.

Apart from the researchers that investigated security issues in Cloud there are also other efforts for examples of security frameworks and architectures. Ko et al. [52] investigate trust for Cloud Computing and propose a Trust Cloud framework that focused on accountability. Pal et al. [53] present their Cloud Security that has emphasized on the architecture and steps of interactions between different services. They explain the role of each major user, their agents and all the 15 steps involved. E.Fernandez et al. [54] activate appropriate countermeasures to respond to new threats for Cloud systems. Huan et al [55] presents framework – MobiCloud to enhance the functionality of MANET and cover security aspect in terms of risk management and secure routing. The National Institute of Standards and Technology (NIST) framework provides a common language for establishing cyber security. The core NIST framework provides a set of activities to identify, protect, detect, respond and recover without more specific examples and case studies implementing a full-security solution [56].

2.2. Security Policy in Cloud Computing

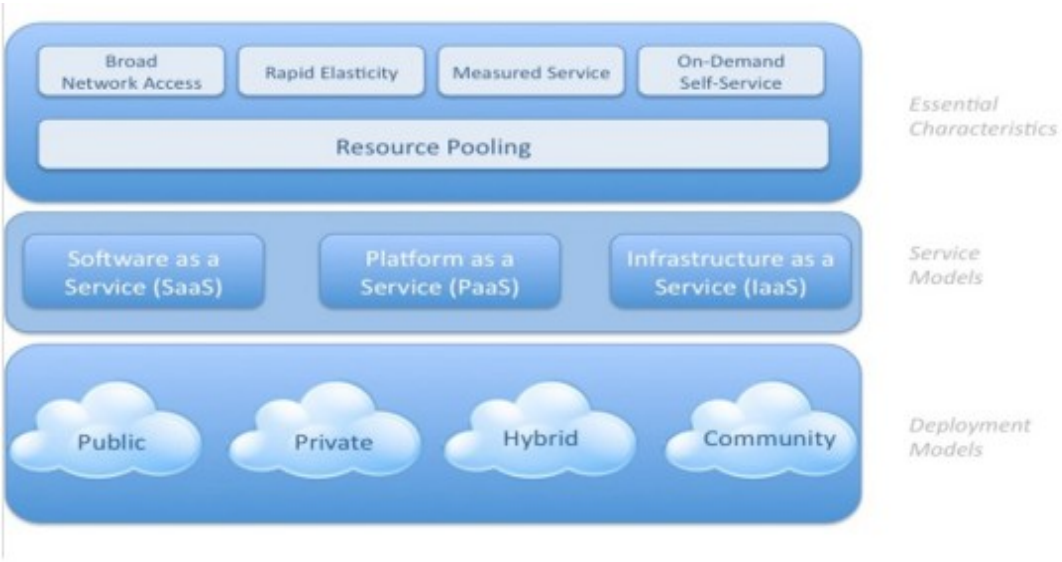
For the new era of Cloud Computing**,** the purpose of a Security Policy is to protect people and information, set rules for expected behavior by users, minimize risks and track compliances with regulation [57]**.** Considering the fact that in recent times anyone with an interest in information technology has come across the term Cloud Computing [58] it is really important to seriously consider the security issues in Cloud Computing: Are there any Security threats in Cloud Computing, that do not appear in non- Cloud Systems? Is the Cloud secure and safe for the users?

As Cloud Computing is achieving popularity, we attempt to demystify the security and privacy risks that are introduced because of its transformational nature [59]**.** The success of a Cloud Policy really depends on the way the security contents are addressed in the policy document and how the content is communicated to

users [60]**.** But, before we analyze all these risks, we should have a clear understanding of what "Cloud Computing" is.

Cloud Computing is a recent trend in Information Technology that moves Computing and data away from desktop and portable PCs into large data centers. It refers to applications delivered as services over the Internet as well as to the actual Cloud infrastructure, namely, the hardware and software systems in data centers that provide these services [61]**(Figure 3).**

Figure 3 Visual Model of NIST Working Definition of Cloud Computing



The advantages of Cloud Computing and specifically its ability to scale rapidly (through subcontractors), store data remotely (in unknown places) and share services in a dynamic environment can become a major flow in maintaining a level of privacy assurance sufficient to sustain confidence in potential customers. Cloud has exacerbated the strain on traditional frameworks for privacy that globalization has already started. To understand the importance of Cloud Computing and its adoption, we must understand its principal characteristics, its delivery and deployment models, how customers use these services and how to safeguard them.

As we mentioned in a previous chapter, there are three Service Models of Cloud Computing: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS) as well as three main Deployment Models which are: Private Cloud, Public Cloud and Hybrid Cloud [62][63][64][65][66][67]**.** These

Service Models place also a different level of security requirements in the Cloud environment. IaaS is the foundation of all Cloud Services, with PaaS built up on it and SaaS in turn built upon it. Just as capabilities are inherited, so are the information security issues and risks.

2.3. The problem of non-existing Security Policy

Cloud Computing is a new computing model originating from grid computing, distributed computing, parallel computing, virtualization technology, utility computing and other computer technologies. It exhibits many advantages such as large scale computation and data storage, virtualization, high expandability, high reliability and low price service. Trust and security in Cloud Computing are more complex than in traditional IT systems. **But, what is exactly the problem?**

In order to have a secure Cloud Computing deployment, it is necessary to consider the following areas: the Cloud Computing architecture, governance, portability and interoperability, traditional security, business continuity and disaster recovery, data center operations, incident response, notification and remediation, application security, encryption and key management, identity and access management [68][69][70]. Many of the security issues arising from the aforementioned areas have been already addressed in other systems. However, the specific characteristics of Cloud environments result into new security concerns.

A lot of researchers have spoken about Cloud Computing security challenges and issues without saying something different. The National Institute of Standards and Technology contends that security, interoperability, and portability are the major barriers to a broader cloud adoption [71]**.** Data confidentiality and service availability in Cloud Computing are also key security issues. A single security Methodology cannot solve the Cloud Computing security problem and many conventional and new technologies and strategies must be employed together for protecting the entire Cloud environment. Robert Gellman's report at the World Privacy Forum [72] focuses on privacy issues and legal compliance of sharing data in

the cloud. He mentions various legal issues such as the possibility of the Cloud being in more than one legal location at the same time with different legal consequences and such uncertainty making it very difficult to assess the privacy protection level offered to the users [73]**.** Also, ENISA investigated the different security risks related to adopting Cloud Computing along with the affected assets, the risks likelihood, impacts, and vulnerabilities in Cloud Computing that may lead to such risks [74]**.**

According to Al Morsy et al. [75] the Cloud Computing Model has different stakeholders involved, namely: Cloud Provider, Service Provider and Service Consumer. Each stakeholder has its own security management systems/processes and each one has its own expectations (requirements) from the other stakeholders. Cloud environments exhibit different architectures based on the services they provide, thus making it even harder to find 'global' security measures. Louay Karadsheh [76] examines the risks encountered by implementing the Infrastructure-as-a-Service (IaaS) model and discusses the role of security policies, Service Level Agreement (SLA) and compliance for enhancing the security of the IaaS Service Model. Subashini and Kavitha [46] describe the various security issues of Cloud Computing in relation to its service delivery model and they list some of the existing solutions that partly address the security challenges posed by the Cloud. Cheng and Lai [77] introduce the characteristics of the newly developed Cloud Computing technology first, and then they highlight the reasons for emphasizing the issue of information privacy in relation to new cloud applications. Vaquero et al. [78] analyze the security risks that multi-tenancy induces the Infrastructure-as-a-Service clouds and present the most relevant threats and relevant state of the art of solutions. Also, in the same paper they continue analyzing the open security issues and challenges that should be addressed. Even though the majority of the research work published focuses on security issues, legal and jurisdictional [79][80][81] and almost everybody accepts that there are a lot of security and privacy issues for Cloud Computing**,** only some of them mention the need for a Cloud Security.

For instance, Karadsheh [76] discusses the role of security policies, SLA and compliance for enhancing the security of the IaaS service model, by presenting several applicable policies. Furthermore, this paper discusses the possibilities of applying different types of security policies to enhance security of IaaS to acceptable

level, but they do not propose a Security Policy. Similar is the approach by Subashini and Kavitha [46] who describe the common security issues posed by the Cloud Service Delivery Models and the security threats posed by the IaaS Delivery Model, but they do not provide a comprehensive analysis of the specific threats to be addressed by Cloud Providers.

In an attempt to assist Cloud Providers to secure the environment that they offer and specifically for the Software-as-a-Service Model (SaaS), the next chapter presents the already reported threats to ease their comprehension. Because of these security threats, there are specific requirements that we claim must be clearly addressed in the Security Policy for the Cloud Environment. Our work focuses on the required structure and contents of such a Security Policy.

Chapter 3: Security Policy in Cloud Computing

3.1. Introduction

The aim of our Security Policy is to ensure a high common level of network and information security across Cloud Providers of Cloud Computing. The policy focuses on security outcomes that are necessary to achieve a proportionate and risk managed approach of security in order for the Organizations to function effectively, safely and securely.

Enforcing the Security Policy should result to:

- Harmonization of the different practices followed by the Cloud Providers.
- Enable Cloud Providers, Organizations and users to check and benchmark their information security capabilities.
- Help the Cloud Providers and Organizations to prioritize their investments on security.
- Establish Good Practices for information security for use across the public and the private sector.

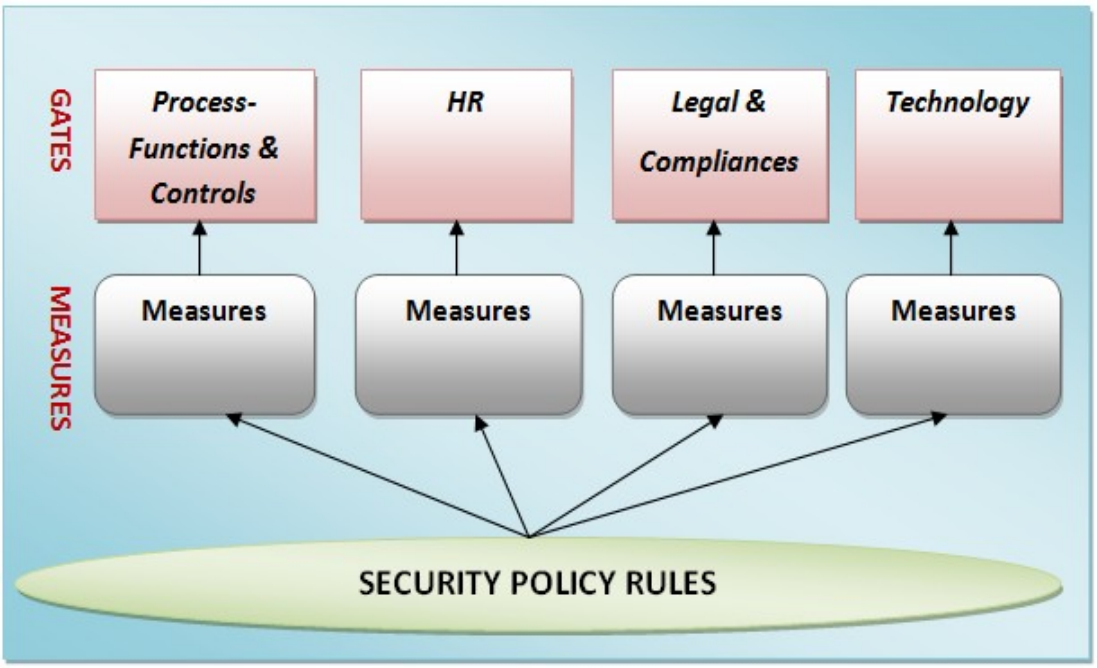
In our thesis, should we like to present the processing of our Policy with a process diagram it would look like the following:

Figure 4 The Processing of our Security Policy

The structure of the Policy includes **Four main Gates-Categories**:

- ***Process-Functions & Controls***
- ***HR***
- ***Legal & Compliances***
- ***Technology***

Figure 5 Structure of the General Security Policy



The **(Figure 5)** above illustrates the structure of the General Security Policy and the interdependencies among its components. The General Security Policy includes a set of high-level requirements in the form of Mandatory Rules for all Organizations. These Mandatory rules are grouped into four (4) Core Gates- pillars:

- ***Process-Functions & Controls***: This Core Policy aims to specify the necessary requirements for the successful implementation and administration of the processes, functions and controls of the Security Policy of an Organization.
- ***HR*****:** The scope of this Policy is to specify the requirements for the physical assets and human assets against possible threats such as the protection of data resources and the awareness of personnel through education against loss deriving from breaches of confidentiality, integrity or availability.
- ***Legal & Compliances***: This Core Policy addresses the requirements that will enable the protection and preservation of information which is the legal framework of the country and the regulations for processing the data.
- ***Technology:*** This Policy refers to the technical measures and procedures required for ensuring the truthfulness and trustworthiness of individuals who access the technology resources.

3.2. An Analysis of the Methodology of our Security Policy Framework – First idea

In this Chapter of this Thesis **we present the analysis of our first idea of** the Methodology that may be adopted for the development of a Cloud Security Policy (**Goal iii** - Implementation of Security Policy Rules and **Goal iv - General Recommendations for SaaS Security Policies)**. In order to test our first idea, we **highlighted some general possible threats** for a Cloud Provider who adopts the Software-as-a-Service (SaaS) model and then we choose one threat, proposing security measures and Security Policy Rules for this threat. The threats that we mention to the next paragraph can be employed for deducing the security requirements that must be satisfied by the Cloud Provider.

This Methodology assesses how security, trust and privacy issues can be addressed in the context of a Cloud Computing Security Policy. So, in our first idea, we analyzed the policy issues related to Cloud Computing, while we presented the proposed Methodology for a Cloud Security Policy, for Cloud Providers in the SaaS Service Model. Then we presented the linking of threats, security measures and Security Policy Rules for **Threat 5 (Introduction of damaging or disruptive software).**

The Cloud Computing Model involves different stakeholders: the Cloud Provider (an entity that offers the cloud infrastructure or /and services to the Cloud Consumers), the Service Provider (an entity that utilizes the Cloud infrastructure to deliver applications/services to the end users) and the Service Consumer (End user; an entity that uses services hosted on the Cloud infrastructure). Each stakeholder has its own expectations (requirements) and security management systems/processes [75]. For instance, if we consider user's expectations these expectations would be that the Cloud Provides: reliability and liability, security, privacy, anonymity, access and usage restrictions [82].

The decision of whether the Cloud Customer or the Cloud Provider (Service Provider) is responsible for a given control and for security and privacy depends on **three factors**:

a) The Cloud Model (SaaS, IaaS, or PaaS) chosen;

b) The extent to which the Cloud Customer is allowed to configure the Cloud Provider's controls;

c) Legislations, which may dictate the assignment of responsibilities and thereby overrides the previous two factors.

Next, **we highlight the possible threats** for a Cloud Provider who adopts the Software-as-a-Service (SaaS) model:

Threat 1: **Masquerading of user identity by insiders:** The threat of masquerading of user identity by insiders covers attempts by authorized users to gain access to information to which they have not been granted access. These users may attempt to gain access to that information by using another user's account.

Threat 2: **Masquerading of user identity by contracted Service Providers:** The threat of masquerading of a user identity by contracted Service Providers covers attempts by people working for a contracted Service Provider to obtain unauthorized access to information by using an authorized person.

Threat 3: **Masquerading of user identity by outsiders:** The threat of masquerading of a user identity by outsiders covers attempts by outsiders to obtain unauthorized access to information by posing as an authorized user.

Threat 4: **Unauthorized use of an application:** It covers various cases of unauthorized use of an application.

Threat 5: **Introduction of damaging or disruptive software:** This threat covers Viruses, Worms, Trojan Horses, logic bombs or any other form of malicious software.

Threat 6: Misuse of system resources: Identifies factors that increase the threat of misuse of system resources, covers people playing games on business systems, people using business systems for personal work, people downloading non-work related information from the internet, people setting up databases or other packages for non-work related matters.

Threat 7: Communications infiltration: This threat covers the following types of event: Hacking into a system using, for example, buffer overflow attacks, Masquerading as a server, Masquerading as an existing user of an e-

commerce application, Masquerading as a new user of an e-commerce application, Denial of service (deliberate), Flaming attacks, and Spamming.

Threat 8: Communications interception: This threat covers Passive interception and Traffic monitoring. The ease of interception is determined by two basic-factors: The medium of transmission and the type of protocols being used. Interception of some types of traffic on the internet is relatively easy. It can be achieved by attackers sending messages to target systems instructing them to send traffic via specific (hostile) machines.

Threat 9: Communications manipulation: Active interception, Insertion of false messages, Deliberate delivery out of sequence, Deliberate delay of delivery, Deliberate misrouting. If an attacker can force a message to be sent via a hostile host, the attacker may be in a position to intercept, alter and the forward the message.

Threat 10: Repudiation: This threat addresses cases of people denying that they sent a message (repudiation of origin) or that they received a message (repudiation of receipt).

Threat 11: Communications failure: Unavailability of Service Provider, Failure of data link, Non –delivery of message, Accidental delivery out of sequence, Accidental delay in delivery, Accidental denial of service. The Internet does not provide a service level agreement. There are no guarantees on how long it will take for a message to get to a recipient, or even that it will get there, eventually.

Threat 12: Embedding of malicious code: Includes email viruses and hostile mobile code (for example hostile Active X applets). Once on a network, they can quickly infect many machines causing significant disruption. Java and Active X raise a range of new security concerns. Users are now running code written by people from outside of the organization, sometimes from unknown sources. This code has often not been tested by the organization. There are concerns that hostile code written using these types of techniques could inflict damage on systems and networks.

Threat 13: Accidental misrouting: The threat of accidental misrouting covers the possibility that information might be delivered to an incorrect address when it is being sent over a network.

Threat 14: Technical failure of host: This threat covers failures of the CPU or other hardware items.

Threat 15: Technical failure of storage facility: This threat covers disk crashes and disk failures.

Threat 16: Technical failure of Print facility: This questionnaire identifies the factors that increase the threat for a technical failure of the print facility.

Threat 17: Technical failure of network Distribution Component: This threat addresses cases of network distribution components, such as bridges and routers, failure.

Threat 18: Technical failure of Network Management or Operational Host: This questionnaire identifies the factors that increase the threat of technical failure of a network management or operation host.

Threat 19: **Technical Failure of Network Interface:** Here the factors that increase the threat of failure of the network interface are identified.

Threat 20: Technical failure of Network Service: Here the factors that increase the threat of failure of the network service are identified.

Threat 21: Power failure: This threat covers the possibility that the power supply to the building may fail. The types of power failure covered include: spikes, surges, brown outs, black outs.

Threat 22: **Air conditioning failure:** This threat covers the possibility that operation may have to be suspended because temperatures in the location fall outside of acceptable parameters.

These threats are being used for illustrating where the dangerous points lurk at every level of the typical SaaS model in a Cloud Provider's environment.

In all three Cloud Models, the Cloud Provider manages and controls the infrastructure which comprises the servers, networks, electricity, human resources and site services. As such, the Cloud Provider is responsible to implement and operate suitable infrastructure controls such as employee training, physical site

security, network firewalls and others. Infrastructure controls are of fundamental importance. It is evident, from the complexity of Cloud Computing and the threats that the Cloud is facing, that the development and adoption of a Security Policy is necessary. Understanding the threats relevant to the SaaS Service Model will assist in formulating a well-established Security Policy.

Although much research, into tackling all security and compliance issues that come up in the cloud services, has been undertaken, we support that the creation of a Security Policy of Cloud Computing will limit all the possible risks that could appear.

Existing research analysis methodologies are not appropriate for Cloud Computing since threats in Cloud are different. The appropriate Security Policies designed for conventional architectures do not map well to the cloud environment. Cloud architectures must have well-defined security policies and procedures in place. As companies move to Cloud Computing, the traditional methods of securing data are being challenged. For instance, it may be difficult for the Cloud Customer to effectively control the data processing that the cloud provider carries out and thus to be sure that the data is handled in a lawful way. Failure to comply with data protection law may lead to administrative, civil and also criminal sanctions which vary from country to country for the data controller. It is therefore important all security requirements, including the ones that are only applicable to the Cloud environments, to be covered by a security policy. Therefore in this part we indeed provide a new methodology for assessing the threats/risks in Cloud, in order to identify new rules, as a final idea of our methodology that must be incorporated in the Cloud Security Policy. The work, in this part, does not result in a Cloud Security Policy. Instead, it proposes a methodology that may be used for the development of the appropriate Cloud Security Policy.

The proposed Methodology for the development of a Cloud Security Policy exhibits **three distinct levels**:

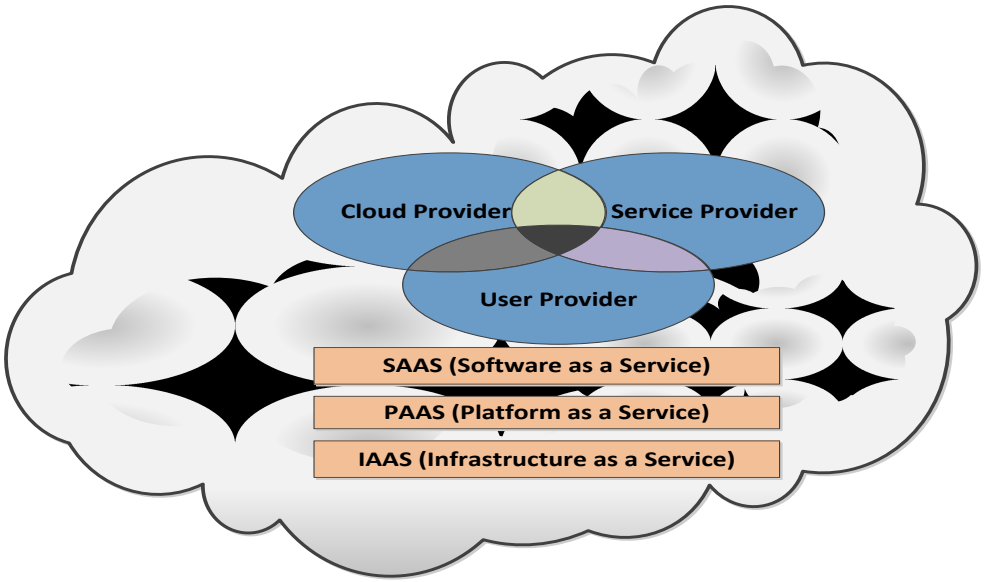
1) The Cloud Provider level,

2) The Service Provider level and

3) The User level.

Even though there are parts of the Security Policy that are common to all levels, each level will also exhibit dedicated Security Policy parts/rules. This three-layered classification of security requirements of Cloud Systems and the common parts of the Policy (colored) is illustrated in **(Figure 6).** As already mentioned earlier, the focus will be on SaaS (Software-as-a-Service) models.

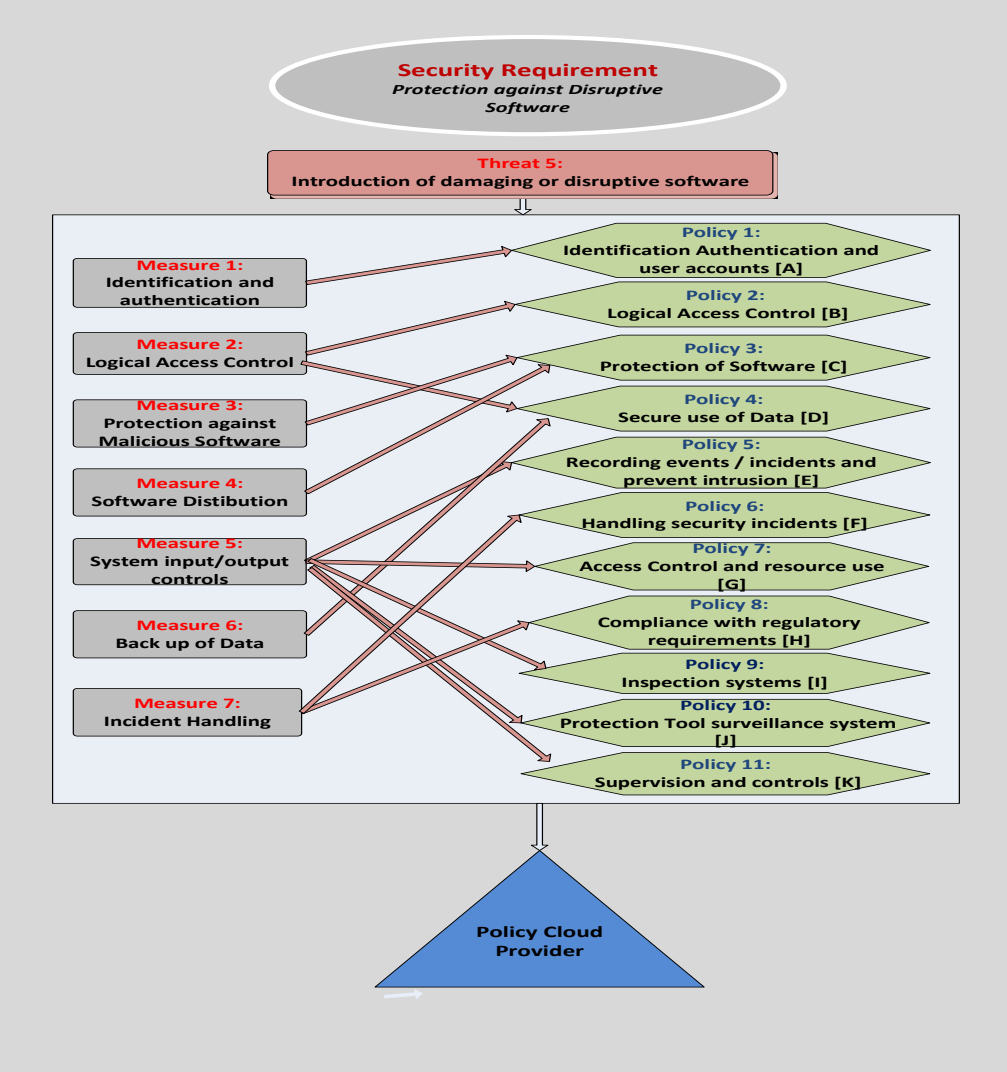
Figure 6 Security Policy Structure for Cloud Providers



The threats to which we referred in the previous section can be employed for deducing the security requirements that must be satisfied by the Cloud Provider. To demonstrate this, **a specific threat (Threat 5 - Introduction of damaging or disruptive software)** has been chosen to depict the correlation between Threat - Requirements – Security Measures – Security Policy Rules for a Cloud Provider (**see Figure 7).**

More specifically, in **(Figure 7)**, each security measure that can be employed for eliminating **Threat 5** is associated with the necessary set of rules that make up the security policy of the Cloud Provider. The same information is provided in more detail with more analysis below. Doing this type of analysis for each Threat that the SaaS Service Model is facing will help in formulating a well-established Security Policy.

Figure 7 Security Policy Rules covering Threat 5



A. Threats

Threat 5: *Introduction of damaging or disruptive software* will be analyzed as an example. In parallel the security measures and policy rules linked to that threat will also be examined.

B. Measures

The security measures associated with the aforementioned threat follow.

- Identification and authentication (*Security Policy Rules A)*
- Logical access control (*Security Policy Rules B & D)*
- Protection against malicious Software *(Security Policy Rules C)*
- Software Distribution *(Security Policy Rules C)*
- System input /output controls *(Security Policy Rules E & G & I & J & K)*
- Back-up of Data *(Security Policy Rules D)*

• Incident Handling *(Security Policy Rules F & H)*

C. Security Policy Rules

The **security policy rules** associated with the aforementioned threat and **security measures** follow.

1) Identification and authentication:

Users are identified uniquely ensuring that any action can be attributed to a specific user. This rule applies to the operating system level and to the application level, while the following minimum requirements should be satisfied.

• Each user has a unique identity (user ID).

• A list of users and their unique identities is maintained.

• Each authentication identifier is assigned to a user and is used by a single user.

• The system administrators have identities that correspond to accounts with elevated privileges.

2) Logical access control:

There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services. Specifically:

• Registered user accounts shall be reviewed for applicability at specific periods.

• Privileges shall be defined for specific business purposes.

• The allocation and use of privileges shall be restricted and controlled.

• Privileges and privilege allocation shall be reviewed for applicability at specified periods.

• The allocation and establishment of user passwords shall be controlled through a formal management process.

• Management shall review user rights at regular intervals using a formal process.

• Users shall be required to follow good security practices in the selection use of passwords.

3) Protection software:

Special care should be taken to control the development and maintenance of software applications. Specifically:

- Application development should be conducted with specific, scientifically accepted methodologies.
- Each new application must be accompanied by sufficient documentation in accordance with international standards.
- The risk analysis must fit into the requirements analysis.
- Systems utilized for the development and testing of software must be separate from the operational systems.

Software changes should be authorized prior to their implementation.

- Application software changes require approval by their respective makers.
- Any proposed change should be examined whether it affects the security of the information system.

Changes that affect - directly or indirectly - security requirements must be approved by the Security Officer. Specifically:

- The amendments must be made in the development/testing environment and should be tested prior to their application to the operational system.
- All changes must be characterized by a unique serial number.
- At each change request it is necessary to record the corresponding date and the name of the applicant.
- All software changes must be accompanied by documentation updates.

In case where urgent changes are required, it is necessary to ensure the following:

- Keep to a minimum the changes that will be performed.
- The modified files must be monitored.
- The Security Officer must be informed.
- Irrespectively of how urgent are the modifications, they must be tested before they are incorporated in the live system.

After any kind of modifications on the live system it is necessary to re-test system security. To this end the Security Officer must monitor the effectiveness of the security mechanisms after the modification took place.

4) Secure Data Management:

Data should be categorized according to the protection they need, as derived from the risk analysis or assessment of the head of Information System. The following categories have been identified:

- **Top secret**: information and critical data of the Information System that any disclosure or unauthorized modification will have direct impacts on the operation.
- **Confidential**: information and data that is important for seamless operation and should be subject to strict controls and protected.
- **Sensitive**: information and data that is subject to legislation on protection of personal data. Disclosure of this data requires specific permission / license.
- **Reportable:** information and data that can be disclosed.

The requirements of Information Security and the way data is processed vary according to the category of information. It is necessary to specify the authorized data recipients according to the above classification. Data processing must ensure procedural and technical resources that can be attributed to a specific individual. Therefore, all critical operations will be accessed in a strictly personalized way.

5) Recording actions / events and intrusion prevention:

Incidents of failure or non-routine functions of hardware or/and software, should be recorded and evaluated in relation to the operation that they support. Critical application systems should exhibit real time alarm systems. If there is a risk of invasion by external systems, intrusion detection and prevention systems should be in place. Systems will record the suspicious actions for the invasion and react automatically if this is dangerous for the security of the Cloud Provider. Proven invasions activate alarm system in real-time. The log files should be protected from loss or intentional corruption. The logs will be inspected by authorized personnel from time to time to highlight events / actions that endangered the Service Provider.

6) Handling security incidents:

A procedure for reporting faults and general security incidents is mandatory. There should be documented procedures that will ensure the timely and effective response to the occurrence of a security incident. This framework should include:

- The roles and responsibilities to be undertaken.
- Recorded evidence of what happened.
- Rescuing electronic material proving the breach (e.g., unchanged medium).
- The process of identifying the cause of the break up.
- The process of recovery.

7) Access control and resource use:

A strict registration process should be in place. As a minimum it should support the following:

- The access rights are determined through a rigorous registration process.
- The new system users are required to submit as an application in order to obtain an account.
- The application contains the elements of the applicant's position and the department to which he/she belongs.
- The application is signed by the user and his/her supervisor and it is forwarded to the IT director.
- The rights granted are always appropriate for the purpose that they serve.
- Inspections must be conducted by the Security Officer.
- If a user changes responsibilities and requires a new set of usage rights he/she should request them through a new application.
- When a user is given a new set of usage rights, the old rights should be removed.
- Users should take care of the safe use of their accounts.
- The idle time of a workstation should be limited. After some time of inactivity, workstations should get locked (e.g., password protected screen saver).

Regarding the use of system resources it is necessary to keep a list of all IT resources (hardware, software and documentation) and record the classification level of each resource.

Furthermore an Access Control Policy is necessary for controlling access to the resources of the Information System. The access control policy should exhibit the following:

• The access policy setting takes into account the principle of «need to know» (need-to-know).

• Users can use only the applications and the resources needed to perform the tasks associated with their position.

• The use rights assigned to each user category are inspected at least once every six months, with the responsibility of Information Security Officer to ensure that it is not given more rights than necessary.

• A copy of the password of the system administrator account must be kept in a safe place. The access to stored passwords should be controlled.

• System administrators should use different passwords for administrative accounts and the accounts they use.

• The exercise of rights of access users will be monitored and controlled in order to avoid the abuse of rights.

8) Compliance with regulatory requirements:

It is necessary to comply with existing legal and regulatory framework. Specifically:

• Monitor all legal and regulatory requirements and examine how they can be satisfied.

• Notification of the Data Protection Authority for keeping personal data.

• If records of sensitive data are kept, permission from the Data Protection Authority is necessary.

• Description of procedures to ensure the fulfillment of legal obligations for use hardware / software, i.e. the necessary licenses.

• Employ the necessary measures for protecting critical data from loss, destruction and unauthorized amendment in accordance with legislative requirements.

• Employ the necessary measures to ensure data protection and privacy as required by laws and regulations.

• Monitor and comply with all existing technical standards.

9) Inspection Systems:

Determine all audit requirements in accordance to the existing legal and regulatory framework as well as the procedures for controlled access to inspection tools in order to avoid damage, loss or misuse.

10) Protection of surveillance system:

Access to the tools of Information System surveillance shall be controlled. Specifically:

- Access to the monitoring tools should be restricted to authorized persons.
- Ensure that maintenance contractors will not have access to surveillance tools. If they need some data they should be provided by the system administrators according to the need-to-know principle.
- Restrict the access rights of the administrators in order to ensure that they will not be able to remove or change registration details of their own actions.
- In order to facilitate correct monitoring, the clocks of different systems must be synchronized.

11) Supervision and control:

Audit trails and event logs must be recorded in order to support the identification of violations or attempted violations and scrutinizing every suspicious incident. To this end, the following are necessary:

- To maintain monitoring data for all systems supporting multi-user access.
- To use special software for managing these files.
- To record the use of privileged functions.
- To record system startup.
- To record failed attempts.
- To record binding energy (log-on).
- To record disconnect actions (log-off).
- To record changes in access rights and use.
- To record the basic data for each suspected case.
- To record the user identifiers (User IDs).
- To record the time and the time of the event.
- To record the type of the event.
- To record the files accessed.

• To record the identity of the station.

• To record the state of the data before and after the changes.

• A copy of the audit data files must be kept in back up media (back-up).

• Data must be kept at least for a period of three months. In systems that manage classified information, data must be retained for the period specified by the national safety regulations.

• Copies are kept in a safe place, so to prevent any theft or sabotage.

• Access to log files is prohibited in those that do not have privileges (administrative rights).

• Log files should be protected from potential disaster.

• There should be integrity checks in place.

• Log files should be tested at least once a year.

• If the space available for log files reaches 75% of its storage capacity, an alarm must be produced.

• Inform users which of their activities are recorded by the system.

• Analyze logs of actions and events.

• Monitor the creation of accounts with elevated permissions.

• Identify deviations from normal use of system resources (e.g. unusually large number of prints from a user).

• The system automatically notifies the Security Officer when it detects certain suspicious events.

3.3. An Analysis of the Methodology of our Security Policy Framework – Final Ideal

As we succeeded in evaluating our First idea of the Methodology of Security Policy for one threat, then, we decided that this analysis could be carried out more targeted and accurate, if **we address only the possible threats of Cloud Computing**. So, after this evaluation, in each of these four Categories-Gates, to improve our understanding of security threats and our Policy generally, we first addressed all the possible threats of Cloud Computing **(Figure 8)** specifically related to the shared, on-

demand nature of Cloud Computing and then, we categorized them in one of **four** General **Categories - Gates** ***(Process-Functions Controls, HR, Legal & Compliances, Technology)***, as presented in **Table 2.** It is worthwhile to be mentioned that, in our Security Policy, we scope all the Cloud Security threats according to the Cloud Security Alliance [16] and some more new Cloud-specific security threats, according to our research. These new specific Security Threats are the ones that have influenced our Security Policy.

Thus, as we have already pronounced in our Goals and after a detailed review of the existing studies on security **(Goal i)** as well as of all the existing threats on security **(Goal ii),** we identify now the existing threats in Cloud Computing **(Goal iii)**

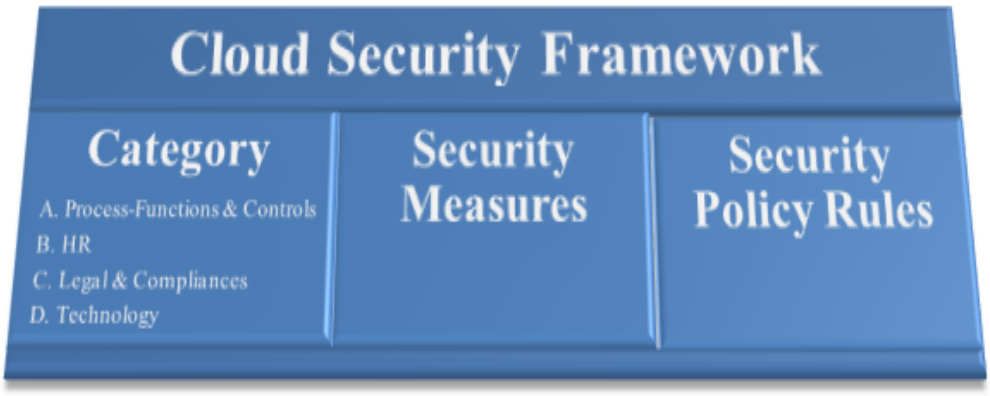
Figure 8 Security Threats in Cloud Computing

Table 2 Linking Threats with Category

Sr. No	THREATS	CATEGORY (of threats)
1.	Data Breach	**LEGAL & COMPLIANCES**
2.	Data Loss	**LEGAL & COMPLIANCES**
3.	Account Hijacking	**TECHNOLOGY**
4.	Insecure Interfaces & API's	**TECHNOLOGY**
5.	Denial of Service	**TECHNOLOGY**
6.	Malicious Insider	**PROCESS – FUNCTIONS CONTROLS**
7.	Abuse of Cloud Services	**PROCESS – FUNCTIONS CONTROLS**
8.	Insufficient Knowledge	**HR**
9.	Unintentional Disclosure	**PROCESS – FUNCTIONS CONTROLS**
10.	Data Protection	**LEGAL & COMPLIANCES**
11.	Luck of Standards	**LEGAL & COMPLIANCES**
12.	International Regulations	**LEGAL & COMPLIANCES**
13.	Subpoena and e-discovery	**TECHNOLOGY**
14.	Third Party Control	**LEGAL & COMPLIANCES**
15.	Back up vulnerabilities	**TECHNOLOGY**
16.	Cloud Burst Security	**TECHNOLOGY**
17.	Authentication and trust	**TECHNOLOGY**
18.	Lack of user control	**PROCESS – FUNCTIONS CONTROLS**
19.	Prohibition against cross border Transfer	**TECHNOLOGY**

Our work proposes a threat identification that will help Cloud Users, Cloud Providers and Organizations to make informed decisions about risk mitigation within a Cloud Security Policy Strategy. In **(Figure 9)** we present the **Methodology** of our **Cloud Security Framework (Goal iv).**

Figure 9 Methodology of Cloud Security Framework



It should be noted that this Cloud Security Framework sets out the basic minimum security requirements and some Cloud Providers may need to take additional measures appropriate to their particular Security Requirements and risk tolerance. In our work, we are based on the understanding of Provider's assets, threats and risk requirements and our General Security Policy Strategy is able to assess confidentiality, integrity and availability for Cloud Computing services.

The last tier of the General Security Policy consists of relevant **Guidelines to Cloud Providers** in order to help them implement **Policies Rules.**

In particular**, this Thesis includes:**

- Detailed guidelines and considerations for the implementation of the Requirements.
- Guidelines and considerations for the implementation of the Cloud specific rules.

It is worthwhile to be mentioned, that the parameters, considerations and the capabilities that have been presented in previous chapters **(2.1, 2.2)** in this Thesis, have become an input to this research and are connected with the requirements of Cloud Computing for the implementation of Cloud Computing. Managing Security Risks proportionately and cost-effectively combined with a proper application of the defensive Security at a Cloud Providers' level will:

- Achieve a high and effective level of network and Information Security within the Organizations and users.

- Develop a culture of Information Security for the benefit of citizens, consumers, business Organizations.
- Address, respond and especially prevent network and Information Security problems.

For the support of the Cloud Providers in the application of these Cloud Requirements, the Security Policy provides several guidelines. These guidelines are included in the next chapters of this Thesis, the Guidelines (**Goal iv – General Recommendations).**

Chapter 4: Auditing our Methodology

4.1.Introduction

The involvement of numerous stakeholders worldwide accents Security in a crucial issue in Cloud Computing achieving an acceptable Security Level in Cloud environments is much harder compared to other traditional IT systems due to its specific Cloud characteristics such as: architecture, openness, multi-tenancy, etc. Conventional security mechanisms are no longer suitable for applications and data in the Cloud since new security requirements have emerged. Furthermore, there is a clear need for a trusted Security Audit method for Cloud Providers. This chapter identifies the security requirements that are specific to Cloud Computing and highlights how these requirements are linked to the Cloud Security Policy while illustrating the structure of a General Security Policy Model. It also proposes a methodology that can be adopted by Cloud Providers for auditing the security of their systems. Although Cloud Security Concerns have been mentioned as one of the top challenges pertaining to Cloud adoption, it is not clear which security issues are specific to Cloud Computing. ISACA and Cloud Security Alliance presented guidelines to mitigate the security issues in cloud [101][102]. P. Radha Krishna Reddy et al. [103] introduced a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing types and the service delivery types. Ramgovid et all [104] presented the management of Security in Cloud focusing in Gartner's list [105]. However, there are several questions that remain open like: Which are the security requirements that exist only in Cloud? What is the structure of a security policy for cloud environments? And does the user have to solely depend on the service provider for proper security measures? By utilizing the general Security Policy cited in [106], we are proposing a methodology for auditing the Security level of a Cloud Provider. In this chapter, we present the Cloud specific security threats, while we propose a list of General Recommendations that should appear in every Security Policy of SaaS environments. Then, we present the proposed Model-Methodology for auditing the Security level of a Cloud Provider and at the end we provide conclusions derived from the undertaken survey .

4.2. Cloud Specific Security Threats

Cloud Computing is a mixture of technologies that supports various stakeholders (Cloud Provider, Service Provider and Users). But how a Cloud differs from other models and what exactly the organizational impact is when moving to a Cloud is not clear yet. For the users, Cloud Computing is a synthesis of computing services without any understanding of the technologies being used. For an organization, it is a scale of different services provided to users for innovating and growing their business income. However, the threats that an organization faces as it shifts to Cloud Computing environments are different. **Table 3** illustrates the treats that we will scope in our paper: **Table 4** provides the nine Cloud security threats according to the Cloud Security Alliance [7], while **Table 5** provides more New Cloud-specific security threats.

Table 3 Security Threats in Cloud Computing

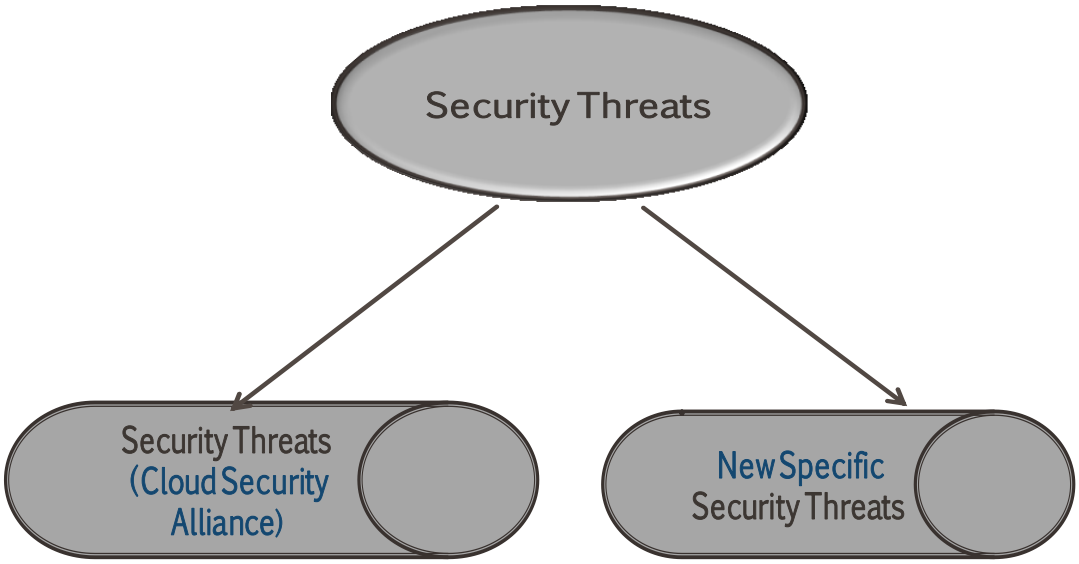


Table 4 A list of Nine Cloud-specific Security Threats (Cloud Security Alliance)

Nine Security Risks (Cloud Security Alliance)	Description
Data Breach	The data from various users and organizations reside together in a Cloud Server. If somebody breaches the Cloud then, the data of all users will be attacked.
Data Loss	For both consumers and businesses, the prospect of permanently losing one's data is terrifying. Data loss may occur when a Server dies without its owner having created a backup.
Account Hijacking	A process through which an individual's email account, computer account or any other account associated with a computing device or service is stolen or hijacked by a hacker.
Insecure Interfaces & API's	Cloud Computing providers expose a set of software interfaces or APIs that customers use to manage and interact with Cloud Services. The security and availability of general Cloud Services is dependent upon the security of these basic APIs. These interfaces must be designed to protect against both accidental and malicious attempts.
Denial of Service	Another common attack for Organizations that operate or use Internet connected services such as websites or Cloud services need to be aware of threats that can disrupt service. A DoS attack makes your network unavailable to the intended users by flooding them with connection requests.
Malicious Insider	It's unpleasant to think that someone in your organization might be collecting a paycheck and planning to repay you with malice. But it does happen. Taking measures to protect yourself doesn't mean you don't trust the others. Systems that depend "solely on the Cloud Service Provider for security are at great risk" from a malicious insider.
Abuse of Cloud Services	This threat is more common in IaaS and in PaaS models. Hackers and other criminals take advantage of the convenient registration, simple procedures and relatively anonymous access to Cloud Services to launch various attacks.
Insufficient Knowledge	Rather than security issues, a lack of knowledge regarding Cloud Computing is precluding businesses that don't already use the service from taking the plunge. It is the main factor in preventing uptake.
Unintentional Disclosure	This risk is the malicious or accidental disclosure of confidential or sensitive information. In a Cloud Computing environment it could be happen many times.

Table 5 New Specific Security Threats to Cloud Computing

New Specific Security Threats	Description
Data Protection	Customers may not know where their data is being stored and there may be a risk of data being stored alongside other customers' information.
Lack of Standards	Several times Cloud Providers may perform similarly in a different way. Security standards for cloud environments that have been developed by international organizations are necessary.
International Regulations	Providers and users must comply with the legal issues related to the data that they collect, process and store.
Third Party Control, Subpoena and e-discovery	This is the most crucial concern in the cloud, since third party access can lead to a loss of confidential information.
Back up vulnerabilities	Providers must ensure that all sensitive data is backed up in order to facilitate quick recovery in case of disasters. Also, they should use strong encryption schemes to protect the backup data. The users need to separately encrypt their data and backups in order to avoid access by unauthorized parties.
Cloud Burst Security	In cloud environments there are applications consisting of several virtual machines. Such bursting machines need strict security policies that will prevent them from being vulnerable.
Authentication and trust	Data in the cloud may be modified without user's permission. As such, data authenticity is very important and needs to be guaranteed.
Lack of user control	In Cloud environments there is a potential lack of control and transparency since a third party holds the data.
Cross border transfer of data	In this case the concern is if the protection level of the destination country is equivalent to that of the originating country. In cases where the destination country has laws that respect the conditions and requirements set by the domestic legal framework data can be transferred, otherwise the transfer is prohibited.

In Cloud Computing environment the threats are diverse depending on the Delivery Models. In the previous tables we have discussed, in general, the risks focusing more on SaaS Cloud Providers. All these risks require substantial security attention. Cloud Providers need to mitigate these security threats by adopting the appropriate security measures in accordance with a well formed Cloud Security Policy. By addressing the aforementioned requirements, Cloud Providers will gain the trust of their users. The proposed Methodology provides solutions for each threat and at the same time, it conforms them to the provisions of the Cloud Security Policy.

4.3. General Recommendations for the Security Policy

Despite that the security capabilities for a SaaS environment have been developed, we argue that if the Security Policy of the Cloud Provider features some general recommendations that reflect the security requirements of an organization or/and a user then, the Providers will mitigate the security risks and concerns. Thus, if an organization chooses a SaaS Provider that complies with the following recommendations, this would facilitate a Third Party Auditor to check the security level of the Cloud Computing environment. It would also ensure that the provision of all resources and the behavior of all users will be in accordance with the recommendations set and thus, compliance issues will be automatically avoided.

Table 6 SaaS Security Recommendations

SaaS Security Recommendations
1. Invest in Education
2. Establish Cloud Strategy
3. Decide what goes to and under which control
4. Invest in Technologies that protect users' data
5. Audit the Provider's Services

1. Invest in Education: There is a need to identify the learning goals, the content structure and the learning experience of Cloud Computing in terms of a senior high technology education, in order to help learners coping with this emerging technology. At the same time, the research result could be effectively applied on integrating emerging technology into a formal technology education.

2. Establish Cloud Strategy: We would like to suggest a few basic steps that organizations can follow to define their Cloud Computing roadmap. This is not just about remedying the problem but more about creating a long-term strategic use of cloud computing that should bring a sustainable strategic value to the enterprise. This would result to a safer Cloud environment and an easier way to test which Provider is more suitable for the users.

3. Decide what goes to and under which control: One of the major problems that security professionals face is to identify which control goes where. The user should not manage or control the underlying Cloud himself as he is not obliged to have technical or managerial knowledge of Cloud. It's for the organizations to choose the controls that meet users' specific needs and provide security certifications and accreditations that would facilitate the procedure of audit control and would strengthen the trust towards Cloud Computing environment.

4. Invest in technologies that protect users' data: If the Provider is not certified for its software and hardware infra-structure by any industry security certification authority then the security control will be much more difficult. Users need a secure and consistent "place" for their data and expect through their SLA (Service Level Agreement) to have a report that will inform them about the encryption solutions, intrusion detection and prevention solutions, data centers and all other technologies and mechanisms that the provider uses .

5. Audit the Provider's services: Organizations or Third Party Control must offer to Cloud Service Providers the means to make their security data available to potential customers. Organizations provide outsourcing services that affect the control environment of their customers. The important element to remedy this problem would be to conduct an audit. The Cloud Auditor should create an audit plan that includes policies and procedures and could be used as a reference guide.

The key thing, to take away of this problem, is a conduct with a Cloud Auditor. The Cloud Auditor should have an audit plan, so that can be used as a guide. The Cloud Auditor provides a standard way to present, automated statistics about performance and security. So, SaaS Customers need only to select the safest Cloud Provider, according to the security functions of the auditor.

It is necessary to agree on the way recommendations for the Security Policy are presented to the Providers. They should be able to identify the recommendations that are relevant to the users' requirements and concerns. SaaS risks can be managed through this approach and Cloud Providers will be able to utilize systems with complex and dynamic environments more easily. Furthermore, the proposed approach will save time, effort and money to the Providers.

4.4. Proposed Model-Methodology for Auditing

The proposed Model provides a solution to the security challenges of Cloud Computing. If Cloud Providers and Organizations follow this model, using the gates of the policy, they will succeed in having a secure Cloud Computing environment. More specifically, the (**Figure 9)** below illustrates the structure of the General Security Framework and the interdependencies among its components. The Cloud Provider or a third party auditor must follow and audit the four general Gates - Categories (***Process-Functions & Controls, HR, Legal & Compliances and Technology***) to avoid threats. In each category it is necessary to ensure and check what provisions are covered by the Cloud Provider according the following security measures- examples. A further analysis of how security controls should be linked to every security measure will be also provided. Until present, the aforementioned audit process was rather difficult because there is no commonly agreed procedure or a common Policy and thus, customers cannot easily rank their Providers in terms of the Security level they support. So, the proposed Cloud Security Model addresses the relationships of security measures and places them in a context together with their relevant security controls and concerns.

Therefore, the proposed General Security Policy requires that **the Third Party**

auditor will audit the following four **Categories-Gates**:

Category 1 – Processes/Functions Controls: It must be ensured that the security measures adopted by the provider meet the requirements set by the Cloud Security Policy. Users expect to have available a report about Cloud Provider's operations, logs and industry security certifications, as well as the assurance of the auditor that the provider is doing these right.

Category 2 – HR: A great number of executives, managers and personnel are not familiar with what cloud computing means. There is a lack of awareness about cloud environments together with a lot of concerns about the various risks and data security. Providers must aim to promote security through education and sharing of good practices with the personnel. The auditor should check if the cloud provider is considering the provisions of this category.

Category 3 – Legal Requirements & Compliances: The auditor should check whether the provisions of the legal framework under which the data is stored or transferred are satisfied. Moreover, the auditor should know in which country the data is located and thus what the regulations, the restrictions for storing, the processing and transferring that data are. In this way, the user can be assured that the storage and data processing carried out by the Cloud Provider Legally.

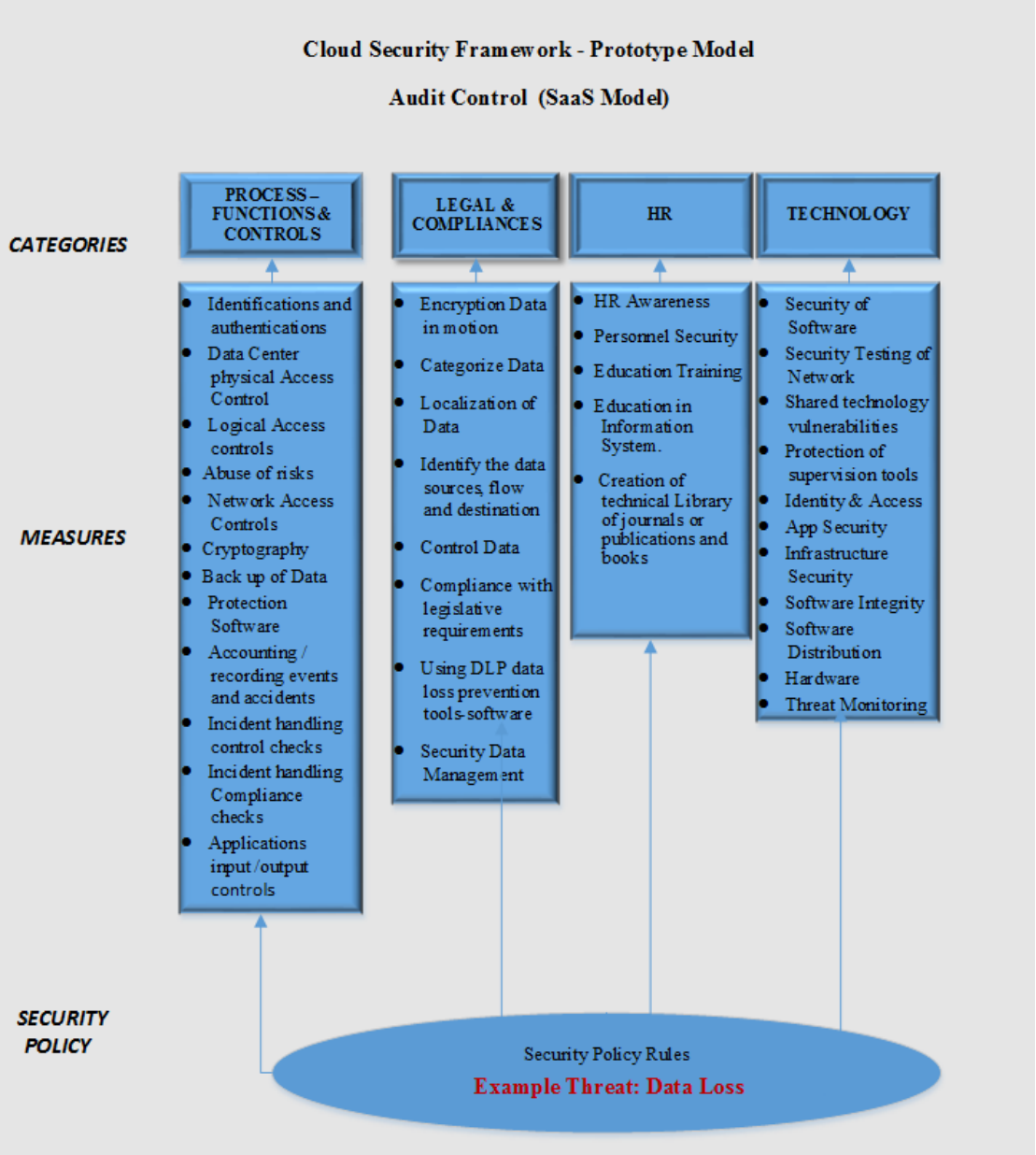
Category 4 – Technology: The auditor should check what software and hardware technologies are used as well as what the applications and the devices users entrust for storing and possibly sharing their data are. Cloud providers might also allow users' data to be transferred to another vendor or platform growing this way the risks on the users' data.

Third party auditors can utilize this framework to understand the SaaS Provider's security context. All the previous threats are assigned to one of the four categories associated with the necessary security measures and then linked with a set of rules that make up the Security Policy of the Cloud Provider. **Table 7** illustrates the relation between Threats and Categories whereas **(Figure 10)** depicts the proposed Cloud Security Framework. In our Auditing example, we choose the **"Data Loss"** Threat that belongs to Category Legal & Compliances.

Table 7 Linking Threats with Category - Auditing Example

Sr. No	THREATS	CATEGORY (of threats)
1.	Data Breach	**LEGAL & COMPLIANCES**
2.	**Data Loss**	**LEGAL & COMPLIANCES**
3.	Account Hijacking	**TECHNOLOGY**
4.	Insecure Interfaces & API's	**TECHNOLOGY**
5.	Denial of Service	**TECHNOLOGY**
6.	Malicious Insider	**PROCESS – FUNCTIONS CONTROLS**
7.	Abuse of Cloud Services	**PROCESS – FUNCTIONS CONTROLS**
8.	Insufficient Knowledge	**HR**
9.	Unintentional Disclosure	**PROCESS – FUNCTIONS CONTROLS**
10.	Data Protection	**LEGAL & COMPLIANCES**
11.	Luck of Standards	**LEGAL & COMPLIANCES**
12.	International Regulations	**LEGAL & COMPLIANCES**
13.	Subpoena and e-discovery	**TECHNOLOGY**
14.	Third Party Control	**LEGAL & COMPLIANCES**
15.	Back up vulnerabilities	**TECHNOLOGY**
16.	Cloud Burst Security	**TECHNOLOGY**
17.	Authentication and trust	**TECHNOLOGY**
18.	Lack of user control	**PROCESS – FUNCTIONS CONTROLS**
19.	Prohibition against cross border Transfer	**TECHNOLOGY**

Figure 10 Cloud Security Framework



In the previous (**Figure 10)**, we illustrate the solutions that are available for securing SaaS environments in accordance to the proposed Security Policy. We have gathered the cloud computing threats and we have suggested measures addressing them.

In the following **Case Study** - example we select the **"Data Loss" Threat** which is connected with the **Legal & Compliances** Category and is crucial for Cloud Computing. In the analysis that follows, we propose security measures that can be adopted in the cloud as well as a set of Rules that will form our Security Policy.

Table 8 Case Study – Data Loss Threat

Threat: Data Loss
Category: *Legal Requirements & Compliances* ***Measures:*** With the exception of some general purpose measures, there are specific techniques and security mechanisms for Cloud Computing environments. The security measures associated with the aforementioned threat are the following: 1. Encryption of data in motion 2. Categorize data 3. Localization of data 4. Identify the data sources, flow and destination 5. Control data 6. Compliance with legislative requirements. 7. Using DLP Data Loss Prevention Tools-software 8. Security Data Management
Security Policy Rules: The Security Policy Rules associated with the aforementioned threat and security measures follow: **1. Encryption of data in motion** The encryption techniques should follow international best practice and should have broad acceptance by the international community as to their effectiveness. Data in transit need to be confidential. • For symmetric encryption to storage media or data transmissions, the appropriate algorithms and key lengths should be selected in accordance with the international authoritative bodies. (e.g. NIST) • Where a digital signature is required the laws of the country in which the provider is located should be adopted, as well as the decisions of the European Union. **2. Categorize data** Data should be classified according to the protection they need based on the evaluation of their criticality through the risk analysis and assessment by the Cloud Provider. **Top secret:** information and vital data for the Cloud Provider of which any disclosure or unauthorized change will have direct impact on operations. **Confidential:** information and data relevant to the operation of the Cloud Provider which should be subject to strict controls. **Sensitive:** information and data subject to laws that protect personal data the disclosure of which needs specific permissions/license. **Reportable:** information and data may be disclosed. The security requirements vary according to the category of the information owned. Each processing of data must be guaranteed by procedural and technical resources that can be attributed to a specific individual. Therefore all critical actions will have strictly personalized access. **3. Localization of data** In Cloud Computing data travels over the Internet to and from one or more regions where the data centers are. The user of a Cloud must know in which country the servers are located, how the data is processed and to which legislation is subject. So, at any moment the Provider should be able to inform its users about these issues. Data located in different countries, provinces or municipalities are subject to different legal frameworks. For this reason, it is essential for the contract between the Provider and the user to clearly state the geographic region of the servers.

4. Identify the data sources, flow and destination

Data should be accomplished. This process must include data discovery and data fingerprinting that provides a better understanding of, whom, where, when and in what format the information is being generated and in what devices it is being stored. In addition, identification of the Cloud Services being used and the type of data being transferred to the cloud is an important step during this process.

5. Control Data

In the absence of control data in a Cloud environment, no activity is recorded which modify or delete users' data. User should know how these data is handled. No information is stored like which nodes have joined, which programs have run, what changes are made. In addition, users want to know who from the Providers have the data, where and in what way they are being processed.

6. Compliance with legal requirements

- Recording and documentation of all legislative and regulatory obligations of the service and how all these obligations are addressed.
- The privacy of the users should be ensured.
- If sensitive personal data is collected, permission from the Data Protection Authority should be acquired.
- Description of the procedures adopted for ensuring compliance with the legal Requirements and regulations.

7. Using Data Loss Prevention Tools-Software

Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network and prevent them by monitoring, detecting and blocking sensitive data while in -use (endpoint actions), in-motion (network traffic), and at-rest (data storage). Users also want DLPs to be used for describing software products that help a Provider to control what data end users can transfer.

8. Security Data Management

When an outside Party owns controls and manages resources, users should be assured that data remains private and secure and that their organization is protected from damaging data breaches. Users want to be sure that data is not readable and that the provider offers strong key management. Cloud Providers should implement access policies which ensure that only authorized users can gain access to sensitive information.

Chapter 5: Security Policy Rules and Required Procedures for two crucial Threats of Cloud Computing

5.1. Introduction

Cloud computing is the most accurate paradigm of next generation internet-based distributed computing systems providing an innovative business model for organizations. It offers potential benefits including cost savings, flexibility and improved business outcomes for organizations. Despite the potential advantages of Cloud Computing the security problem is one of the major issues remaining questionable. As the security is a vital factor in the Cloud, different security threats have been discovered in these years, which need to be carefully considered by the Cloud Service Providers.

In this chapter of this thesis, two crucial security threats of Cloud Computing systems are presented and are assigned to one of four Categories – Gates of our Security Policy. We facilitate both Users and Providers to know about these security threats and we propose security measures that Providers could use to evaluate and secure their services. Finally, we describe the necessary Security Policy Rules and Required Procedures for these requirements. Our approach tackles the loss of unsecure Cloud Computing environment, especially for the Software-as-a-Service Model (SaaS), providing guidance in the form of a set of rules which can be utilized for monitoring the implementation and effectiveness of security controls in Cloud environments.

The processes involved in evaluating Cloud Computing can be difficult and subject to legal restraints, technical and compliance requirements on the actions of stakeholders, despite this we present an evaluation of transferring a system to Cloud Computing that Organizations could follow. Although every environment is unique, Security Privacy issues are most important for all the systems, the same with Cloud Computing. As Cloud Computing rapidly gains popularity, it is important to highlight the threats that are specific to Cloud. In our previous work, in chapter 3, we

presented these threats according to Cloud Security Alliance [16] and new one that are specific to Cloud Computing. Although security policies are varying, Cloud Providers should follow some rules and procedures, when working with a new Cloud Computing.

In this part of our thesis, we **propose** a **General Security Policy** focusing on the Cloud Computing and **an evaluation of transferring a system to Cloud that Organizations could follow**. We recommend that if Cloud Providers follow a Cloud Computing Strategy in order to define their approach to Cloud Computing, the organizations and the users will imitate the risk when moving to the Cloud. There are many different ways to approach Cloud Security Policy. In our work, we based on the understanding of Provider's assets, threats, risk requirements, and our General Security Policy strategy is able to assess confidentiality, integrity and availability for Cloud Computing services. When Organizations or Customers consider a movement to Cloud Computing, they must have a clear understanding of potential security risks associated with Cloud Computing. By utilizing the general Security Policy and the proposed Methodology for auditing the security level of a Cloud Provider, we provide in this chapter a list of security policy rules and considerations for two of Cloud Computing threats**.** Each security consideration contains more detailed information about the security Policy Rules. The aim of this Security Policy Framework in this chapter is, firstly, to protect information, people, organizations that use Cloud Computing services and secondly, to analyze the security implications of cloud computing, so we could reach to the creation of a Trusted Cloud Service Provider.

5.2. Literature Review

Many of the security issues arising from the aforementioned areas have been already addressed in other systems. However, the specific characteristics of Cloud environments result into new security concerns; Cloud architecture is fundamentally different from other systems, the Cloud environment is by nature multitenant with shared resources, and the location of the data and the local privacy requirements

will not be controlled by the user. Since no proper standards for Cloud Computing exist, it becomes extremely difficult for a company to secure the services that it offers or uses through a Cloud. Considering the technical reports and safety instructions in Cloud Computing organizations such as NIST, the ENISA and the CSA and research of Fernandes et al., Srinivasan et al. etc. They gathered significant risks and safety issues concerning the use cloud computing services to provide the Cloud model:

- **The National Institute of Standards and Technology:** lead efforts to develop standards and guidelines in close consultation and collaboration with standards bodies, the private sector, and other stakeholders. NIST present the core set of Security Components and how to use it for a particular Cloud Deployment Model [83].
- **The Cloud Security Alliance (CSA):** has created industry-wide standards for Cloud Security, seeing both the promise of Cloud Computing, and the risks associated with it. For this purpose, CSA released the "Security Guidance for Critical Areas in Cloud Computing", the "Security as a Service Implementation Guidance" and the "The Treacherous 12 - Cloud Computing Top Threats in 2016" [84][[85][86]. It is worthwhile to be mentioned that the last report focuses on 12 specifically threats related to the shared, on-demand nature of Cloud Computing.
- **ENISA:** investigated the different security risks related to adopting Cloud Computing along with the affected assets, the risks likelihood, impacts, and vulnerabilities in Cloud Computing that may lead to such risks. In his reports presents the best practices and a list of recommendations, covering all aspects of Cloud Computing [87][88].
- **Fernandes et al:** addresses vulnerabilities, threats and attacks and proposes taxonomy for their classification [89].
- **Madham Kumar Srinivasan et all**: analyzes the current security challenges in Cloud Computing environment based on state-of-the-art cloud computing security taxonomies under technological and process-related aspects [95].

Although, the Cloud characteristics and the basic issues are presented by these Standards and some Researchers, there are still some threats that are not covered from these analyses. Our work comes to fulfill these gaps and presents a more analytically view of the threats and a best suitable approach for the appropriate Security Policy of Cloud Computing.

As Cloud Computing is frequently exposed to different types of threats which can cause various types of damages that might lead to significant financial losses. Any discussion of threat in Cloud Computing must begin with "**What is a threat",** as a first step? **Table 9** lists the definition of threats compiled from a range of resources. In general, in computer security the various definitions refer to a possible danger that might exploit a vulnerability to breach security and thus cause possible harm. A threat can be either "intentional" (e.g., an individual cracker or a criminal organization) or "accidental" or otherwise a circumstance, capability, action, or event.

Table 9 Contending definitions of Threats

Source	Definition
ENISA	*Any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service [91].*
National Information Assurance Glossary	*Any circumstance or event with the potential to adversely impact an IS through unauthorized access, destruction, disclosure, modification of data, and/or denial of service [92].*
ISO 27005	*A potential cause of an incident, that may result in harm of systems and organization [93].*
The Open Group	*Anything that is capable of acting in a manner resulting in harm to an asset and/or organization; for example, acts of God (weather, geological events), malicious actors, errors, failures [94].*
NIST	*Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access,*

	destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability[95]
ISACA	*Anything (e.g., object, substance, human) that is capable of acting against an asset in a manner that can result in harm [96]*

The **Second Step** is to understand the nature of security threats. Cloud computing has transformed business, and created new security threats. It is a vast technological achievement, a mix of technologies with different Models and Services, a key technology enabler for the future Internet.

But the threats that an organization faces as it shifts to Cloud Computing environments are different than the other traditional systems. While there are many threats to Cloud Security, the **(Figure 8)** in Chapter 3 focuses on threats specifically related to the shared, on-demand nature of Cloud Computing.

5.3. Evaluation of transferring a System to Cloud

The evaluation of the possibility of carrying an information system in Cloud Computing environment according to our Security Policy, should examine the following Initial Step with 5 Stages detailed below. It is worthwhile to be mentioned that this Initial Step of the evaluation, should be examined before an Organization follows our Security Policy (**Figure 11).**

Stage 1: Exploring Compliance

At this stage of the Methodology considers the requirements of the legal and regulatory framework regarding whether allow installation of an information system in cloud environment. The investigation is done using the control / test point of the:

Table 10 Control point of the Compliance

Attribute	Criterion	Answer
Exploring Compliance	The legal and regulatory framework allows for the installation of an information system in cloud environment	Yes or No

The persons who should have the responsibility of evaluating the suitability for installation / transport to a Cloud environment system answering the question in the previous table. If the answer to the panel question is positive ("YES"), the evaluation proceeds to Step 2. Otherwise, if the answer is negative ("NO"), then the evaluation is completed. As a result of the evaluation, the system may not be installed / transferred to a Cloud environment.

Stage 2: Investigation of technical system characteristics

At this stage of the Methodology explored some basic technical characteristics of the system under consideration, as to the establishment / transfer of a Cloud environment. These technical features considered necessary to allow the system to be installed / transferred to a Cloud environment. The investigation is done using the control points / criteria are presented in the following table:

Table 11 Control point of Technical System Characteristics

Attribute	Criterion	Answer
System architecture	Does the system follow service oriented or layered web-based architecture?	**Yes or No**
Virtualization	Does the system support virtualization technologies and is capable of packaging the overall software stack (source code, software libraries, operating system) in one or more virtual machine images	**Yes or No**

The persons who have shouldered the responsibility of evaluating the suitability for installation / transport to a Cloud environment system answering the questions in the previous table. If the answer to all the questions in the table is positive **("YES"),** the evaluation proceeds to **Step 3.**

Otherwise, if even one answer is negative **("NO"),** then the evaluation is completed. As a result of the evaluation, the system should not be installed / transferred to a Cloud environment.

Stage 3: Evaluation of requirements and operating system features

At this stage of the Methodology explored requirements and functional characteristics of the system under consideration as to whether the installation / transport in Cloud environment. The investigation is done with the use of specific control / criteria points, which are presented in the following table (checklist). Not considered at this stage of system security and data of which are the subject of investigation of Step 4 Methodology

Table 12 Control points of Requirements and Operating System features

Attribute	Criterion	Answer (0,1,2)
Computational requirements	Does the system load increase significantly in specific periods (e.g. magazines or based on any landmark / decision / deadline)?	
Integration/communication with on-premises infrastructure	Has the system limited integration / communication requirements (by frequency and trading volume) with on-premises systems)?	
Sharing data	Has the system has limited access requirements to data hosted on databases on-premises infrastructure?	
Performance requirements	Has the system standard / limited performance requirements or have higher requirements but which are expected to be sufficiently covered by a Provider of Cloud computing services? (taking into account and delays that may be caused by network infrastructures that mediate communication between users of the Cloud environment)	
Mobile working/ Teleworking	Does the system serve functions that appeal to mobile users?	
Scalability	Is the system is especially designed to fully exploit the potential fluctuation of the resources provided by a Cloud environment?	

The Board members who have the responsibility of evaluating the suitability for transport to a cloud environment system answering the questions in the previous table. Responses take a value in the **range of 0 to 2**, where in:

- **0 =** the system does not have this feature.
- **1 =** the system has this feature, but it does not belong to the basic elements.
- **2 =** this feature belongs to the basic elements of the system.

The **result** of the evaluation can be a value in the **range 0-12,** leading to one of the following options:

1. Evaluation Grade ≥ 8: The system appears appropriate in terms of requirements and functionalities for installation / transport to a Cloud environment. The evaluation proceeds to Step 4.

2. Grade ≥ evaluation 5 and <8: The system appears partially suitable in terms of requirements and functionalities installation / transport to a cloud environment. The Board members decide whether to proceed with further investigation (i.e. whether to go to Step 4).

3. ≤ 4 Rate this: The system is not suitable to be installed / transferred to a cloud environment and the evaluation is completed.

Step 4: Risk assessment and system security requirements

At this stage of the Methodology explored the possible consequences that may arise for the organization of the new threats and security issues introduced by the use of Cloud Computing. Exploring in step 4 requires to take into account the specificities of Cloud Computing. The following table **Table 13** shows the steps for risk assessment and system security requirements with the changes brought about by the use of Cloud Computing.

Table 13 Steps for Risk Assessment and System Security Requirements

Sr.No	Step	Instructions
1.	**Select SaaS Model**	This step selects the SaaS model which examined as to the exploitation.

2.	**Acceptable Risk level**	Select the maximum degree of risk that may be accepted by the body.
3.	**Asset Identification**	In accordance with common practices.
4.	**Asset Valuation**	The valuation of each asset should be done by the respective asset owner, who estimates the value of the consequences / costs that would have been possible loss of a safety feature (minimum: confidentiality –integrity –availability)
5.	**Threat identification**	In this step is the identification of threats In addition to the threats that can create security problems in that system are examined further and threats arising specifically due to the use of SaaS Cloud Computing. Note that you will only realize the threats that are applicable in the SaaS Model selected in step 1.
6.	**Threat assessment**	This step assesses the threats identified earlier based on the probability of the event.
7.	**Vulnerability assessment**	This step estimates the degree of vulnerability of each asset based on the likelihood of security feature of successful violation of (confidentiality –integrity –availability) of a threat.
8.	**Risk Calculation**	In accordance with common practices.
9.	**Management of threats / vulnerabilities**	For goods with a degree of risk that exceeds that defined by the body (in Step 2) maximum acceptable value (acceptable risk level) in investigating security measures that could minimize the likelihood of threats (threat assessment) or to reduce vulnerabilities the agency. Then, the desired countermeasures selected for implementation.
10.	**Recalculate risks**	At this point again performed from steps 6, 7 and 8 taking into account the efficiency of the additional security measures that were selected in step 9. If after the application of countermeasures even a risk of exceeding the maximum acceptable level of risk determined in step 2, then this SaaS Cloud Model is not appropriate for this information system and the evaluation is completed. Otherwise, the choice of the Model Cloud could be further examined on the basis of economic criteria (Step 5).

Step 5: Evaluate economic feasibility of transition to Cloud SaaS

At this stage of the methodology, originally conducted market research for specific Providers Cloud SaaS and then becomes, for although cases where the system is already in operation, cost-benefit analysis (financial analysis only) for alternative cloud SaaS implementation solutions, where the test solution is to implement SaaS cloud and the competitive scenario of the current situation (Business-as-Usual),while in cases where the system is under design only investigated the relevant costs of all solutions (ie alternative Providers of Cloud and on operating premises) for the reference period (also with the method of discounted cash flows).

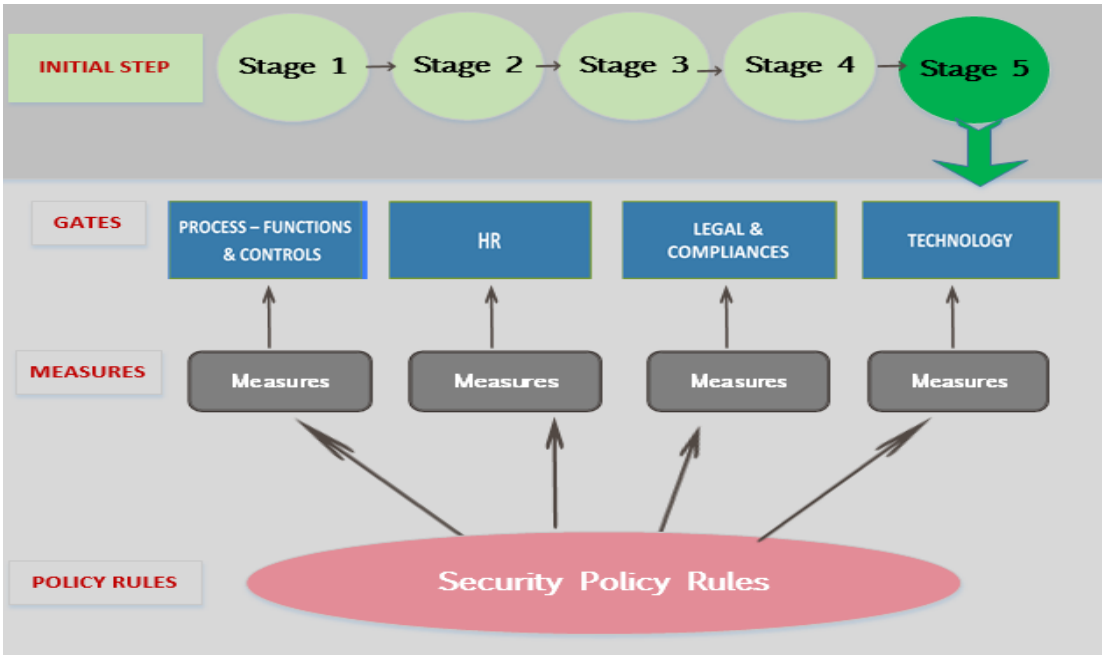
The analysis will show if it is a financial benefit from the installation / transport to a Cloud environment system and how much is it in the long run. The result of the analysis results in one of the following options:

- A **positive** or very positive effect analysis (i.e. clear economic benefit from the transport to a Cloud environment system): This system appears suitable for transport to a cloud environment.
- A **Negative** effect analysis (i.e. No apparent economic benefit from the transfer system in Cloud environment): The system does not appear suitable for transport to a Cloud environment.

The final recommendation for the transition or not in the Cloud made by the analyst, after balancing quality and quantity all the benefits (financial highlighted in Step 5, technically in Step 3), the remaining risks (Step 4), any other quality features (if any), strategic decisions etc.

After this evaluation of transferring a System to Cloud, our **Overall Methodology of Cloud Security Framework** with the evaluation will be with an Initial Step with five stages as presented below in Figure 11**.** So, if the result of the analysis of transferring a system to Cloud is positive, that means the systems is suitable for transport to a Cloud environment, the Organizations is ready to follow our Cloud Security Framework that consists of Four Gates-Categories, Measures and Security Policy Rules , as presented in (**Figure 9).**

Figure 11 Overall Methodology of Cloud Security Framework with the evaluation



5.4. Two types of threats in Cloud Computing – Case Studies

Cloud computing has transformed business, and created new security threats. It is a vast technological achievement, a mix of technologies with different models and services, a key technology enabler for the future Internet. Many of the security issues and threats that need to be addressed in Cloud Computing are already known in other systems. But the Cloud Computing system has certain characteristics and attributes that create new threats.

Organizations as ENISA [97][98] presents a list of threats and mentions that loss of control and governance as a top risk of cloud computing. The Cloud Security Alliance (CSA) lists data breaches and data loss as two of the top nine threats in Cloud Computing [99]. There are instead different aspects, with related issues, challenges, and threats that need to be considered and that can find application in different scenarios.

In this Chapter of our thesis, of all the threats that we presented previously, we decided to select, two specific threats that are crucial for Cloud Computing, and are

characteristic of every Gate –Category of our Policy. The first one is the **"Lack of user control"** and the second is the **"Insufficient Knowledge".** As we can mention in **Table 14,** its one exist in another Category of our Security Policy. The first one **#threat1 "Lack of user control"** belongs to **Category A – Processes/Functions Controls**: and the second one **#threat2** "**Insufficient Knowledge**" belong to **Category C – HR** according to our Methodology.

Table 14 Two Crucial Threats and their Categories

Sr.No	THREATS	CATEGORY (of threats)
18.	Lack of user Control	A. PROCESS-FUNCTIONS & CONTROLS
8.	Insufficient Knowledge	B. HR

In the Analysis that follows, we propose the appropriate security measures that can be adopted in a Cloud System and then we give a set of Security Policy Rules for these measures that will form our Security Policy. Selecting appropriate security controls optimally require a correct reading of the threat environment. Our goal is to provide an identification deliverable for these two threats that can be quickly updated to reflect the Security Policy of Cloud Computing.

It is worthwhile to be mentioned that the **#threat1 "Lack of user control"** in Cloud Computing appears, because it is an a multi-tenant third party control system and it has luck of transparency and limited user control, since a third party holds the data. The Cloud Provider may subcontract some resources of a third party whose level of trust is questionable. In cloud also the technical control is given to the Cloud Computing Provider, and customers often want to have an external audit of this provider. So, logging and auditing information may change by default or not of a user.

The **#threat2 "Insufficient Knowledge"** in Cloud Computing systems is the most usual threat because it is stopping businesses from earning money with the not appropriate use of Cloud.

Therefore, in our Methodology in General Security Policy, in the **Category A - Processes/Functions Controls**, we gather all the operations, logs and industry security functions that an organization has to do, during the being in Cloud Computing environment. Also, in the **Category B- HR,** we conclude all the awareness about Cloud environments and the concerns about the various risks that personnel and managers must have education and sharing of good practices in the organizations.

5.5. Case study of the 1st Threat - Proposed Security Policy Rules

As Cloud Computing rapidly increases, it is important to highlight the threats. Through our approach, we managed the SaaS threats, so Cloud Providers will be able to minimize risk in their environments and increase the trust of their systems. In the previous work, we illustrated the solutions that are available for securing SaaS environments, in accordance to the proposed Security Policy. We have gathered the Cloud Computing threats and we have suggested measures addressing them. The proposed analysis can fulfill the entire list of security requirements of every threat and is a part of our General Security Policy of Cloud Computing. With the guidelines of this, the Third Party Auditors can utilize this framework to understand the SaaS Provider's security context.

Therefore, in our thesis**,** we analyze two Case Studies as Examples that are covered by the following Provisions and the following Security Policy Rules of the Cloud Security Policy.

In the following analysis of **Case Study - Example** 1, we select the **#threat1 "Lack of user control",** which has to do with the **Process –Functions Controls**. In the analysis that follows we propose security measures that can be adopted in the Cloud Computing and confront this threat, and then propose a set of Rules that will form our Security Policy of Cloud Computing.

Access control sounds simple, until we tease rights and permissions for every user in Cloud environment. In Cloud Computing, the multiple operating systems,

mobile platforms, access to non managed systems, make more complicated to control users. As all control is given to the Cloud Computing Provider, Customers often want to have an external audit of this Provider. Therefore logging and auditing information has to be stored and protected in order to enable verification.

Table 15 Security Policy for the Threat1 "Lack of user control"

Example 1
Threat: Lack of user control
Category: Process – Functions & Controls
Measures: *With the exception of some general purpose measures, there are specific techniques and security mechanisms for Cloud Computing environments. The security measures associated with the aforementioned threat are the following:* 1. Identification and Authentication 2. Data Center Physical Access Control 3. Logical Access Controls 4. Abuse of risks 5. Network Access controls 6. Cryptography 7. Back up of Data 8. Protection of Software 9. Accounting/Recording events and accidents 10. Incident handling Compliance checks 11. Applications input/output controls
Security Policy Rules for Requirements of Category A (Processes-Function & Controls): The security policy rules associated with the requirements of the Category A (Processes-Functions & Controls) and belongs there the threat "Lack of user control". **Business continuing:** A business continuity plan should be in place in order to ensure the availability of all critical services and assets have critical functions, the absence of which could lead to many unwanted situations, even to threat of human life. Some of these functions include health and safety systems, large scale

financial transactions etc. To identify and mitigate those risks, thus providing uninterrupted services for critical governmental functions, Cloud Provider shall follow a series of steps that are called Business Continuity planning (BCP). The whole procedure needs the employment of many other security policy elements, such as asset evaluation, risk management, incident response, reporting etc. The first step of adequate Business Continuity planning is identification. Cloud Provider shall evaluate assets, business functions, and differentiate critical from non-critical ones. This impact assessment has to be done according to:

- functions/services whose disruption is unacceptable (e.g. health systems),
- critical governmental infrastructure (e.g. power plants),
- environmental and other factors (e.g. areas with earthquake history),
- critical assets/functions that will result from risk management processes.,

After asset identification and impact assessment, it is important that Cloud Provider identify the best and most cost-effective solutions for recovering from disaster scenarios. Thus, solution for Business Continuity might include, but not limit to:

- Disaster Recovery (DR) Sites,
- Spare software/equipment,
- Data replication methodologies,
- Hard copies of critical data,
- Offices for staff to work in case of emergency,
- Methodologies for working without IT infrastructure.

Developing and implementing a Cloud Provider Information Security Policy:

All the Cloud Providers shall develop and implement an Information Security Policy adapted to the Organization's information security requirements

- The Security Policy ensures that:
    - Information will be protected against any unauthorized access
    - Confidentiality of information will be assured
    - Integrity of information will be maintained
    - Availability of information for business processes will be maintained
    - Legislative and regulatory requirements will be met
    - Business continuity plans will be developed, maintained and tested
    - Information security training will be available for all employees
    - All actual or suspected information security breaches will be reported to the CISO and will be thoroughly investigated
- Procedures exist to support the policy, including malware/virus control measures, passwords and continuity plans.
- Business requirements for availability of information and systems will be met.

- The Information Security team is responsible for maintaining the policy and for providing support and advice during its implementation.
- All managers are directly responsible for implementing the policy and ensuring staff compliance in their respective departments.
- Compliance with the Information Security Policy is mandatory.

Baseline Security Procedures and Measures:

Implement and enforce fundamental security procedures and measures to achieve a baseline integrity and availability level for the Services provided

- All procedures pertaining to the daily use of the Information Computer Security shall be documented
- A well-defined procedure for data back-up shall be in place
    - Proper data back-up shall take place regularly
    - Back-up media management and storage is of great importance
- A well-defined procedure for detecting, preventing and removing malware and virus software shall be in place
    - A legally-acquired and up-to-date anti-malware/anti-virus solution shall be chosen as the Organisation's default
    - Every new or alien removable media and/or executable program shall be scanned before gaining access to the Cloud Provider ICT infrastructure
    - The anti-malware/anti-virus solutions in use shall themselves be protected
- All software or hardware changes, removals, alterations, upgrades and updates shall have the permission of the Application / Infrastructure Heads and the Asset Owner and shall be logged in a suitably protected storage (e.g. a data storage device protected by encryption or an external data storage device kept in secure office furniture)
- All critical or important administrative actions shall be logged in a suitably protected storage
- All important software and hardware malfunctions shall be logged in a suitably protected storage and their impact on the Cloud Provider security shall be assessed

Access Control:

Access to important information assets shall be strictly controlled and regulated to ensure that it does not endanger the security of the Information System and its data.

- Well documented procedures for authenticating users and devices shall be in place and enforced.
- Access control procedures shall suit the security requirements of the protected information asset and the business needs of the Organisation

- Granting of access rights to users shall take into account the following:
  - It shall follow well-defined procedures
  - It shall be enforced by well-defined access control means
  - Only authorized personnel may grant access to information assets
  - Users need to make a binding declaration that they are responsible for protecting their access tokens (passwords, passphrases, hardware tokens etc.)
  - Users shall be given clear instructions on the use and protection of their access tokens and shall be made aware of where they can find updates and corrections to these instructions
  - Access of third parties, contractors, sub-contractors and temporary staff shall be strictly controlled and monitored.
- Regular audits shall take place to ensure that
  - There is no misuse of any given access right
  - All access rights are immediately revoked when they are no longer required (e.g. when an employee leaves the Organisation or changes position within the Organisation)
  - Access control procedures shall evolve and follow
    - technological changes
    - the renewed business needs of the Cloud Provider
    - the results and recommendations of IT auditing and other security checks

Network Security:

Information Systems connected to a network have greater security needs as they are exposed to more dangers, for this reason added security countermeasures need to be established.

- All devices belonging to the internal network shall by authenticated using a suitable authentication mechanism
- By default Internal networks shall not be directly connected to external networks unless necessitated by business needs. If and when a connection is required, then the connection:
  - Shall have the authorization of the Application / Infrastructure Heads.
  - Shall use suitable mechanisms to ensure the confidentiality, integrity and availability of the internal network's information assets and systems.
- Proper security mechanisms (e.g. encryption) shall be employed to ensure the confidentiality and integrity of important information exchanged between the Cloud Provider and another Cloud Provider or Third Party.
- The employed security mechanisms shall themselves be protected.
- Communication shall be protected using anti-malware/anti-virus solutions.

- Interconnected systems have greater security needs from isolated ones.
    - All non-essential services and ports shall be permanently disabled.
    - Continuous monitoring of the network is required.

Telecommunication Services Security:

All network services acquired by external Telecommunication Providers shall have a Service Level Agreement (SLA) that takes into account security issues.

- Telecommunication services shall be constantly monitored.
- The binding agreement of the Telecommunication Provider shall include terms pertaining to the security of the provided services.
- In case of security incident, it shall be clear which Party and to which extend is responsible to handle it.

Guidelines for Applying Physical Security Rules

Identifying Physical Assets:

The term physical asset includes the buildings, rooms, equipment a Cloud Provider is using. The assets may be at the Cloud Provider's possession or they may be at its plans to obtain.

In defining physical assets, the following guidelines should be considered:

- Only assets that are used by the Cloud Provider's need to be defined.
- If multiple assets of the same type are used, and are likely to be subject to similar risks, these may be grouped together and only defined once.
- Assets that carry out multiple functions can be classified as multifunction assets.

Develop and Implement Cloud Provider Physical Security Policy

Threat and vulnerability assessment:

Risk analysis method will reveal the potential threats against facilities, employees and clients. Depending on the identified value of assets, both physical and electronic, the need for the implementation of countermeasures will be revealed.

Countermeasure selection and recommendation:

Cloud Providers shall put in place physical security protection measures that match the evaluated security risk. They shall put in place the necessary building and entry control measures for areas that have been characterized as "restricted". Any attempt for an unauthorized access shall be detected and an effective response shall be activated.

Security Policy Management:

There shall be adequate procedures for implementing, maintaining, auditing and reviewing the

Information Security Policy

Security management:

Security management should be based on risk assessment and should be dynamic, encompassing all levels of participants' activities and all aspects of their operations. The requirements of security management depend upon the level of involvement, the role of the participant, the risk involved and system requirements.

Continual Reassessment:

Of information security and making of appropriate modifications to security policies, practices, measures and procedures.

Risk assessment:

Risk assessment will help to identify threats and vulnerabilities and to determine appropriate controls to reach to acceptable levels of risks. Risk assessment should be sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications.

- *Threat* is defined as any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.
- *Vulnerability* is a weakness of an asset or group of assets that can be exploited by one or more threats.
- *Risk* is defined as the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation.

Security Incidents Handling

Assurance and Reporting:

Policy requirements, as well as regulatory or other obligations, shall be integrated in the Organization's everyday operations, as well as to those of delivery partners and Third Party suppliers. In order to accommodate this need, the Organization shall have installed a system that will:

- inform all parts on their compliance responsibilities,
- ensure that requirements have been integrated into business processes,
- include procedures for reporting non-conformities and
- provide mechanisms for reporting to upper management.

The aforementioned system will correlate information from lots of different sources, such as systems and networks (log files, uptime reports), ERP systems (HR, maintenance planning),

scheduled human input and post mortem reports.

Recruitment Controls:

Casual staff shall undergo appropriate recruitment controls, in accordance to the Law. Organizations who own an Information System may request a higher level of assurance of a person's suitability to perform a particular role, based on their risk assessment policy, through appropriate recommendations to the Information Security Team. Organizations should always ensure the proportionality between the extra recruitment controls and associated risks. All extra recruitment controls, if additional to the existing will be included to the Scheme of Service and will be published by the Cloud Provider.

Identification of Positions requiring a Security Clearance:

The identification of positions should be based on Government Organisation's risk assessment results and the Cloud Provider's Security Policy. Cloud Provider should keep a record of all identified Security Positions and should follow appropriate screening procedures for granting a Security Clearance according to the instructions/recommendations of the National Security Authority (NSA).

Post-Verification:

Upon the completion of the baseline and any incremental recruitment controls imposed by the Organization, Cloud Provider shall ensure that the employee's recruitment record is created. This record contains all the checks that have been applied during the recruitment process and accompanies the employee throughout his/her employment life-cycle.

Reporting changes of personal circumstances:

Employees who have access to Cloud Provider's resources should be obliged to promptly report any changes in their personal circumstances that might imply unreliability or a conflict of interest. This obligation should be depicted in a corresponding document that will be signed during the employment agreement phase.

In order to support this obligation and effectively manage the reporting capabilities, Cloud Provider shall ensure that all the necessary arrangements have been established and communicated to all employees. These may at least include the specification of:

- the formal procedures that all staff should follow for reporting personal changes,
- the contact point for the reports,
- in which cases an employee is required to inform the relevant appropriate authority.

Cloud Provider shall support on-going personnel security management by staying in line with any obligations they have to the Public Service Commission and ensuring that the formal reporting procedure is communicated to all Cloud Provider's employees. To this end, the Cloud Provider

should be responsible to remind this obligation to all employees at regular intervals, through relevant updates.

Upon designing the reporting procedure, Cloud Provider should take into consideration that access to personal information should also be restricted based on the "need to know" principle.

In regards to those employees that hold a Security Clearance, the Cloud Provider is responsible to inform the National Security Authority (NSA) for any changes they are aware of or any concerns they might have about the continued suitability of their employees.

Incident Reporting:

Cloud Provider shall establish a well-defined policy for Incident Handling and should communicate the formal procedures for incident reporting to all staff. In addition employees should also be strongly encouraged to report any changes in personal circumstances of other employees, colleagues or contractors, they might be aware of, that could potentially introduce a conflict of interest and harm the Organization. This obligation is essentially critical when violations or changes of personal circumstances concern employees who hold a Security Clearance.

Termination of employment controls:

There are many cases where an employee might leave from a specific post. The most common ones are: retirement, resignation, end of contract, transfer to another Organization within the public service or division, leave long duration (e.g. for health/personal reasons) etc. Organization shall ensure that:

- Employees who are about to leave Organisation are subject to a number of termination of employment controls, and be obliged to return all Organisation 's resources and access media,
- Employees who are about to undertake a different position or to be transferred to another division within the Organisation are also subject to controls that are similar to the termination of employment controls in terms of access rights to organisation's Information resources and organization equipment management,

Through the establishment of formal procedures that Organization should follow when an employee is about to leave his current post. Organizations shall stay in line with the procedures defined by the Public Service Commission and their obligations as defined by the Public Service Law and relevant regulations. To this end organization must:

- Submit a proposal to the PSC through formal procedures.
- Make sure that the officer who is about to leave, has no financial obligations towards the state of if he has such obligations he shall settle them and no disciplinary or criminal case is pending against him.

In addition, when an employee leaves the Organisation and also a minimum set of controls that

should be applied in order to ensure protection from possible access violations. An indicative list of checks includes:

- Returning all assigned equipment, hardware and software, including mobile and portable devices, as well as any manuals, documents and information stored on electronic media.
- Returning all kinds of access media, cards, keys or tokens etc. that grant physical access to the Organisations' buildings, offices, rooms and logical access to Information Systems.
- Disabling all employees' user accounts.
- Removing employee from all mailing lists and groups.
- Renewing any common passwords that were given to the user, for accessing ICT resources.
- Notifying division managers and co-workers that the employee or contractor has terminated his employment/collaboration with the Organisation.
- Signing an agreement similar to the recruitment agreement, about employee's obligations to the Organisation.

Methods to Control Access:

There is a variety of methods to control access. In order to choose the appropriate method, the required level of protection, the associated costs and the level of inconvenience that each option provides, must be considered. The control of access should be as convenient to normal operations as possible. To grant access the person shall first be authenticated, i.e. securely identified. Authentication is based on the following authentication factors:

- What you know (PIN, password, etc.).
- What you possess (smart card, RFID, keys, etc.).
- What you are (biometrics, physical identification, etc.).

The authentication can be mechanical, electronic or performed by human. Common access control methods include:

- Mechanical access control ("*What you possess*"), i.e. locking devices operated by keys.
- Electronic access control ("*What you know"/ "What you possess"/ "What you are*").
- Personal recognition ("*What you are*"), by security staff physically located at entry and exit points or by security staff who monitor entry and exit points using closed circuit television cameras and similar devices.
- Access badges (*"What you possess"*) by security staff physically located at entry and exit points.

Depending on the desired level of security and the risk assessment, one or more of the above can be used.

Technical measures for access control:

Access control is based on the security that the physical barriers offer along with some additional

means that permit access (usually a key).

- Mechanical measures include doors, turnstiles and gates.
- The most common mechanical means is the keyed lock.
- If keys can be easily copied, control of access cannot be guaranteed.
- If a key is lost, lent or stolen, there is a risk of unauthorized access. If the lost key is a master key, then a greater number of access points will be affected.
- If proper key control is maintained, keyed mechanical locks may be an effective and inexpensive method to contribute to controlling access.
- There are turnstile designs that physically prevent unauthorized access. Usually they are expensive and not well accepted by users due to their inconvenience.
- User friendly turnstiles require additional monitoring of the access point.
- Access control turnstiles are designed to allow only one person to enter at a time.

Detailed technical specifications for doors, turnstiles and gates shall be provided by the Information Security Team

Cryptography:

- Sensitive data must be sufficiently protected, e.g., by means of strong cryptographic encryption. Public key infrastructure, certificates must be managed to ensure authenticity of key holders (smartcards, connectors, server, etc.)
- Communications paths between all involved parties must be encrypted

Protection of Software

Biometrics:

Biometric devises can provide some assurance that the person requesting entry is not using someone else's electronic access card or secret code, as they require that the person present a physical characteristic to a reader (iris, fingerprint, a hand, face etc.).

- Secure biometric systems are often expensive systems and they can have false rejections.
- Biometric systems are not appropriate for high-traffic areas.
- Biometric systems should be used only in high security zones and only as an extra security mechanism.
- Biometric systems shall be carefully implemented and comply with legislation.
- Detailed technical specifications for biometric systems shall be provided by the Information Security Team.

5.6. Case study of 2nd Threat - Proposed Security Policy Rules

In the following analysis of **Case Study - Example 2**, we select the **#threat2** "**Insufficient Knowledge**" which belongs to the **HR category**. The same in this part, in the analysis that follows we propose security measures that can be adopted in the Cloud Computing and confront this threat and then we propose a set of Security Policy Rules that will form our Security Policy of Cloud Computing. According to a research of Digital Agenda [100] the main factor preventing enterprises from using Cloud services is "insufficient knowledge" of Cloud Computing.

Table 16 Security Policy for Threat2 "Insufficient Knowledge"

Example 2
Threat: Insufficient Knowledge
Category: HR
Measures: 1. HR awareness 2. Personnel Security 3. Education Training 4. Education in Information System and alertness 5. Creation of technical Library of journals or publications and books 6. Segregation of duties 7. Confidentiality agreement prior to given information
Security Policy Rules for Requirements of Category C (HR): The security policy rules associated with the requirements of the Category C (HR) and belongs there the threat "Insufficient Knowledge". **Awareness , information and training of staff in security issues:** The security of information systems, in general, is an issue that requires the involvement of all users. For example, no authentication method, or using passwords or smart cards, or even biometric methods can be successfully applied if users do not follow safe practices, such as the non disclosure of the password to Third parties. Therefore, achieving a high level of awareness and awareness and

to educate users on security issues is a condition for the success of a security plan. It is important that employees become aware of the security policy, and the responsibilities that derive from it, as soon as they are hired. Security awareness training shall be included in introductory seminars, right after the job assignment. In order to develop a positive attitude towards security, Cloud Providers are to ensure that all staff members are kept informed throughout their career at that Organization, by attending to security awareness programs regularly. Hence, security culture and awareness should be constantly developed with the use of:

- security briefings or seminars held periodically,
- campaigns that inform on specific threats or security incidents,
- exercises that assess the Organisation's readiness, and

  Inclusion of security attitude in the employee's performance evaluation and incentive program.

Security Education and Alertness:

Socially engineered messages are one of the most common techniques used to spread malware. Once technical measures fail, users are the last line of defense in ensuring a socially engineered email does not lead to malware being installed on a workstation. Organizations need to ensure their users are aware of the threat and educated on how to detect and report suspicious emails.

Personnel security :

is essential for the protection of information assets, especially since information systems and services are operated by people. The main objective of Personnel Security is to ensure that people who access Health resources are qualified and properly trained, and to provide a level of assurance as to the trustworthiness, reliability and honesty of health's employees, contractors and casual staff Personnel Security Management .An effective Personnel Security Management, based on the existing health recruitment policies and related legal framework, will help minimize the risks associated with human errors, theft, fraud or misuse of assets.

Security Organizational Structure and Responsibilities:

Cloud Provider should adopt the appropriate security organizational structure with the appropriate roles and suitably trained staff in order to support the security policy. The involved people or committees should have clear lines of responsibility and accountability. The roles, together with the privileges / responsibilities of each role, that are necessary to support the Security Policy, shall be defined.

Security Culture and Awareness:

It is important to ensure that all members of staff are aware of their responsibilities, regarding the protection of the Cloud Provider's assets, as well as the consequences that they may have in case

they breach a security rule.

- Ensure that the security policy is kept in a centralised location.
- Ensure that the security policy is written in simple.
- Ensure that provisions of the security policy are clearly linked to specific roles
- Ensure that all staff members have been briefed on their responsibilities and that they have easy access to regular security briefings and security awareness programs sponsored by the Cloud Provider
- All users of ICT systems shall be familiar with the security operating procedures governing their use, they shall receive appropriate security training, and be aware of local processes for reporting issues of security concern.

There is a clearly stated and available policy and mechanisms in place, to allow for independent and anonymous reporting of security incidents.

Continuous Monitoring:

Ensure continuous monitoring of employee's status through the development and maintenance of employee records for all permanent and casual staff. Organization shall ensure that information contained in employee records is up-to-date by establishing the necessary procedures, in accordance to the Public Service Law and relative regulations.

In addition, Organizations who own an Information System and have applied incremental recruitment controls during the recruitment process shall establish procedures in order to ensure continuous monitoring of employees' status and that this information is always available and up-to-date. The context of employee records shall be coherent in the sense that it should provide a complete snapshot for each employee status at a given time. Employee records may include the following basic components:

- Personal information (Name, date of birth, identification numbers, previous employment etc.). This information can be obtained during the recruitment process.
- Qualifications (Education, certificates and working experience). This information can also be obtained during the recruitment process.
- Roles and responsibilities.

Continuous monitoring of employee status can be achieved by conducting regular reviews of employees' records, based on granted access rights, and by integrating all reported changes to the primary files. For example, during the employment life-cycle, these primary files may be enriched with additional components, like:

- Education and training during his current employment. This field will contain a list of any awareness, education and training programs he has attended within the Organisation. This information should be updated by the Responsible Officer, whenever employees attend seminars sponsored by the Organisation.

- Changes of personal circumstances.
- Changes of responsibilities.

Employee records and personal information should be processed and handled in accordance with applicable legislation for employment data protection and with the rules introduced by Cloud Provider's Information Security policy.

Confidentiality agreement prior to being given to information:

All the staff should agree with the terms and policy of organization, through a confidential agreement about the information that the use and share to others.

Creation of technical Library of journals or publications and books:

All the manuals, books, technical support, laws and recommendations should be kept for security of information in electronic libraries that could be easily accessed by personnel.

This Core Security Policy addresses the requirements that will enable the protection and preservation of information, physical assets and human assets against possible threats of Cloud Computing.

Chapter 6: Security in e-Health System

6.1.Introduction

Information and communication technology (ICT) has introduced the idea of central business model in e-health. The use of digital technologies in providing health care services is in general described under the term e-Health. Healthcare is increasingly being supported by IT applications, such as Cloud Computing. But sharing sensitive personal information in Cloud Computing can be risky, when an unauthorized user gets access to this information and uses it other than those intended by Providers. Many countries are keen to shift their traditional health care services to the new technology of Cloud Computing, in order to improve the quality of care and reduce the cost. However, these opportunities introduce new security risks which cannot be ignored. So**,** in this Chapter, our work focuses on examine which are the challenges when using Cloud Computing in e-health and how we could mitigate these risks.

In **this Chapter**, we present a traditional e-health system, as a **case study** we use the e-health system of Europe, and then we propose the same system based in Cloud Computing technology. Then we present a list of core security requirements that must be considered when migrating e-health systems to a SaaS Cloud environment by both health care Providers and Cloud Service Providers. These requirements are analyzed and categorized in four Categories-Gates, so the Providers or the organizations could use them in general Security Policy of Cloud Computing for e-health and then we propose the solution for these requirements. Finally, we describe the measures and Provisions of the Cloud Security Policy and give a trust establishment, using this Methodology in the e-health Cloud Computing landscape.

6.2. Information Privacy in Health Informatics

The healthcare environment is undergoing fundamental changes. The preview years, doctors and hospitals used to have many papers and envelopes to keep the health of their patients and every time that a patient used to change doctors, there were nothing about their history of their health. Nowadays, many countries in order to improve their services on e-health, change their traditional medicine care into new technologies.

Internet technologies protect patient privacy, confidentiality of sensitive medical data, while at the same time improve quality of care. The benefits provided by the Internet, however, come with a significantly greater element of risk to the integrity of information. Despite the myriad of studies, information security and privacy remain a high concern for citizens and patients regarding their health data [107][108].

Unfortunately, traditional security mechanisms are not appropriate to meet the requirements of the patients in new technological advances in e-Health services, so the creation of a general e-health Security Policy that it defines the security requirements for Cloud Computing e-heath system is needed. To better understand the developments in terms of e-Health it is necessary to understand what is e-Health and what is exactly e-Health Policy in new technologies? And why is needed in health industry?

When we mention the term E-Health, we mean the use of information technologies across health related functions and activities [109]. An electronic health service system, is a collection of components working together to implement the e-health services. As data is processed into practical information by the information system, authentication and authorization become one of the essential concerns of the e-health service systems [110]. Also, the European Commission defines e-Health very generally as “The use of modern information and communication technologies to meet needs of citizens, patients, healthcare professionals, healthcare providers, as well as policy makers” [111].

To use properly and effectively an e-health system we need an e-Health Policy. A Health Policy has been defined as “a set of statements, directives,

regulations, laws, and judicial interpretations that direct and manage the life cycle of e-health" [112].

In the area of health, the creation of n e-health policy that balances the need for access (authorization) with the needs and rights of the citizens is the biggest challenge. There are several examples of countries that have national e-health strategies Italy, France, UK, while others have introduced the electronic health card, like Germany [118][119].

New technologies, such as Cloud Computing, could improve services in e-health to their patients. Health data could share everywhere, easier and doctors could have better diagnosis for the health of their customers, without expenses and professional personnel. Cloud based e-health services could change the traditional e-health environment and could bring a lot of advantages [115][116][117]. The industry may considerably improve the access to information and patients will have improved diagnosis and treatment, faster care and faster decision making responses from assigned medical professionals. However, despite the potentially high value of the new technological development of cloud computing, in the area of e-health , the security of medical information, as well as data handling, is a serious issue [118][119][120][121]. In order to achieve the security levels in medical environment, need to be carefully addressed the security requirements. In our research we protect the confidentiality of patient information and facilitate the processes of the e-health system, with some suggestions for health care Providers. Security requirements of a Cloud Service provider are analyzed, using the case study e-health system of Europe.

6.3. Case Study of e-Health System in Europe and EEA Members States

In Europe, the European Union(EU) has endeavored to promote the implementation of e-Health within the 28 Member States by making e-Health a key part of EU health policy [122][123][124][125]. The big challenge and the vision of the EU is to achieve the wide spread adoption of e-Health systems across Europe as part of the EU's Flagship initiative 'Digital Agenda for Europe' [126][127][128]. Also a key

ambition of the EU policy is the provision of better care services at the same or lower cost [129]. The 2004 EU e-Health Action Plan was the first initiative that set in motion the EU's plans to encourage European co-operation on health care issues [130]. In our research we illustrate as an example application scenario the traditional European Union e-Health system and the implementation strategies that use across the European Union and EEA Member States. So, in this Chapter, we will present an existing Information System in e-health, the system in Europe that consists of national e-health programs of 27 European Countries and illustrates the overall framework. Then, we will present how this Information System would be with the use of Cloud Computing, what the New Security Requirements that have been created by the use of Cloud Computing on this e-health system are. Which the proposed solutions for these Cloud Computing Security Requirements on e-health system are and how these requirements could increase the reputation of this Cloud Computing e-Health system.

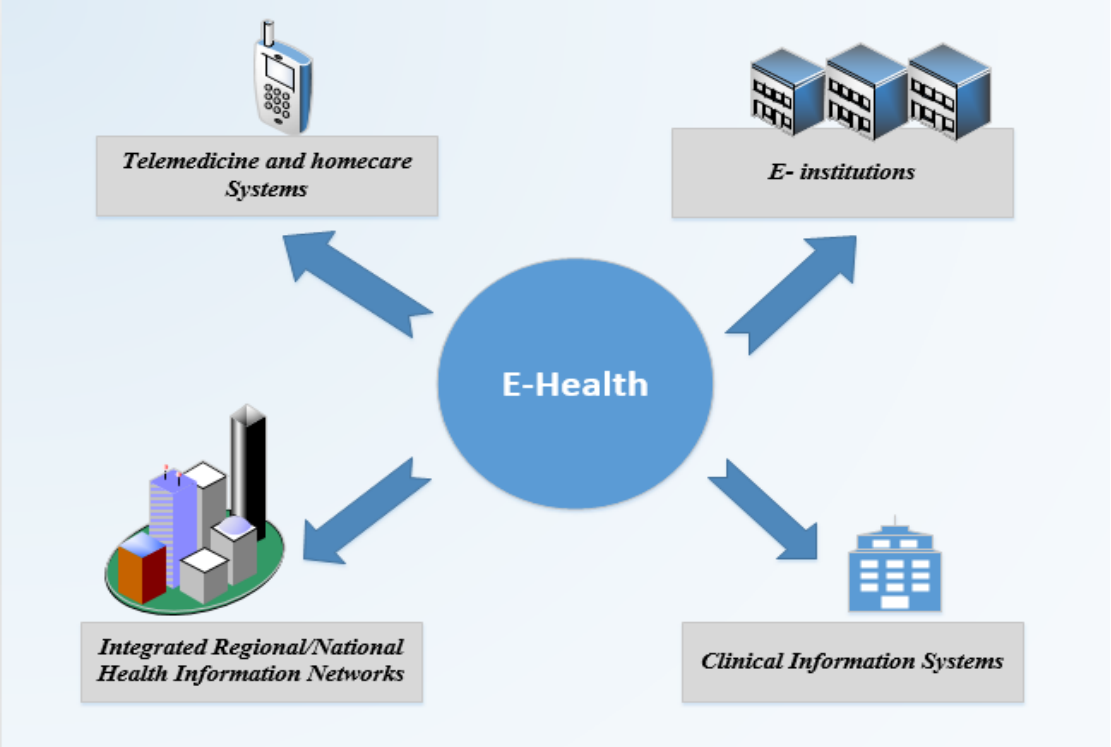
In this scenario - Case Study, the approach of European system conceptualizes the healthcare system as a value system of a variety of health Service Providers each of which has to manage its own health system. As depicted in this research, this health system which consists of individual health service providers, promote good health and long term care services, supports disease prevention and provides healthcare.

The European Commission’s e-Health Action Plan mentions the lack of awareness and confidence in new technologies among health professionals and citizens as a barrier to adopt them [131][25].

The previous years, the European Commission (EC) has established working parties and expressed its intention for information development in all public health programmes [132][133][134]. Examples of the term of e-health according to the European Commission’s e-Health Taskforce are: clinical information systems, e institutions, Telemedicine and homecare systems, Integrated regional/national health information networks, Secondary usage non-clinical systems [135] (**Figure 12)** other examples also include: electronic health records, portable communicable systems including those for medical implants, health portals, and many other ICT-based tools assisting disease prevention, diagnosis, treatment, health monitoring

and lifestyle management (this description is based on text at the Europe's Information Society e-Health portal) This system makes it difficult to share information beyond organizational boundaries.

Figure 12 E-health example Types



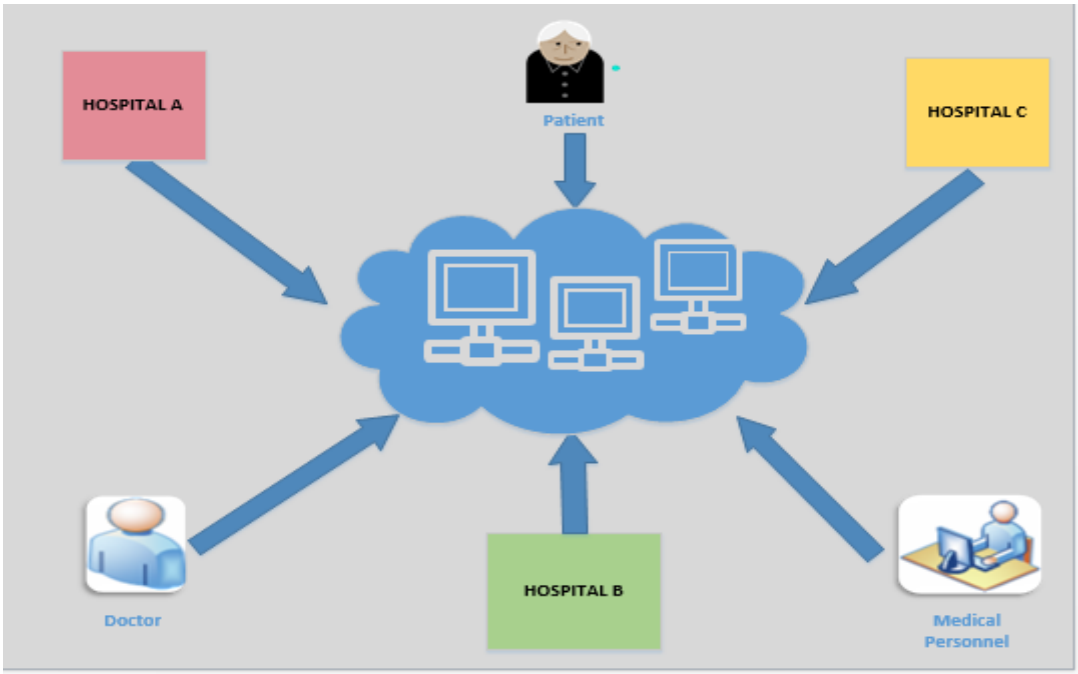
The increasing prevalence of ICTs can have transformative impacts on many industries, including healthcare where ICTs can deliver citizen centric healthcare and foster a dyadic information symmetric physician-patient relationship [136].

6.4. E-Health Cloud Computing Implementations Issues

Cloud Computing has been widely recognized as the next generation's technology and it offers several advantages to its users. Cloud Computing can also offer many opportunities to improve health care services. According to the official NIST definition, "Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources". These characteristics are particularly appealing to the needs of healthcare providers. On Cloud Computing for an e-health system, the consumer does not manage or control the Cloud infrastructure, but mainly the software services are provided by

the Provider to its members or end users, clinicians and patients [137] [138] [139] [140] [141] [142] [143] [144]. In addition, Cloud Computing is characterized by consumers who use Cloud services as needed, who consume shared resources as a service, which pay only for what is used and who access services over a networked infrastructure. Cloud adoption also provides the ability to exchange data between disparate and separate systems. In healthcare it can be implemented, as a way for maintaining or managing patient information, at different Locations. It is needed to be mentioned that also, Management is responsible for taking care of security risks to protect data of patients. Today, still, a lot of differences can be found between member states in both the quality and availability of health data. So, a Cloud Based Information System on e-health communicates with the following actors (doctors, patients, medical personnel) and hospitals via a lot of Clouds and via network connections (**Figure 13**). This part of the Cloud Provides a common Service for all the Information systems of the sharing hospitals/ countries. To provide consistent, coordinated care at a reasonable cost, Providers must be able to share patient's medical information freely while maintaining information security of their data.

Figure 13 A Cloud Based e-Health System



The proposed health Cloud system presents the end users (authorized doctors and patients) that could take part in SaaS health Cloud System. They are

been navigated through the sharing hospitals and the whole Information systems. As we can understand, the most important thing to this system is to ensure the security and guarantee the confidentiality of the data, because we have to deal with sensitive data and the protection of stored information comes as a top priority. And how can we succeed this? By defining, which the assets we want to protect are, what the possible security requirements are and which the solutions can be. The asset of such Information system, based on Cloud Computing is defined to ensure the availability, integrity, authentication and confidentiality of the service, e transformation of data. The **security requirements** and the **proposed solutions** we will be analyzed in the next chapter of the Thesis.

6.5. Requirements: Cloud-Specific Security Aspects for E-Health Systems

However, whatever the choices of the organization or hospital are, there are some security challenges that need to be addressed for those who decide to implement e-health on the cloud.

There are a number of steps for a successful transition from a traditional system to a Cloud System. This study aims to support the development of an EU Health Information System based on Cloud Computing by identifying the necessary key requirements relevant to build up a comprehensive system that supports health policy making. In the following **Table 17** we describe the security requirements involved in an e-health Cloud Computing system. In the **Table 18, Table 19, Table 20, Table 21** we provide the solutions-measures that must be done to the security challenges of an e-health Cloud Computing System. If Cloud Providers and Organizations follow this model, using the gates of the policy, they will succeed to have a secure Cloud Computing environment on e-health. It worthwhile to be mentioned that there are different security tasks for every Service Model of Cloud Computing (IaaS, PaaS, IaaS) but we focus only to the tasks of the Cloud Provider for a SaaS Service Model. In the diagram below **Figure 14** we illustrate only the certain security tasks for the **type of SaaS services.** It is not provide an exhaustive list of

security processes at the Providers side. In the case of e-health system, it is important to carefully be assessed which security tasks are outsourced to the Provider and which security tasks remain under the organization/ hospital. In this scenario, a trusted Third Party is needed to serve as the group manager, who is trusted by all group members and is responsible. In our policy, the Cloud Provider or Organization that uses this e-health Cloud System must follow the four general **Categories-Gates** to avoid threats. These four Categories-Gates that proposed in our General Security Policy on e-health System require that **the Third Party will mitigate these security requirements** by adopting the appropriate security measures in accordance to a well formed Cloud Security Policy:

Category 1 (A) – Processes/Functions Controls: are associated with execution of business services, operations, logs and industry security certifications.

Category 2 (B) – HR: Providers must aim to promote security, through education and sharing of good practices with the personnel.

Category 3 (C) – Legal Requirements & Compliances: the legal framework under which data are stored and/or transferred are satisfied. In which country the data are located and thus what the regulations / restrictions for storing / processing / transferring that data are. Regulatory requirements, such as Sarbanes Oxley Act (controls over initiation, authorization, processing and recording of transactions). Whatever is associated with noncompliance to various legal, government and regulatory requirements.

Category 4 (D) –Technology: is associated with constantly evolving technologies and lack of standardization in how they integrate or interoperate. What are the applications and the devices that users trust to store and possible share their data? Standardize on integration methods.

Understanding and documented the security requirements of an e-health Cloud System, gives a solution targeting to each threat and at the same time maps them with the provisions of the Cloud Security Policy. In each category it is necessary to ensure what security requirements are covered by the Cloud Provider according the following security measures. The proposed Cloud Security Model addresses the

relationships of security measures and places them in context with their relevant security solutions and concerns.

In the following analysis, we select as threats of E-health Cloud System

- The Abuse of Cloud Services,
- The Malicious Insider,
- Unintentional Disclosure
- Lack of user control

Those threats belong to the **Category A** of "**Process-Functions & Controls**", according to our Methodology. These specific threats are crucial for Cloud Computing. In the Analysis that follows we propose security measures-requirements that can be adopted in an e-health Cloud System and then we give a set of Solutions-Measures **(Table 17)(Table 18)(Table 19)(Table 20)(Table 21)** that will form our Security Policy.

Security Requirements: there are specific requirements for Cloud Computing environments of an e-health system, some of them are the following:

#A1. Data controls: when the health care data are stored on the Cloud may require appropriate controls to be in place. Data are at the core of a security concerns for any e-health system, whatever the form of infrastructure that is used. For SaaS, much more responsibility is likely to be placed into the provider. The distributed nature of the cloud computing and the shared responsibilities that it involves bring the Security considerations both to data at rest and also to data in motion, on the priority.

#A2. Disaster recovery procedures: Having Disaster recovery procedures in the cloud of an e-health system, reduces the need for data center space, IT infrastructure and IT resources, which leads to significant cost reductions, enabling smaller hospitals to deploy disaster recovery options. If the hospital will damage in a natural disaster, the provider should know how to get the e-health organization rebuilt and continue it from any remote location.

#A3. Unauthorized access by e-health professional: Cloud providers are responsible for separating their clients in multi-tenant situations. Some information such as health data are of a sensitive nature, so a cloud provider

may not allow direct access to the information to everyone, without appropriate authorization being required before any user is permitted to access sensitive data in any way.

#A4. Ubiquitous network connectivity to the hospital: consumers evaluate the external and internal network controls of a cloud provider. In the information system of an e-health , each user's requirements will be different, but it is recommended that users evaluate the internal network controls of a service provider such as : Protect clients from one another, protect provider's network, monitor for intrusion attempts and the external network requirements such as: traffic screening, intrusion detection, logging and notification.

#A5. QoS (Quality of service) and reliability: one of the challenges posed by an e-health cloud system is QoS, which is the problem of allocating resources to the application to guarantee a service level along dimensions such as performance, availability and reliability. QoS denotes the levels of performance, reliability, and availability offered by an application and by the platform or infrastructure that hosts it. In the system of e-health based on clod the problem is more difficult.

#A6. Data Centers - unauthorized entities: as in accessing patient data by unauthorized users. Data security and privacy protection issues are relevant to both hardware and software in the cloud architecture. According to The explanation of "cloud computing" from the National Institute of Standards and Technology (NIST) cloud computing provides a convenient on-demand network access to a shared pool of configurable computing resources. Resources refer to computing applications, network resources, platforms, software services, virtual servers, and computing infrastructure. The 'Cloud' itself is a virtualization of resources, which the end user has on-demand access to. These resources can require authorized access and management or service provider interaction. In the e-Health cloud, the unlawful entities may obtain access to the patients' health data by spoofing the identities of the authorized users, such as doctors and patients themselves.

#A7.Digital signatures/ certificates: A digital certificate is an electronic "passport" that allows a person, computer or organization to exchange information securely over the Internet using the public key infrastructure (PKI). A digital certificate may also be referred to as a public key certificate. Healthcare professionals can gain access to health data using a digital certificate.

#A8. Malicious insider (doctor, staff, and family member): A malicious insider is well-known to most organizations. A malicious insider, in an e-health system, could access the sensitive data, steal information, sell the data to other parties or perform any number of other malicious activities. User needs to make sure cloud providers are doing the best through their hiring practices and administrative controls. The insider may have access to servers and data, and could be a member of the staff, a doctor, another patient or a family person.

#A9. Abuse of Cloud Services: Cloud Computing providers are actively being targeted, partially because their relatively weak registration systems facilitate anonymity, and providers' fraud detection capabilities are limited. This huge flaw in the registration system coupled with weak fraud detection capabilities lends cloud computing models to malicious attacks by criminals who can leverage those technologies and target cloud providers.

#A10. Unintentiona Disclosure: An event when health professionals unintentionally or by mistake reveal confidential information.

#A11. Lack of user control: Ownership and accountability, however, are often not well defined or applied even in traditional IT Providers should examine what they are trying to control in the system of e-health.: Control over data, Control over functionality, Control over assets. These highlight some of the areas that IT providers need to consider for an e-health system.

Then, In **Table 18, Table 19, Table 20, Table 21**, we present the solutions targeting to the requirements that we have mentioned for every Category of the four and then we depict them in **Figure 14.** As described in studying numerous relevant publications, a common practice to minimize the risk, is understanding the internal

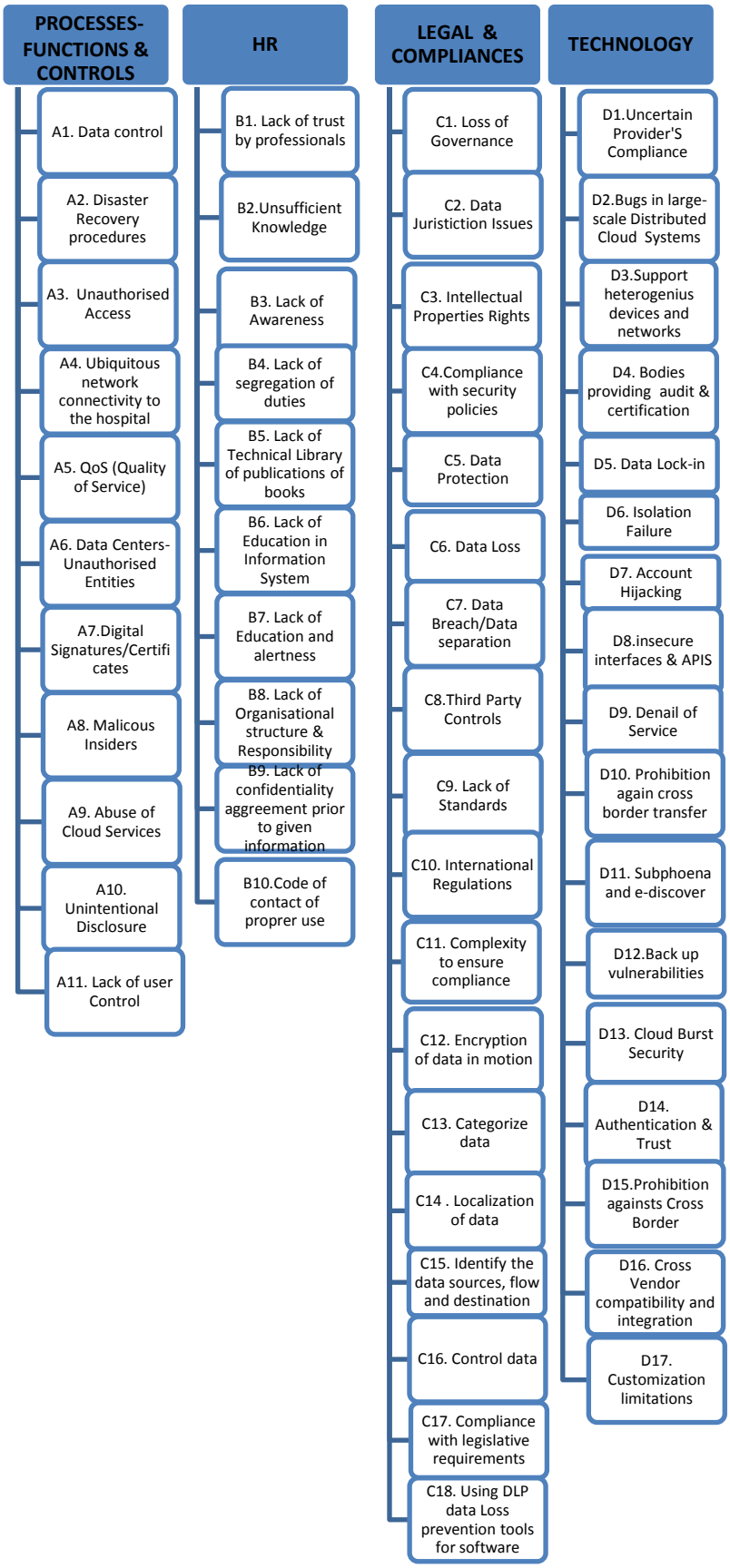
control environment of a Cloud Provider and examining, analyzing all the aspects, so to identify possible contributing factors risks, and other governance issues, including and begin to define mitigation strategies. This is exactly what we present in our study.

Table 17 Cloud Computing Requirements of e-health system

Sr. No	CATEGORY	REQUIREMENTS
A.	**Processes-functions &controls**	A1. Data control A2. Disaster recovery procedures A3. Unauthorized access by e-health professional A4. Ubiquitous network connectivity to the hospital A5. QoS (Quality of service) and reliability A6. Data Centers - unauthorized entities A7. Digital signatures/ certificates A8.Malicious insider(doctor, staff, family member) A9. Abuse of Cloud Services A10.Unintentional Disclosure A11. Lack of user control
B.	**HR**	B1. Lack of trust by health care professionals B2.Insufficient Knowledge by health care professionals B3. Lack of awareness B4. Lack of Segregation of duties B5. Lack of technical Library of publications and books B6. Lack of Education in Information System B7. Lack of education and alertness B8. Lack of Organizational Structure & Responsibilities B9. Lack of Confidentiality agreement prior to being given information B10. Code of contact of proper use
C.	**Legal & Compliances**	C1. Loss of governance C2.Data jurisdiction issues C3. Intellectual property rights

		C4. Compliance with security policies C5. Data protection C6. Data loss C7. Data Breach/ data separation C8.Third party controls C9. Lack of industry standards and certifications C10. International Regulations C11. Complexity to ensure compliance C12. Encryption of data in motion C13. Categorize data C14. Localization of data C15. Identify the data sources, flow and destination C16. Control data C17. Compliance with legislative requirements. C18. Using DLP Data Loss Prevention Tools-software
D.	**Technology**	D1.Uncertain provider's compliance D2.Bugs in large-scale distributed cloud systems D3. Support heterogeneous devices and networks (hospitals, tablets, different mobile and stationary devices) D4. Bodies providing audit & certification of management systems D5. Data lock-in D6. Isolation failure D7.Account Hijacking D8. Insecure interfaces & APIS D9. Denial of Service D10. Prohibition against cross border transfer D11. Subpoena and e-discovery D12. Back up vulnerabilities D13. Cloud Burst Security D14. Authentication and Trust D15. Prohibition against cross border transfer D16. Cross-vendor compatibility and integration D17. Customization limitations

Figure 14 Cloud Computing Requirements of E-health system



The proposed methodology can fulfill the entire list of security requirements of every Category that are covered by the following Metrics and Provisions of the Cloud Security Policy. More analytically:

Table 18 Security Policy Rules of E-Health Cloud System (for Category A)

Requirements (A1-A11) of Category A (Processes - Function & Controls) are covered by the following Policy Rules:
Security management: *Security management should be based on risk assessment and should be dynamic, encompassing all levels of participants' activities and all aspects of their operations. The requirements of security management depend upon the level of involvement, the role of the participant, the risk involved and system requirements.* ***Continual Reassessment:*** of information security and making of appropriate modifications to security policies, practices, measures and procedures. ***Risk assessment***: Risk assessment will help to identify threats and vulnerabilities and to determine appropriate controls to reach to acceptable levels of risks. Risk assessment should be sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications. ***Threat:*** is defined as any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. ***Vulnerability***: is a weakness of an asset or group of assets that can be exploited by one or more threat. ***Risk***: Is defined as the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation. ***Security Incidents Handling:*** It is necessary to have the appropriate policies and procedures in order to effectively handle a range of security incidents and thus avoid, as much as possible, the disruption of critical activities. Define the specific reporting and response procedures, according to the type of the security incident. Security incidents shall be properly recognized, reported, assessed, handled and debriefed, in order to prevent any damage caused to the Organization. First of all, employees and external service providers shall recognize the most common types of security incidents, which are the following: • unauthorized use of Cloud resources, • leakage of passwords or other types of identification mechanisms, • criminal actions, such as fraud, phishing, electronic attacks, theft, etc., • sharing of sensitive information to unauthorized persons, and • natural phenomena that could affect cloud security. The Organization shall take all necessary measures in order to raise the awareness of the personnel regarding recognizing security incidents. To that end, appropriate seminars or other types of training, as well as campaigns, informative sessions etc., shall be performed. Organization security policy should include that employees and external service providers recognize and report security

incidents. To that end, a simple and easy to use mechanism should be in place for reporting security incidents that will include at least the following:

- description of the incident,
- date/time of the incident, and the location where it took place,
- assets or resources involved,
- nature and circumstances of the incident, and
- the degree of the potential harm to the Organisation.
- Other fields for recording possible corrective actions that were taken should also be in place, but those shall be filled at a later stage, during the mitigation of the security incidents.
- Recognition and reporting of an incident shall be followed by its assessment, in order to calculate the degree of the potential damage caused to the GO, and to determine the appropriate actions that should be taken. In terms of assessing security incidents, a first estimation is performed by the employee or the external service provider during its reporting. However, this assessment shall be validated by the GO's security officers, as they have a better understanding of the threat landscape, and better information on same or similar incidents that may have been also reported.

According to the effect that an incident might have on the Organization, it can be further divided in three categories: Normal, Escalated and Emergency.

- **Normal**: those are not events that don't affect critical systems nor do they cause serious damage to the organisation. Those incidents don't need immediate reporting or escalation to higher level personnel, and can be handled with minor modifications to the ICT infrastructure or procedures.
- **Escalated**: those are more serious incidents that affect critical systems and shall be immediately reported to higher management as well as to the relevant CERTs.
- **Emergency**: those are events that may have a major impact on the employees' health and safety may cause a great damage to ICT infrastructure which could critically affect the performance of the Cloud, or may cause significant problems in the Cloud's compliance in laws and regulations. Emergency incidents shall be immediately reported to higher management, CERTs, law enforcement authorities etc. Moreover, appropriate procedures shall be in place for the personnel to follow in case of an emergency incident

Apart from the differentiation in handling and response, the categorization of incidents should also be utilized in forcing different disciplinary procedures, as post-incident actions, against the employee who is responsible for the incident. Thus, according to the incident's severity, the employee's manager should or shouldn't be notified for further disciplinary procedures.

Assurance and Reporting:

Policy requirements, as well as regulatory or other obligations, shall be integrated in the Organization's everyday operations, as well as to those of delivery partners and third party suppliers. In order to accommodate this need, the Organization shall have installed a system that will:

- inform all parts on their compliance responsibilities,
- ensure that requirements have been integrated into business processes,
- include procedures for reporting non-conformities, and
- Provide mechanisms for reporting to upper management.

The aforementioned system will correlate information from lots of different sources, such as systems and networks (log files, uptime reports), ERP systems (HR, maintenance planning), scheduled human input and post mortem reports.

Recruitment Controls:

- Identity Verification: Confirmation of name, date of birth, address, national insurance number or other unique personal identifying number
- Confirmation of permission to work in system: Nationality, Citizenship, immigration status
- Qualification checks: Education, References, additional qualifications/licenses
- Employment history: Details of previous employers, references

- Additional checks required by the Government Organization

Identification of Positions requiring a Security Clearance:

The identification of positions that require a Security Clearance should be based on Organization's risk assessment results and the Cloud Information Security Policy, as well as on the regulation of Security of classified information, documentation and hardware and related matters. Cloud Provider Organizations should keep a record of all identified Security Positions and should follow appropriate screening procedures for granting a Security Clearance according to the instructions/recommendations of the National Security Authority (NSA). As per the Minimum Requirement Controls, Cloud Provider, will make all necessary amendments at the Schemes of Service and follow the Public Service Law and Regulations.

Recruitment controls for casual staff:

Casual staff shall undergo appropriate recruitment controls, in accordance to the Law

Handling exceptions from a Security Clearance:

- **Temporary access** arrangements may be considered in cases where there is a need for an employee or casual staff or contractor's staff to have access to only a part of classified information or assets (in a higher level than his/her clearance authorizes him/her), and for a small period of time. Cloud Provider should consult the National Security Authority (NSA) for decisions upon handling temporary access. They should also review the possibility of escalating this position to a Security Position and applying for a permanent Security Clearance.
- **Emergency access** can be considered in cases where there is a need for an employee or casual staff or contractor' staff to have access to classified information or assets (in a higher level than his clearance authorizes him), to meet a critical requirement. Again, Cloud Provider should consult the National Security Authority (NSA) for decisions upon handling emergency access and under what circumstances this type of access can be granted.

Security Incidents Handling

Assurance and Reporting:

Policy requirements, as well as regulatory or other obligations, shall be integrated in the Organization's everyday operations, as well as to those of delivery partners and third party suppliers. In order to accommodate this need, the Organization shall have installed a system that will:

- inform all parts on their compliance responsibilities,
- ensure that requirements have been integrated into business processes,
- include procedures for reporting non-conformities, and
- provide mechanisms for reporting to upper management.

The aforementioned system will correlate information from lots of different sources, such as systems and networks (log files, uptime reports), ERP systems (HR, maintenance planning), scheduled human input and post mortem reports.

Recruitment Controls:

Casual staff shall undergo appropriate recruitment controls, in accordance to the Law. Organizations who own an Information System may request a higher level of assurance of a person's suitability to perform a particular role, based on their risk assessment policy, through appropriate recommendations to the InfoSec Team. Organizations should always ensure the proportionality between the extra recruitment controls the associated risks. All extra recruitment controls, if additional to the existing will be included to the Scheme of Service and will be published by the Cloud Provider.

Recruitment controls for Corporate Contractors and Third Parties

Organizations usually assign the implementation of very large projects or new services to corporate contractors or joint ventures. These contractors may need to recruit new contracted staff or reassign smaller parts of the project to other sub-contractors. This hierarchical scheme of contractors and subcontractors will make the recruitment control of outsourced staff even more complicated.

In order to ensure the universal application of recruitment controls, Organizations should incorporate all these aspects in the tendering process for the procurement of outsourced ICT services as well as in their contracts with the leader company. An indicative list of issues addressed by the contract includes:

Recruitment controls for employees and sub-contractors that will participate in the specific project.

- The right of the organization to approve any subsequent choice of subcontractor.
- The right of the organization to audit the implementation of the security controls at any point in the contracting chain.
- Responsibilities for the security controls including the obligation of contractors to participate in security awareness, training and education programs in order to be informed about their responsibilities and the Organization's formal procedures and policies.

Identification of Positions requiring a Security Clearance:

The identification of positions should be based on Government Organisation's risk assessment results and the Cloud Provider's Security Policy. Cloud Provider should keep a record of all identified Security Positions and should follow appropriate screening procedures for granting a Security Clearance according to the instructions/recommendations of the National Security Authority (NSA)

Post-Verification:

Upon the completion of the baseline and any incremental recruitment controls imposed by the Organization, Cloud Provider shall ensure the employee's recruitment record is created. This record contains all the checks that have been applied during the recruitment process and accompanies the employee throughout his/her employment life-cycle.

Reporting changes of personal circumstances:

Employees who have access to Cloud Provider's resources should be obliged to promptly report any changes in their personal circumstances that might imply unreliability or a conflict of interest. This obligation should be depicted in a corresponding document that will be signed during the employment agreement phase.

In order to support this obligation and effectively manage the reporting capabilities, Cloud Provider shall ensure that all the necessary arrangements have been established and communicated to all employees. These may at least include the specification of:

- the formal procedures that all staff should follow for reporting personal changes,
- the contact point for the reports, and
- in which cases an employee is required to inform the relevant appropriate authority.

Cloud Provider shall support on-going personnel security management by staying in line with any obligations they have to the Public Service Commission and ensuring that the formal reporting procedure is communicated to all Cloud Provider's employees. To this end, the Cloud Provider should be responsible to remind this obligation to all employees at regular intervals, through relevant updates. Upon designing the reporting procedure, Cloud Provider should take into consideration that access to personal information should also be restricted based on the "need to know" principle. In regards to those employees that hold a Security Clearance, the Cloud Provider is responsible to inform the National Security Authority (NSA) for any changes they are aware of or any concerns they might have about the continued suitability of their employees.

Incident Reporting:

Cloud Provider shall establish a well-defined policy for Incident Handling and should communicate the formal procedures for incident reporting to all staff. In addition employees should also be strongly encouraged to report any changes in personal circumstances of other employees, colleagues or contractors, they might be aware of, that could potentially introduce a conflict of interest and harm the Organization. This obligation is essentially critical when violations or changes of personal circumstances concern employees who hold a Security Clearance.

Termination of employment controls:

There are many cases where an employee might leave from a specific post. The most common ones

are: retirement, resignation, end of contract, transfer to another Organization within the public service or division, leave long duration (e.g. for health/personal reasons) etc. Organization shall ensure that:

- Employees who are about to leave Organisation are subject to a number of termination of employment controls, and be obliged to return all Organisation 's resources and access media,
- Employees who are about to undertake a different position or to be transferred to another division within the Organisation are also subject to controls that are similar to the termination of employment controls in terms of access rights to organisation's Information resources and organization equipment management,

Through the establishment of formal procedures that GOs should follow when an employee is about to leave his current post. Organizations shall stay in line with the procedures defined by the Public Service Commission and their obligations as defined by the Public Service Law and relevant regulations. To this end, organization must:

- submit a proposal to the PSC through formal procedures.
- make sure that the officer who is about to leave has no financial obligations towards the state of if he has such obligations he shall settle them and no disciplinary or criminal case is pending against him.

In addition, when an employee leaves the Organisation and also a minimum set of controls that should be applied in order to ensure protection from possible access violations. An indicative list of checks includes:

- Returning all assigned equipment, hardware and software, including mobile and portable devices, as well as any manuals, documents and information stored on electronic media.
- Returning all kinds of access media, cards, keys or tokens etc. that grant physical access to the Organisations' buildings, offices, rooms and logical access to Information Systems.
- Disabling all employees' user accounts.
- Removing employee from all mailing lists and groups.
- Renewing any common passwords that were given to the user, for accessing ICT resources.
- Notifying division managers and co-workers that the employee or contractor has terminated his employment/collaboration with the Organisation.
- Signing an agreement similar to the recruitment agreement, about employee's obligations to the Organisation.

Application of Access Control

Methods to Control Access:

There is a variety of methods to control access. In order to choose the appropriate method, the required level of protection, the associated costs and the level of inconvenience that each option provides, must be considered. The control of access should be as convenient to normal operations as possible. To grant access the person shall first be authenticated, i.e. securely identified. Authentication is based on the following authentication factors:

- What you know (PIN, password, etc.).
- What you possess (smart card, RFID, keys, etc.).
- What you are (biometrics, physical identification, etc.).

The authentication can be mechanical, electronic or performed by human. Common access control methods include:

- Mechanical access control ("*What you possess*"), i.e. locking devices operated by keys.
- Electronic access control ("*What you know"/ "What you possess"/ "What you are*").
- Personal recognition ("*What you are*"), by security staff physically located at entry and exit points or by security staff who monitor entry and exit points using closed circuit television cameras and similar devices.
- Access badges (*"What you possess"*) by security staff physically located at entry and exit points.

Depending on the desired level of security and the risk assessment, one or more of the above can be used.

Technical measures for access control:

Access control is based on the security that **the physical barriers offer** along with some additional means that permit access (usually a key).

- Mechanical measures include doors, turnstiles and gates.
- The most common mechanical means is the keyed lock.
- If keys can be easily copied, control of access cannot be guaranteed.
- If a key is lost, lent or stolen, there is a risk of unauthorized access. If the lost key is a master key, then a greater number of access points will be affected.
- If proper key control is maintained, keyed mechanical locks may be an effective and inexpensive method to contribute to controlling access.
- There are turnstile designs that physically prevent unauthorized access. Usually they are expensive and not well accepted by users due to their inconvenience.
- User friendly turnstiles require additional monitoring of the access point.
- Access control turnstiles are designed to allow only one person to enter at a time.

Detailed technical specifications for doors, turnstiles and gates shall be provided by the Information Security Team

Guidelines for Applying Physical Security Rules

Identifying Physical Assets:

The term physical asset includes the buildings, rooms, equipment a Cloud Provider is using. The assets may be at the Cloud Provider's possession or they may be at its plans to obtain.

In defining physical assets, the following guidelines should be considered:

- Only assets that are used by the Cloud Provider's need to be defined.
- If multiple assets of the same type are used, and are likely to be subject to similar risks, these may be grouped together and only defined once.
- Assets that carry out multiple functions can be classified as multifunction assets.

Develop and Implement Cloud Provider Physical Security Policy

Threat and vulnerability assessment:

Risk analysis method will reveal the potential threats against facilities, employees and clients. Depending on the identified value of assets, both physical and electronic, the need for the implementation of countermeasures will be revealed.

Countermeasure selection and recommendation:

Cloud Providers shall put in place physical security protection measures that match the evaluated security risk. They shall put in place the necessary building and entry control measures for areas that have been characterized as "restricted". Any attempt for an unauthorized access shall be detected and an effective response be activated.

Biometrics:

Biometric devises can provide some assurance that the person requesting entry is not using someone else's electronic access card or secret code, as they require that the person present a physical characteristic to a reader (iris, fingerprint, a hand, face etc.).

- Secure biometric systems are often expensive systems and they can have false rejections.
- Biometric systems are not appropriate for high-traffic areas.
- Biometric systems should be used only in high security zones and only as an extra security mechanism.
- Biometric systems shall be carefully implemented and comply with legislation.

Detailed technical specifications for biometric systems shall be provided by the Information Security Team.

Third Party:

- Third party audits should be performed to monitor the secure the cloud service provider's compliance to agreed terms and the effective implementation of and adherence to security

policies, procedures and standards.

- The cloud service provider should provide customer transparency around controls, security and operations
- use of electronic signatures by each of the parties
- Protocols used to communicate between all involved parties should be secure

Protection of Software:

- Maintain a version control for all software updates
- Ensuring changes are submitted by authorized users
- Ensure that software are changed as necessary to remain appropriate
- Identify all software, database entities and hardware that require amendment

Cryptography:

- Sensitive data must be sufficiently protected, e.g., by means of strong cryptographic encryption.
- public key infrastructure, certificates must be managed to ensure authenticity of key holders (smartcards, connectors, server, etc.)
- communications paths between all involved parties must be encrypted

Network Security:

Information Systems connected to a network have greater security needs as they are exposed to more dangers, for this reason added security countermeasures need to be established.

- All devices belonging to the internal network shall by authenticated using a suitable authentication mechanism.
- By default Internal networks shall not be directly connected to external networks unless necessitated by business needs. If and when a connection is required, then the connection:
  - shall have the authorization of the Application / Infrastructure Heads.
  - shall use suitable mechanisms to ensure the confidentiality, integrity and availability of the internal network's information assets and systems.
- Proper security mechanisms (e.g. encryption) shall be employed to ensure the confidentiality and integrity of important information exchanged between the Cloud Provider and another Cloud Provider or third party.
- The employed security mechanisms shall themselves be protected.
- Communication shall be protected using anti-malware/anti-virus solutions.
- Interconnected systems have greater security needs from isolated ones.
  - All non-essential services and ports shall be permanently disabled.
  - Continuous monitoring of the network is required.

Telecommunication Services Security:

All network services acquired by external Telecommunication Providers shall have a Service Level Agreement (SLA) that takes into account security issues.

- Telecommunication services shall be constantly monitored.
- The binding agreement of the Telecommunication Provider shall include terms pertaining to the security of the provided services.
  In case of a security incident, it shall be clear which party and to which extend is responsible to handle it.

Business continuing:

A business continuity plan should be in place in order to ensure the availability of all critical services and assets have critical functions, the absence of which could lead to many unwanted situations, even to threat of human life. Some of these functions include health and safety systems, large scale financial transactions etc. To identify and mitigate those risks, thus providing uninterrupted services for critical governmental functions, Cloud Provider shall follow a series of steps that are called Business Continuity planning (BCP). The whole procedure needs the employment of many other security policy elements, such as asset evaluation, risk management, incident response, reporting etc. The first step of adequate Business Continuity planning is identification. Cloud Provider shall

evaluate assets
and business functions, and differentiate critical from non-critical ones. This impact assessment has to be done according to:

- functions/services whose disruption is unacceptable (e.g. health systems),
- critical governmental infrastructure (e.g. power plants),
- environmental and other factors (e.g. areas with earthquake history),
- critical assets/functions that will result from risk management processes.,

After asset identification and impact assessment, it is important that Cloud Provider identify the best and most cost-effective solutions for recovering from disaster scenarios. Thus, solution for Business Continuity might include, but not limit to:

- Disaster Recovery (DR) Sites,
- Spare software/equipment,
- Data replication methodologies,
- Hard copies of critical data,
- Offices for staff to work in case of emergency,
- Methodologies for working without IT infrastructure.

Baseline Security Procedures and Measures:

Implement and enforce fundamental security procedures and measures to achieve a baseline integrity and availability level for the Services provided

- All procedures pertaining to the daily use of the ICS shall be documented.
- A well-defined procedure for data back-up shall be in place
  - Proper data back-up shall take place regularly
  - Back-up media management and storage is of great importance
- A well-defined procedure for detecting, preventing and removing malware and virus software shall be in place
  - A legally-acquired and up-to-date anti-malware/anti-virus solution shall be chosen as the Organization's default
  - Every new or alien removable media and/or executable program shall be scanned before gaining access to the Cloud Provider ICT infrastructure
  - The anti-malware/anti-virus solutions in use shall themselves be protected
- All software or hardware changes, removals, alterations, upgrades and updates shall have the permission of the Application / Infrastructure Heads and the Asset Owner and shall be logged in a suitably protected storage (e.g. a data storage device protected by encryption or an external data storage device kept in a secure office furniture).
- All critical or important administrative actions shall be logged in a suitably protected storage.
- All important software and hardware malfunctions shall be logged in a suitably protected storage and their impact on the Cloud Provider security shall be assessed.

Developing and implementing a Cloud Provider Security Policy:

All to the Cloud Providers shall develop and implement an Information Security Policy adapted to the Organization's and user's information security requirements:

- The security policy ensures that:
  - Information will be protected against any unauthorized access
  - Confidentiality of information will be assured
  - Integrity of information will be maintained
  - Availability of information for business processes will be maintained
  - Legislative and regulatory requirements will be met
  - Business continuity plans will be developed, maintained and tested
  - Information security training will be available for all employees
  - All actual or suspected information security breaches will be reported to the CISO and will be thoroughly investigated
- Procedures exist to support the policy, including malware/virus control measures, passwords and continuity plans.

- Business requirements for availability of information and systems will be met.
- The InfoSec team is responsible for maintaining the policy and providing support and advice during its implementation.
- All managers are directly responsible for implementing the policy and ensuring staff compliance in their respective departments.
- Compliance with the Information Security Policy is mandatory.

Identifications and authentications*:*

- Determinants of authentication and user accounts.
- Specifies identity of users to ensure that any action can be attributed to a specific user. This rule applies to the operating system level and at the level of applications.
- Each user has identifier ID (user ID).
- Be a list of users and their respective determinants identity.
- Each identifier ID assigned to a user and used by a single user.
- The system operators must have individual identifiers and every identity will correspond to accounts with elevated privileges and do not use the system administrator account .The rule applies for all systems including database management systems.

Categorized of Data:

Data should be categorized in accordance with the protection they need, as this identified through the risk assessment or the assessment of the SP controller.

- Top Secret: information and vital data for the CP which any disclosure or unauthorized alteration will cause a direct impact on business operations.
- Confidential: information and data important to the operation of CP which must be subject to strict controls and protected.
- Sensitive: Information and data that are subject to legislation on protection of personal data, the disclosure of which need specific permission / authorization
- Reportable: information and data may be disclosed.

The security requirements of information and data, differentiated according to the category information belonging and how to use them. Authorized data recipients should be identified, according to the above classification. Any processing of data must be ensured by procedural and technical means that can be attributed to a specific person .In conclusion, all critical operations will be strictly made with personalized access.

ICT Outsourcing

Providers shall ensure that all security issues associated with the procurement of outsourced ICT services are assessed, and the appropriate measures are taken. To that end, the information that is passed to the external providers that are involved in the procurement phase shall be regulated, and they should sign a Non-Disclosure Agreement regarding this information. Every contract with an external provider for outsourced ICT services shall have a contract manager within the Provider. This person is responsible for the technical details of the contract, which include the enforcement of security controls and conditions to the provider.

The security controls that are to be included in the contract shall be determined by every Organization, under the supervision and approval of the contract manager, taking into account:

- national, international or other types (e.g. sectorial) of regulations,
- the outcome of a risk management procedure regarding the provided service by the external party, and
- the highest level of (classified) information that the provider will access during the course of the contract.

Those security controls, and thus the contract with the provider, should be updated when changes in the cooperation with the Provider, the regulations, or the general threat environment occur. Depending on the time of occurrence, those contract updates can be further divided to ad hoc and periodic.

Ad hoc updates will occur in the following circumstances:

- changes in national or international regulations,

- security incidents within the Organization that directly or indirectly affect the external provider,
- security incidents within the external provider,
- changes in the overall threat landscape, and
- changes in the contract's details.

On the other hand, periodic updates will occur in the following occasions:

- completion of internal or external audits, and
- Contractual dates for updating the terms of contract.

Contracts should also include controls that will restrict the providers by using information that was provided by the Organization, or was produced as a result of the contract, to purposes other than the ones stated in the contract. Moreover, Organizations are to include in the contract controls that will allow them to monitor the compliance of the service providers to the security controls as well as their response to security incidents. Special terms and conditions should be in place that will allow the Organizations to terminate the contract in case the provider fails to comply with the security controls stated in it. Organizations are to ensure that contracts will include the provider's agreement to regular visits of the Organization's representatives to the provider's premises in order to assess the aforementioned compliance to the imposed security controls.

Security Controls according to ISO 27002

The customer must get assurance from the provider that appropriate security controls are in place. Assurance may be provided by means of audit and assessment reports, demonstrating compliance to such security standards as ISO 27002. The security controls include:

- Physical Infrastructure and facilities should be held in secure areas. A physical security perimeter should be in place to prevent unauthorized access, allied to physical entry controls to ensure that only authorized personnel have access to areas containing sensitive infrastructure. Appropriate physical security should be in place for all offices, rooms and facilities that contain physical infrastructure relevant to the provision of cloud services.
- Protection against external and environmental threats. Protection should be provided against fire, floods, earthquakes, civil unrest or other potential threats that could disrupt cloud services.
- Control of personnel working in secure areas. Controls should be applied to prevent malicious actions by any personnel who have access to secure areas.
- Equipment security controls. Controls should be in place to prevent loss, theft, damage or compromise of assets.
- Supporting utilities such as electricity supply, gas supply, telecommunications, and water supply should have controls in place. Controls are required to prevent disruption to cloud services either by failure of a utility supply or by malfunction (e.g. water leakage). This may require the use of multiple routes and multiple utility suppliers.
- Control security of cabling. In particular, controls are needed to protect power cabling and telecommunications cabling, to prevent accidental or malicious damage.
- Proper equipment maintenance. Controls should be in place to perform necessary preventive maintenance of all equipment to ensure that services are not disrupted through foreseeable equipment failures.
- Control of removal of assets. Controls are required on the removal of assets to avoid theft of valuable and sensitive assets.
- Secure disposal or re-use of equipment. Controls are required for the disposal of any equipment and particularly any devices which might contain data such as storage media.
- Human resources security. Appropriate controls need to be in place for the staff working at the facilities of a cloud provider, including any temporary or contract staff.
- Backup, Redundancy and Continuity Plans. The provider should have appropriate backup of data, redundancy of equipment and continuity plans for handling equipment failure situations

Table 19 Security Policy Rules of E-Health Cloud System (for Category B)

Requirements (B1-B4) of Category B (HR) are covered by the following Security Policy Rules:
Personnel security: It is essential for the protection of information assets, especially since information systems and services are operated by people. The main objective of Personnel Security is to ensure that people who access Health resources are qualified and properly trained as well as to provide a level of assurance as to the trustworthiness, reliability and honesty of health's employees, contractors and casual staff Personnel Security Management .An effective Personnel Security Management based on the existing health recruitment policies and related legal framework, will help minimize the risks associated with human errors, theft, fraud or misuse of assets.   ***Awareness of the need of security in Information Systems***:   Awareness of the risks and available safeguards is the first line of Defense for the security of Information Systems; including their information assets, computing and communication systems. Information systems can be affected by both internal and external risks. IS owners should understand that security failures may significantly harm systems and networks under their control.   • **Confidentiality**: The protection of communications or stored data against interception and reading by unauthorized persons .The property that information is not made available or disclosed to unauthorized, individuals, entities or processes.   • **Integrity:** The confirmation that data which has been sent, received, or stored is complete and unchanged. The property that data has not been altered or destroyed in an unauthorized manner   • **Availability:** The fact that data is accessible and services are operational.   The security of information systems in general, is an issue that requires the involvement of all users. Therefore, achieving a high level of awareness and awareness and education of users on security issues is a condition for the success of a security plan. It is important that employees become aware of the Security Policy and the responsibilities that derive from it, as soon as they are hired. Security awareness training shall be included in introductory seminars, right after the job assignment. In order to develop a positive attitude towards security, Cloud Providers are to ensure that all staff members are kept informed throughout their career at that Organization, by attending to security awareness programs regularly. Hence, security culture and awareness should be constantly developed with the use of: • security briefings or seminars held periodically,   • campaigns that inform on specific threats or security incidents,   • exercises that assess the Organisation's readiness, and   • Inclusion of security attitude in the employee's performance evaluation and incentive program.   ***Responsibility:***   All participants are responsible for the security of information systems and networks. Participants depend upon interconnected local and global information systems and networks should understand their responsibility for the security of those information systems and networks. They should be accountable in a manner appropriate to their individual roles.   ***Response:***   Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents, recognizing the interconnectivity of information systems and networks and the potential for rapid and widespread damage. They should share information about threats and vulnerabilities, as appropriate and implement procedures for rapid and effective co-operation to prevent, detect and respond to security incidents. Where permissible, this may involve cross-border information sharing and co-operation.

Security Organizational Structure and Responsibilities:

The roles together with the privileges / responsibilities of each role, that are necessary to support the Security Policy, shall be defined. Organization should adopt the appropriate security organizational structure with the appropriate roles and suitably trained staff in order to support the security policy. The involved people or committees should have clear lines of responsibility and accountability. It is important to ensure that all members of staff are aware of their responsibilities, regarding the protection of the assets, as well as the consequences that they may have in case they breach a security rule.

- Ensure that all staff members have been briefed on their responsibilities and that they have easy access to regular security briefings and security awareness programs sponsored by the Government.
- All users of ICT systems shall be familiar with the security operating procedures governing their use, receive appropriate security training and be aware of local processes for reporting issues of security concern.
- There is a clearly stated and available policy, and mechanisms in place, to allow for independent and anonymous reporting of security incidents.
- Ensure that the security policy is kept in a centralised location.
- Ensure that the security policy is written in simple, plain language.

Ensure that provisions of the security policy are clearly linked to specific roles

On-going staff education, Security Culture, awareness and Education

Organizations shall ensure that all employees are properly informed about their rights and obligations and that they understand and accept their security responsibilities, in accordance to the Public Service Law and to any additional restrictions imposed by the Organization. Employees should also be aware of the formal procedures that they should follow in order to report to the Organization and to the Public Service Commission any changes in their personal circumstances or any possible violations of other employees and should be strongly encouraged to do so. In order to fulfill this obligation, Cloud Providers should encompass the above requirements to their Education and Awareness.

It is important that employees become aware of the Cloud Provider's security policy and the responsibilities that derive from it, as soon as they are hired. Thus, in order to ensure the Security awareness training is included in introductory seminars, after starting with the Cloud Provider.

In order to develop a positive attitude towards security, Cloud Providers are to ensure that all staff members are kept informed throughout their career at that Organization. Hence, security culture and awareness should be constantly developed with the use of:

- security briefings or seminars held periodically,
- campaigns that inform on specific threats or security incidents,
- exercises that assess the Organisation's readiness and
- Inclusion of security attitude in the employee's performance evaluation and incentive program.
- Human factor is of great importance for building and operating secure information systems. Thus, Cloud Providers are to ensure that they have security operating procedures in place for every ICT system. Moreover, those procedures should become known to the employees as soon as they gain access to each individual ICT system.
- For certain ICT systems that are subject to many security incidents, e.g. laptops/tablets/smartphones, a separate informative session or seminar regarding their safe use, apart from the ones that were mentioned above, should take place. ICT users should also receive training on recognizing and reporting security incidents, or possible improvements to the systems' security.
- In order for those incidents to be appropriately reported and further handled by the technical staff, a clearly defined procedure should be in place that ICT users could follow to record their security observations. This procedure, together with instructions on how to use each Cloud Provider's security incident mechanisms, should be made known to the ICT users through informative sessions.
- Cloud Provider's can benefit from the employees' observations and reporting of security incidents, by investing in policies, procedures and mechanisms for incident reporting,

handling and mitigation.

- First of all, a clearly stated and available policy regarding security incident reporting should be in place, as part of the overall security policy. This policy is to ensure that all staff members are encouraged to anonymously report information security incidents, as well as vulnerabilities that could lead to security incidents.
- Cloud Provider's are also to ensure that independent mechanisms are in place for reporting security incidents. These mechanisms might differ from system to system; in some systems, reporting might be performed with the press of a button, or by filling a web form. Some others, such as violation of physical security, might just be reported by phone. In any case, a clear procedure describing the mechanism(s) used each time should be described and become known to all staff members.

It is important to ensure that all members of staff are aware of their responsibilities, regarding the protection of the Cloud Provider's assets, as well as the consequences that they may have in case they breach a security rule.

- Ensure that the Security Policy is kept in a centralised location.
- Ensure that the Security Policy is written in simple.
- Ensure that provisions of the security policy are clearly linked to specific roles
- Ensure that all staff members have been briefed on their responsibilities and that they have easy access to regular security briefings and security awareness programs sponsored by the Cloud Provider
- All users of ICT systems shall be familiar with the security operating procedures governing their use, receive appropriate security training, and be aware of local processes for reporting issues of security concern.
- There is a clearly stated and available policy, and mechanisms in place, to allow for independent and anonymous reporting of security incidents.

Security Education and Alertness:

Socially engineered messages are one of the most common techniques used to spread malware. Once technical measures fail, users are the last line of defense in ensuring a socially engineered email however this does not lead to malware being installed on a workstation. Organizations need to ensure their users are aware of the threat and educated on how to detect and report suspicious emails.

Continuous Monitoring:

Ensure continuous monitoring of employee's status through the development and maintenance of employee records for all permanent and casual staff. Organization shall ensure that information contained in employee records is up-to-date by establishing the necessary procedures, in accordance to the Public Service Law and relative regulations.

In addition, Organizations who own an Information System and have applied incremental recruitment controls during the recruitment process shall establish procedures in order to ensure continuous monitoring of employees' status and that this information is always available and up-to-date.

The context of employee records shall be coherent in the sense that it should provide a complete snapshot for each employee status at a given time. Employee records may include the following basic components:

- Personal information (Name, date of birth, identification numbers, previous employment etc.). This information can be obtained during the recruitment process.
- Qualifications (Education, certificates and working experience). This information can also be obtained during the recruitment process.
- Roles and responsibilities.

Continuous monitoring of employee status can be achieved by conducting regular reviews of employees' records, based on granted access rights and by integrating all reported changes to the primary files. For example, during the employment life-cycle, these primary files may be enriched with additional components, like:

- Education and training during his current employment. This field will contain a list of any

awareness, education and training programs employee has attended within the Organisation. This information should be updated by the Responsible Officer, whenever employees attend seminars sponsored by the Organisation.

- Changes of personal circumstances.
- Changes of responsibilities.

Employee records and personal information should be processed and handled in accordance with applicable legislation for employment and data protection and with the rules introduced by Cloud Provider's Information Security policy.

Creation of technical Library of journals or publications and books:

All the manuals, books, **technical** support, laws and recommendations should be kept for **security** of information in electronic libraries, that could be easily be accessed by personnel.

Confidentiality agreement prior to being given to information:

All the staff should agree with the terms and policy of organization, through a confidential agreement about the information that the use and share to others.

Code of contact of proper use

Users should understand their roles and their responsibilities with respect to information security and infrastructure.

- To secrecy on matters designated as confidential.
- To use legitimate software, to protect copyrights and intellectual property.
- To keep secret personal accounts and passwords to alert for leaks.
- Do not make the misuse of funds for personal use.

Table 20 Security Policy Rules of E-Health Cloud System (for Category C)

Requirements (C1-C10) of Category C (LEGAL & COMPLIANCES) are covered by the following Security Policy Rules:
Ethics*:** Participants should respect the legitimate interests of others. Given the pervasiveness of information systems and networks in our societies, participants need to recognize that their action or inaction may harm others. Ethical conduct is therefore crucial and participants should strive to develop and adopt best practices and promote conduct that recognizes security needs and respects the legitimate interests of others. ***Categorized of Data Data should be categorized in accordance with the protection they need, as this identified through the risk assessment or the assessment of the SP controller. ▪ Top Secret: information and vital data for the CP which any disclosure or unauthorized alteration will cause a direct impact on business operations. ▪ Confidential: information and data important to the operation of CP which must be subject to strict controls and protected. ▪ Sensitive: Information and data that are subject to legislation on protection of personal data, the disclosure of which need specific permission / authorization ▪ Reportable: information and data may be disclosed.. The security requirements of information and data, differentiated according to the category information belonging and the use them. Authorized data recipients should be identified, according to the above classification. Any processing of data must be ensured by procedural and technical means that can be attributed to a specific person .In conclusion, all critical operations will be strictly made with personalized access. ***Localization of data*** In Cloud Computing data travels over the Internet to and from one or more regions where the data centers are. The user of a cloud must know in which country the servers are located, how the data are processed and under which legislation. So, at any moment the provider should be able to inform its users about these issues. Data locat-ed in different countries, provinces or municipalities are subject to different legal frameworks. For this reason it is essential for the contract between the provider and the user to clearly state the geographic region of the servers . ***Identify the data sources, flow and destination*** Data should be accomplished. This process must include data discovery and data fingerprinting that provides a better understanding, who, where, when and in what for-mat the information is being generated and in what devices it is being stored. In addi-tion, identifying the cloud services being used and the type of data that is being trans-ferred to the cloud is an important step during this process. ***Control Data*** In the absence of control data in a cloud environment, no activity is recorded which modify or delete users data. User should know how these data is handled. No information is stored like which nodes have joined, which programs have run, what changes are made. In addition, users want to know who the providers have the data from, where and in what way they are being processed. ***Compliance with legislative requirements*** ○ Recording and documentation of all legislative and regulatory obligations of the service and how all these obligations are addressed. ○ The privacy of the users should be ensured. ○ If sensitive personal data are collected, permission from the Data Protection Authority should be acquired. ○ Description of the procedures adopted for ensuring compliance with the legal requirements and regulations.

- Notification to the European Data Protection Supervisor (or current, depending on the continent where we are) for keeping personal data.
- If a record is kept of sensitive personal data, should be asked permission from the Data Protection Authority
- Description of procedures to ensure the fulfillment of the laws for hardware / software requirements,(ie the necessary licenses)
- Notification to the European Data Protection Supervisor (or current, depending on the continent where we are) for keeping personal data.
- Measures to protect critical data from loss, destruction and unauthorized modification, in accordance with legislative requirements.
- Documentation where the use of encryption mechanisms (if any) is consistent with the legal requirements and regulations.

Using DLP data loss prevention tools-software

Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network and prevent them by monitoring, detecting and blocking sensitive data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage). Users also want DLPs to be used for describing software products that help a provider to control what data end users can transfer.

Security Data Management

When an outside party owns, controls, and manages resources, users should be assured that data remains private and secure, and that their organization is protected from damaging data breaches. Users want to be sure that data is not readable and that the provider offers strong key management. Cloud Providers should implement access policies which ensure that only authorized users can gain access to sensitive information.

- Back up mechanisms the Cloud provider implements to separate the data of all the companies that are sharing the same servers.
- Maintain proof and evidence of ownership of licenses, disks, etc.
- Labeling of information
- Carrying out reviews that only authorized software and licensed products are installed
- Complying with terms and conditions for software and information obtained from public networks
- Guidelines should be issued on the retention , storage, and disposal of records and information
- A retention schedule should be drawn up identifying records and the period of time which they should be retained.
- Restrictions on import or export of computer hardware and software for performing cryptographic functions
- Mandatory or discretionary methods of access by the countries authorities to information encrypted by hardware or software to provide confidentiality of content

Conformance to Technical Standards:

Provide specialized expertise on relevant National and International technical standards. Apposite International technical standards include:

- ISO/IEC 27000 Series of standards
- NIST SP 800 standards
- Request for Comments (RFC 1281 Guidelines for the Secure Operation of the Internet)
- The Information Security Forum (ISF) Standard of Good Practice for Information Security
- Control Objectives in IT (COBIT) from ISACA
- ITIL
- Good Practices from recognized bodies such as ENISA, CERTS, NATO, the German BIS, SANS or EU NSAs

Data Ownership

The Organizations and the users shall ensure that it retains the “Exclusive” right to data ownership

throughout the duration of the agreement. The ownership includes all copies of data available with the Cloud Service Provider including backup media copies if any. Organizations and user should require that Cloud Service Providers are not permitted to use data for advertising or any other non-authorized secondary purpose.

Legal Prevalence

The Organizations and the users shall ensure that the Cloud Service Provider's own data privacy policy complies with the applicable laws in their country

Data Breach Notification

- The Organization and the users Agency shall contractually ensure that they are "immediately" notified of any confirmed breach without any undue delay.
- The Organization and the users contractually ensure that they are notified within 4 hours of any "Suspected" breach. From the time of breach discovery.

Table 21 Security Policy Rules of E-Health Cloud System (for Category D)

Requirements (D1-A15) of Category D (Technology) are covered by the following Security Policy Rules:
Security design and implementation: Security shall be a fundamental element of all products, services, systems and networks and shall be incorporated in the system design and architecture phase. A major, but not exclusive, focus of this effort is the design and adoption of appropriate safeguards and solutions proportionate to the value of the information on the organization's systems and networks. To this end, all new and future ICT systems shall conform to the Organization's Common Criteria and to relevant the Organization's Standards. **Servers Security** ***General Configuration Guidelines:*** Operating System configuration should be in accordance with approved InfoSec guidelines. • Services and applications that will not be used shall be disabled wherever this is feasible. • Access to services shall be logged and/or protected through access-control methods • The most recent security patches shall be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements. • Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do. • Always enforce the standard security principle of Least Privilege to restrict access rights required to perform a function. • Do not use root/admin when a non-privileged account will do. • If a methodology for secure channel connection is available (i.e., technically feasible), privileged access shall be performed over secure channels (e.g., encrypted network connections using SSH or IPSec). • Servers shall be physically located in an access-controlled environment. • Servers are specifically prohibited from operating uncontrolled cubicle areas. ***Monitoring:*** All security-related events on critical or on sensitive systems shall be logged and audit trails saved as follows: ○ All security related logs will be kept online for a minimum of 1 week. ○ Daily incremental tape backups will be retained for at least 1 month. ○ Weekly full tape backups of logs will be retained for at least 1 month. ○ Monthly full backups will be retained for a minimum of 2 years. • Depending on the criticality of the processed data, security-related logs and audit trails shall be stored in WORM (Write Once Read Many) data storage devices or a system offering similar protection, to assure that the logged data cannot be tampered with once it is written. • Security-related events will be reported to the Security Team, who will review logs and report incidents to the Organization's IT management and Corrective measures will be prescribed as needed. Security-related events include, but are not limited to: ○ Port-scan attacks ○ Evidence of unauthorized access to privileged accounts ○ Anomalous occurrences that are not related to specific applications on the host. ***Compliance:*** • Audits will be performed on a regular basis by authorized Organisations within the Cloud Provider. • Audits will be managed by the internal audit teams.

- Every effort will be made to prevent audits from causing operational failures or disruptions.

Workstation Security:

At a minimum, the following information is required to positively identify the point of contact Workstation user(s) and location

  - Hardware and Operating System and Version
  - Main functions and applications, if applicable
  - Workstation group membership
  - Image file version containing current configuration

Information in the government enterprise management system / systems inventory shall be kept up-to-date.

- Suitable security software, such as malware protection software and firewall, shall be installed, properly configured and maintained up to date.
- Always enforce the standard security principle of Least Privilege to restrict access rights required to perform a function.
- Access should be logged and/or protected through access-control methods; such as passwords and passphrases.
- Access should be logged and/or protected through access-control methods; such as passwords and passphrases

  Physical access to workstation shall be restricted

Malware Protection:

- Never download files from unknown or suspicious sources.
- Never install unauthorized programs or applications
- The Information Security team shall choose and issue default anti-malware/anti-virus software that is to be used on the Organizations systems
- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
- Always scan removable media (e.g. USB flash disks, CDs etc.) for viruses before using it.
- The Information Security team of Cloud Provider shall maintain an up-to-date read-only repository containing the default anti-malware/anti-virus software, its updates definitions. This repository will be the official source of the software and its updates/definitions for all systems.

Back-up critical data and system configurations on a regular basis and store the data in a safe place

Password Security:

All system-level passwords shall be changed on at least a quarterly basis.

- All production system-level passwords should be part of the InfoSecurity administered global password management database (e.g. Active Directory).
  - All legacy systems that cannot be integrated to a global password management database shall be identified and recorded in an up-to-date list.
  - All new and future systems shall be able to integrate with the global password management database in use.
- All user-level passwords (e.g., email, web, desktop computer, etc.) shall be changed at least every six months.
- User accounts that have system-level privileges granted through group memberships or programs shall have a unique password from all other accounts held by that user.
- All users at the Organization should be aware of how to select strong passwords
- Always use different passwords for Organization accounts from other not related to the Organization access (e.g., personal email account).
- Always use different passwords for various Organisation access needs whenever possible. For example, users could select one password for systems that use directory services (i.e. LDAP, Active Directory, etc.) for authentication and another one for locally authenticated access.
- Always decline the use of the "Remember Password" feature of applications (e.g., browsers,

email applications).

In addition, users should not:

- Share Organisation passwords with anyone, including administrative assistants, secretaries or IT support staff. All passwords are to be treated as sensitive, confidential Organisation information.
- Write down or store passwords on-line without encryption.
- Reveal a password in email, chat, or other electronic communication.
- Speak about a password in front of others.
- Hint at the format of a password (e.g., "my family name followed by my birthday")
- Reveal a password on questionnaires or security forms

Security of Software

Security in the development and maintenance of application software.

To take special care to control the development and maintenance of application software

- The development of applications to follow specific, scientifically acceptable, information systems development methodologies.
- Every new application to be accompanied by appropriate documentation in accordance with international standards.
- In every new application developed to place risk analysis.
- The risk analysis be included in the requirements analysis.
- The systems that are subject to development and software testing be separated from systems where the software will be operational software modification Authorization

Changes to the software are approved prior to their implementation.

- Applications software changes require approval by their respective makers.
- Any proposed change to consider whether affecting the safety of Information System

Changes that affect - directly or indirectly - Safety requirements must be approved by the Safety Officer of Information System

- The amendments to be made to copies of the software and tested before being put into productive operation.
- Comply registry software changes.
- Any changes must be characterized by a unique serial number.
- Each application software change should be recorded due date.
- In every software change request submitted must record the name of the applicant.
- Any changes to the software be accompanied by updating of documentation.

Urgent changes to software

- To be controlled and kept to a minimum software changes pre-must be undertaken urgently before given authorization.
- The urgent corrections are recorded in the file changes.
- To inform the Security Officer PS where changes may affect the safety of Information System
- The urgent corrections as urgent if considered, tested before being integrated in the operating system.

Technical review of operating system changes

- When changing the operating system to recheck the system security.
- Change Operational System is preceded update by Security Officer
- The Safety Officer monitors the effectiveness of safety devices after changing the Operational System

Malware Protection:

Attacks against vulnerabilities in web-based and other application software.

- The Information Security team shall choose and issue default anti-malware/anti-virus software that is to be used on the Information system. Different default anti-malware/anti-virus software might be issued for different sub-systems.
- The Information Security team shall maintain an up-to-date read-only repository containing the default anti-malware/anti-virus software, its updates and malware/virus definitions. This

repository will be the official source of the software and its updates/definitions for all Information systems.

- When an Information System is compartmentalized in separate and isolated sub-networks, each sub-network will maintain its own copy of the repository.

Always run the Information System's standard, supported anti-malware and anti-virus software which is available from the repository. Download and run the current version; download and install anti-malware/anti-virus software updates and definitions as they become available.

Portable Computing

Protection:

Portable information assets shall be adequately protected wherever they are used, whilst being transported or stored and when being disposed of.

- Portable information assets shall be:
    - Physically protected against loss, theft, damage and unauthorized access - they shall not be left unattended in public areas, unlocked offices, vehicles, hotel rooms, homes etc. without being physically secured e.g. using an approved security cable lock, safe or at the very least tucked away out of sight.
    - Logically protected against malware, unauthorized access and unauthorized configuration changes etc. using security products approved for this purpose by CISO.
- Sensitive personal or proprietary data stored on portable information devices and media shall be encrypted using suitable products and procedures approved by Information Security Team.

Management & Usage:

- Provider's IT equipment, including portable devices and media, shall only be used by authorized users for legitimate business purposes.
- Unauthorized software shall not be loaded onto Provider's IT equipment, including portable devices and media.
- Employees shall not interfere with or disable security controls on Provider's IT devices, including portable devices and media.

End of life:

- Before Provider's information assets, including portable devices and media, are disposed of or allocated to other users, residual information shall be physically destroyed or securely erased using procedures approved for this purpose by Information Security Team.

Backup & Recovery

- Provider's data shall be protected by regular backups.
- The Provider shall develop independent procedures for Daily, Weekly and Monthly backup
    - The Monthly backup should be a Full System Backup; which includes both data and important application software.
    - Any exceptions to the standard process shall be approved by the CISO.
- Backup copies shall enjoy the same or equivalent protection level as their original data
    - Backup copies shall be stored in an environmentally protected and access controlled secure offsite location.
    - Provider's data that are created or stored in isolated Information Computer System for security reasons shall be backed up using suitable encryption.
- Stored copies shall be made available upon authorized request.
- A record of the physical movements of all backup copies shall be maintained.
- Detailed procedures for the handling and storage of information shall be developed by the Organization, in order to prevent unauthorized disclosure, misuse or loss.
- Backup copies are to be maintained in accordance with the Organization's Retention and Disposal Schedule for backup copies.
    - At least three generations of backup should be retained; one of which shall be a full

system backup

- All backup media shall be appropriately disposed.
- A regular report on the Provider ability to recover data shall be submitted to the Security team periodically.
- Business Continuity Plans and Disaster Recovery Plans shall be tested to verify correct operation of processes and adequate restoration of services.

Facilities: Selection and Design

A Security Equipment Catalogue shall be maintained by the Information Security Team including technical specifications for:

- Building protection
- Doors and frames
- Locks and keys
- Keying systems
- Alarm systems
- Key cabinets
- Closed Circuit Television systems
- Fences and wall

Building construction:

- Cloud Providers shall assess the suitability of construction methods and materials to give the protection needed before leasing or constructing premises.
- Cloud Providers shall include special building elements to address security risks identified in their risk assessment (blast mitigation measures, ballistic resistance, etc.).
- Increasing the level of building security afterwards may be expensive or impossible.
- Cloud Providers shall always seek professional engineering advice before making structural changes.

Alarm systems:

- Alarm systems are used for early warning of unauthorised access.
- Alarm systems complement other access control mechanisms.
- Alarm systems are divided into two types:
    - perimeter security alarm systems,
    - internal security alarm systems.
- Cloud Providers shall have direct control, administration and management of the alarm systems in the Personnel, Security and High Security zones.
- Alarm systems can be sectionalised alarm systems allowing fine grained surveillance.
- Cloud Providers shall develop appropriate testing and maintenance procedures to ensure the alarm system is continually operational.
- Cloud Providers shall use appropriately cleared and trained personnel as alarm system operators

Locks and door hardware

Locks and Keying:

- Locks can prohibit unauthorized access to information and physical assets.
- Locks shall be chosen according to the required level of security
- Cloud Providers shall place keys cabinets within a facility's secure perimeter and where possible within the perimeter of the Zone where the locks are located.
- Key cabinets may be manual or electronic.
- Cloud Providers should maintain a register of all keys held and issued. Registers should include:
    - key number
    - details of person holding the key

    - History of the key (date and time issued, date/ time returned or reported lost).
- Cloud Providers shall limit to the minimum possible the number of master keys.
- Master keys shall be strictly controlled.
- Cloud Providers shall periodically confirm the location of all keys.
- Depending on the required level of security, the keying system shall offer:
    - High level of protection against compromise techniques
    - High level of difficulty in obtaining or manufacturing valid key blanks
    - High level of difficulty in obtaining or manufacturing the machinery and equipment used to create duplicate keys
    - High legal protection offered by the manufacturer

Doors:

Cloud Providers should select doors that provide a similar level of protection to the locks and security level of the zone they protect.

- There is a plethora of door types with a variety of security levels offered: solid core timber, metal framed insert panel, metal clad solid core, glass swing opening, rotating glass, glass sliding, single and double.
- Technical specifications for secure doors shall be provided by the Information Security Team.

Closed Circuit Television (CCTV)

- Applicable at least to facilities with Security and High security zones.
- Closed Circuit Television management systems shall be carefully designed and implemented to comply with relevant legislation. Specialist advice is required.
- Closed circuit television (CCTV) systems offer visual deterrent to unauthorised access, theft or violence and as an auditable access record.
- Cloud Providers can use CCTV to cover and give a visual record of:
    - zones access points
    - full site perimeter coverage, or
    - access to specific physical assets or work areas.
- A high cost solution. The initial installation and the on-going monitoring, maintenance and support costs may be high.
- Data retention shall comply with relevant legislation.
- The CCTV
    - shall fit into the context of the overall security plan of the site
    - shall (depending on the facility) be adequate for presentation in a court room. Excessive compression must be avoided.
    - can be event-activated, i.e. not recording all the time. It is triggered by another security mechanism/alarm.

Security lighting

If possible lighting, both internal and external, should be considered at the design stage.
Lighting includes also motion detection devices.
Security lighting aims:

- to assist patrols,
- illuminate areas with CCTV coverage
- safety lighting for employees.

Perimeter access control

- Applicable at least to facilities with Security and High security zones.
- The need for perimeter is shown during the initial security risk assessment.
- Types of perimeter control include but are not limited to:
    - fences and walls
    - pedestrian barriers, and
    - vehicular barriers.
- The level of protection a fence or wall offers is defined by its
    - height,

- construction,
- material used,
- access control mechanism,
- monitoring,
- alarms.

- Cloud Providers shall ensure that access points are at least as strong as any fence or wall used.
- Pedestrian and vehicular barriers shall be installed at controlled entry or exit points and shall be secured with mechanical or electronic access control systems.

E-Discovery SLAs

The users and the Organizations shall ensure that e-discovery costs and forensics requirements including cost and response times are detailed in the contract.

Security in the development and maintenance of Application Software

To take special care to control the development and maintenance of application software

The development of applications must follow specific, scientifically acceptable, information systems development methodologies.

- Every new application to be accompanied by appropriate documentation in accordance with international standards.
- In every new application developed to place risk analysis.
- The risk analysis be included in the requirements analysis.
- The systems that are subject to development and software testing be separated from systems where the software will be operational.

Software modification Authorization

Changes to the software are approved prior to their implementation.

- Applications software changes require approval by their respective makers.
- Any proposed change to consider whether affecting the safety of Cloud Provider's Changes that affect directly or indirectly - Safety requirements must be approved by the Safety Officer of Information System.
- The amendments to be made to copies of the software and tested before being put into productive operation.
- Comply with registry software changes.
- Any changes must be characterized by a unique serial number.
- Each application software change should be recorded due date.
- In every software change request submitted must record the name of the applicant.
- Any changes to the software be accompanied by updating of documentation.

Urgent changes to software

- To be controlled and kept to minimum software changes pre-must be undertaken urgently before given authorization.
- The urgent corrections are recorded in the file changes.
- To inform the Security Officer of Information System where changes may affect the safety of this.
- The urgent corrections as urgent if considered, tested before being integrated in the operating system.

Technical review of operating system changes

When changing the operating system must be rechecked the system security.

- Change to operational System is preceded update by the Security Officer of Information System.
- The Safety Officer monitors the effectiveness of safety devices after changing the Operational System.

Security Testing of Network

- The network devices must be checked for weaknesses or vulnerabilities.

- Networks and equipment be checked to ensure that all known vulnerabilities have been addressed.
- The configuration of network devices must be checked to identify vulnerabilities.
- The type of control network devices must be specified.
- The control must be performed using suitable analysis software that is for vulnerabilities.
- The software must be updated frequently.
- The information cannot be fully automated via the Internet, but always under the supervision of manager

Network management

The Network management Remote connection of external entities:

- should be carried out via a secure network using cryptographic methods
- should be used in cases of repetition of data transmission Protection Agency (replay attack).
- The central servers (Database, Application, Web, LDAP, Mail and VPN) to be protected from security dyke

Protection of Supervision and Monitoring tools

It must be controlled access to the surveillance tools

- The access to the surveillance tools It must be restricted to authorized persons.
- To prohibit the access of users to the surveillance tools.
- To ensure that maintenance contractors will not have access to surveillance tools. If they need some of these data should be given to them from system administrators, having checked and removed from them any unnecessary data on the basis of knowledge need (need-to-know).
- To limit the access rights of managers in system monitoring tools and related records to ensure that managers will not be able to remove or to change log information of their own actions
- It must be synchronized the system clocks of different systems that record actions and events.

Chapter 7: Conclusions and Future Work

7.1. Conclusions

Cloud Computing is a very promising technology that helps companies reduce operating costs while increasing efficiency. Even though Cloud Computing has been deployed and used in production environments, security in Cloud Computing is still in its infancy and needs more research attention.

Researchers have identified a lot of critical issues for trusted Cloud Computing Systems, and several recent works discuss general issues on Cloud Security and privacy. To preserve business continuity, the SaaS Provider must have a portfolio of security measures.

In this thesis, we have proposed a Security Model that gives a solution to the security challenges of a Cloud Provider in a SaaS Cloud Computing Environment. If the Cloud Providers follow the proposed Model, using the gates-categories of our Security Policy, they will succeed to have a professional Security Audit Model of Cloud Computing and thus a high level of security in their Cloud Computing environment.

So, the most important insight from this study is, the creation of a Trusted Cloud Service Provider that achieves the required assurance level and minimizes the risk of the user's data.

Based on the information presented in this study, through the analysis of case studies and the given status of e-Health security in the Europe, as is a priority for the European Commission (EC), we defined the minimum requirements for the protection of e-Health infrastructures, classified the policy rules and include them in clear cyber security guidelines. Combined with the general recommendations that are presented in this thesis, these guidelines could form the basis for the development of a standard protection level for the critical Infrastructures and could identify relevant assets, in Cloud Computing Systems.

Furthermore, our guidelines that refer to specific use cases and technical infrastructures and assets commonly deployed, in terms of their protection measures, could use as a practical guide for Organizations and Cloud Providers,

providing them a solution for their threats by linking them with the appropriate measures and rules of our Methodology of the Security Policy. With the use of this standardized way, this thesis can help some of the enterprises to look forward in using the Cloud Computing services.

7.2. Future Work

Data security has consistently been a major issue in information technology. In the cloud computing environment, it becomes particularly serious because the data is located in different places even in all the globe. Though many techniques on the topics of cloud computing have been investigated data security and privacy protection are becoming more important for the future development of cloud computing technology in government, business and especially in health environment. Data security and privacy protection issues are relevant to both hardware and software in the Cloud architecture and is the next step in our work. After evaluation of our Cloud Security Policy in e-health system, we thought that our next research will be to secure this part, because data security in e-health systems is foundational to health care reform, so it should be on first priority to us and other researchers. So, as a future work we will present a brief guide that gives an intro to the new regulation GDPR and key challenges for Cloud Providers according to this change. We will undertake a study to present how our Cloud Security Methodology that was developed in this Thesis is applicable to the GDPR and how Cloud Computing could help Developers and Providers to build secure and compliant health Systems.

References

[1] National Institute of Standards and Technology, systems, “Guide for developing security plans for federal information systems”, vol. 800-18, February 2006, [Online]. Available from: http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf/, [accessed December 2013].

[2] Divers S. - SANS Institute, "Information Security Policy A development Guide for large and small companies", November 2007, pp. 43-44.

[3] Svantesson D. and Clarke R., “Privacy and consumer risks in Cloud Computing", Computer Law and Security Review, vol. 26, 2010, pp. 391-397

[4] Kshetri, N., “Privacy and security issues in Cloud Computing: The role of institutions and institutional evolution”. 2012, Bryan School of Business and Economics, The Univ. of North Carolina at Greensboro, NC27402-6165,USA

[5] National Institute of Standards and Technology."The NIST Definition of Cloud Computing" (PDF), September 2011. [Online]. Available from: https://csrc.nist.gov/publications/detail/sp/800-145/final, [accessed November 2013].

[6] European Network and Information Security Agency (Enisa), “Cloud Computing Benefits, risks and recommendations for information security”, November 2009, [accessed June 2012].

[7] Arnold S., “Cloud Computing and the issues of privacy”, July 2009, KM World, pp.14-22

[8] Whitepaper, A, “Enterprise Cloud Computing: Transforming IT”, Platform Computing, viewed 13 March 2010, pp.6.

[9] Global Netoptex Incorporated, “Demystifying the cloud. Important opportunities, crucial choices”, 13 December, 2009, pp. 4-14. [Online]. Available from: http://www.gni, [accessed January 2013].

[10] Kuyoro S.O., "Cloud Computing Security Issues and Challenges", Proc. International Journal of Computer Networks (IJCN), 2011, vol. 3, Issue: 5.

[11] KavithaV. and Subashini S.,“A survey on security issues in service delivery models of cloud”, International Journal of Network and Computer Applications, January 2011, vol. 34 Issue 1, pp.1-11

[12] Robinson N., Valeri L., Cave J., Starkey T., Graux H., Creese S., Hopkins P.: The Cloud: Understanding the Security, Privacy and Trust Challenges. Prepared for the Unit F.5, Directorate- General Information Society and Media, European Commission (2010)

[13] Pallis, George. "Cloud Computing: The New Frontier of Internet Computing." IEEE Internet Computing 14.5 (2010): 70-73. [Online]. Available from: http://cgi.di.uoa.gr/~ad/M155/Papers/palis-ic10.pdf, [accessed November 2012].

[14] “Securing the Cloud: A Review of Cloud Computing, Security Implications and Best Practices”. Available from :http://www.centurylinktechnology.com/sites/default/files/savvis_vmw_whitepaper_0809.pdf [accessed January 2013].

[15] Sans Institute, "An Introduction to Securing a Cloud Environment”, June 2012. [Online]. Available from: https://www.sans.org/reading-room/whitepapers/cloud/introduction-securing-cloud-environment-34052 [accessed November 2012].

[16] Cloud Security Alliance: “The Notorious Nine: Cloud Computing Top Threats in 2013”. [Online]. Available from: http://www.cloudsecurityalliance.org/topthreats/, 2013

[17] D. Lekkas, Establishing and managing trust within the public key infrastructure, Computer Communications 26 (16) (2003).

[18] G. Reese, Cloud Application Architectures: Building Applications and Infrastructure in the Cloud, in: Theory in Practice, O'Reilly Media, 2009.

[19] B. Rajkumar, C. Yeo, S. Venugopal, S. Malpani, Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility, Future Generation Computer Systems (2009)

[20] https://www.techopedia.com/definition/25114/cloud-computing-security

[21] http://www.wtmnews.gr/it-services-07/2792-Gartner-Global-IT-Council-for-Cloud-Services-Outlines-Rights-and-Responsibilities.html

[22] Wang, J.-J.; Mu, S. Security issues and countermeasures in cloud computing. In Proceedings of the 2011 IEEE International Conference on Grey Systems and Intelligent Services (GSIS), Nanjing, China, 15–18 September 2011; pp. 843–846.

[23] Houmansadr, A.; Zonouz, S.A.; Berthier, R. A cloud-based intrusion detection and response system for mobile phones. In Proceedings of the 2011 IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops (DSN-W), Hong Kong, China, 27–30 June 2011; pp. 31–32.

[24] Gu, C.-D.; Li, J.-X.; Wu, J.-P.; Fu, Y.-L.; Lu, K.; Si, M.-X. Wireless broadband application technology investigation of IPv6 optical network cloud computing. In Proceedings of the 2010 6th International Conference on Advanced Information Management and Service (IMS), Seoul, Korea, 30 November–2 December 2010; pp. 191–194.

[25] Sabahi, F. Virtualization-level security in cloud computing. In Proceedings of the 2011 IEEE 3rd International Conference on Communication Software and Networks (ICCSN), Xi'an, China, 27–29 May 2011; pp. 250–254.

[26] Wang, C.; Wang, Q.; Ren, K.; Lou, W. Towards secure and dependable storage services in cloud computing. IEEE Trans. Serv. Comput. 2012, 5, 220–232.

[27] Lingfeng, C.; Hoang, D.B. Towards scalable, fine-grained, intrusion-tolerant data protection models for healthcare cloud. In Proceedings of the 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Changsha, China, 16–18 November 2011; pp. 126–133.

[28] Morin, J.; Aubert, J.; Gateau, B. Towards cloud computing SLA risk management: Issues and challenges. In Proceedings of the 2012 45th Hawaii International Conference on System Science (HICSS), Maui, HI, USA, 4–7 January 2012; pp. 5509–5514.

[29] Gul, I.; ur Rehman, A.; Islam, M.H. Cloud computing security auditing. In Proceedings of the 2011 The 2nd International Conference on Next Generation Information Technology (ICNIT),Gyeongju, Korea, 21–23 June 2011; pp. 143–148.

[30] Kandukuri, B.R.; Paturi, V.R.; Rakshit, A. Cloud security issues. In Proceedings of the IEEE International Conference on Services Computing, 2009 (SCC '09), Bangalore, India,21–25 September 2009; pp. 517–520.

[31] Chen, Z.; Yoon, J. IT auditing to assure a secure cloud computing. In Proceedings of the 2010 6thWorld Congress on Services (SERVICES-1), Miami, FL, USA, 5–10 July 2010; pp. 253–259.

[32] Tripathi, A.; Mishra, A. Cloud computing security considerations. In Proceedings of the 2011 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC),Xi'an, China, 14–16 September 2011; pp. 1–5.

[33] Sengupta, S.; Kaulgud, V.; Sharma, V.S. Cloud computing security—Trends and research directions. In Proceedings of the 2011 IEEE World Congress on Services (SERVICES),Washington, DC, USA, 4–9 July 2011; pp. 524–531.

[34] Chow, R.; Golle, P.; Jakobsson, M.; Shi, E.; Staddon, J.; Masuoka, R.; Molina, J. Controlling data in the cloud: Outsourcing computation without outsourcing control. In Proceedings of the 2009 ACM Workshop on Cloud Computing Security, Chicago, IL, USA, 13 November 2009; ACM Press: New York, NY, USA, 2009; pp. 85–90.

[35] Samarati, P.; di Vimercati, S.D.C. Data protection in outsourcing scenarios: Issues and directions. In Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security (ASIACCS '10), Chicago, IL, USA, 4–8 October 2010; ACM: New York, NY, USA, 2010; pp. 1–14.

[36] Popovic, O.; Jovanovic, Z.; Jovanovic, N.; Popovic, R. A comparison and security analysis of the cloud computing software platforms. In Proceedings of the 2011 10th International Conference on Telecommunication in Modern Satellite Cable and Broadcasting Services (TELSIKS), Nis, Serbia, 5–8 October 2011; Volume 2, pp. 632–634. Computers 2014, 3 30

[37] European Network and Information Security Agency – ENISA . "Cloud Computing: Benefits, Risks and Recommendations for Information Security", 2009. [Online]. Available from: http://www.enisa.europa.eu/activities/riskmanagement/files/deliverables/cloudcomputing-risk-assessment/at_download/fullReport

[38] Cloud Security Alliance – CSA, Top Threats Working Group (2013). The Notorious Nine - Cloud Computing Top Threats in 2013. [Online]. Available from : http://www.cloudsecurityalliance.org/topthreats

[39] International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 11, November 2015 Copyright to IJIRCCE DOI: 10.15680/IJIRCCE.2015. 0311243 11969 Improved Trusted Third Party Auditing in Shared Cloud Environment B Nagarjuna, G Lakshmi Vara Prasad

[40] Outlook: Cloudy with a Chance of Security Challenges and Improvements. [Online]. Available from: https://www.computer.org/cms/ComputingNow/homepage/2010/0310/W_SP_OutlookCloudy.pdf

[41] KPMG (2010) From hype to future: KPMG's 2010 Cloud Computing survey. [Online]. Available from: http://www.techrepublic.com/whitepapers/from-hype-to-futurekpmgs-2010-cloud-computing-survey/2384291KSHETRI, N. (2013) Privacy and security issues in cloud computing: The role of institutions and institutional evolution. Telecommunications Policy, 37, 372-386.

[42] Almporsy, M., Grundy, J. & Ibrahim, A. S. (2011) Collaboration-Based Cloud Computing Security Management Framework. IEEE 4th International Conference on Cloud Computing.

[43] Lombardi, F. & Di Pietro, R. (2011) Secure virtualization for cloud computing. Journal of Network and Computer Applications, 34, 1113-1122.

[44] Stinchcombre, N. (2009) Cloud computing in the spotlight. Infosecurity, 6, 30-33.

[45] Mansfield-Devine, S. (2008) Danger in the clouds. Network Security, 2008, 9-11.

[46] SUBASHINI, S. & KAVITHA, V. (2011) A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34, 1-11.

[47] Abdul Nasir Khan, M.L. Mat Kiah, Samee U. Khan & Madani, S. A. (2013) Towards secure mobile cloud computing: A survey. Future Generation Computer Systems, 29, 1278- 1299.

[48] ENISA, "Cloud computing: benefits, risks and recommendations for information security," 2009, [Online]. Available from: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computingrisk-assessment. [Accessed On July 2010]

[49] Bernd Grobauer, Tobias Walloschek and Elmar Stöcker, "Understanding Cloud-Computing Vulnerabilities," IEEE Security and Privacy, vol. 99,2010

[50] Rosado, D., Gómez, R., Mellado, D., Fernández-Medina, E.: Security Analysis in the Migration to Cloud Environments. Future Internet 4(2), 469-487 (2012)

[51] Rebollo, O., Mellado, D., F-Medina, E.: A Comparative Review of Cloud Security Proposals with ISO/IEC 27002. In : Proceedings of the 8th International Workshop on Security in Information Systems, pp.3-12 (2011)

[52] R.K. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, B.S. Lee, TrustCloud: A framework for accountability and trust in cloud computing, in: 2011 IEEE World Congress on Services, SERVICES, July, 2011, pp. 584–588.

[53] S. Pal, S. Khatua, N. Chaki, S. Sanyal, A new trusted and collaborative agent based approach for ensuring cloud security, 2011. arXiv Preprint arXiv:1108.4100.

[54] E.B.Fernandez, Raul Monge, and Keiko Hashizume, “Building a security reference architecture for cloud systems”, Requirements Engineering. (2015).

[55] Huan,D., Zhang, X., Kang ,M., Luo ,J.: MobiCloud: building secure cloud framework for mobile computing and communication, in: Proc. 5th IEEE Int. Symposium on Service Oriented System Engineering, SOSE ’10, Nanjing, China,(June 2010)

[56] NIST, Framework for Improving Critical Infrastructure Cybersecurity, Technical Report, Version 1.0, February, 2014

[57] Divers S. - SANS Institute, "Information Security Policy A development Guide for large and small companies", November 2007, pp. 43-44.

[58] Svantesson D. and Clarke R., “Privacy and consumer risks in Cloud Computing", Computer Law and Security Review, vol. 26, 2010, pp. 391-397.

[59] Kshetri, N., “Privacy and security issues in Cloud Computing: The role of institutions and institutional evolution”. 2012, Bryan School of Business and Economics, The Univ. of North Carolina at Greensboro, NC27402-6165,USA.

[60] Hone K., Eloff J. H., “Information security policy: what do international information security standards say?”, Proc. of the 8th European Conference on Information Warfare and Security, Computers

[61] Dikaiakos, Katsaros M.D., Mehra D., Pallis P. and Vakali G, “Cloud Computing Distributed Internet Computing for IT and Scientific Research”, IEEE Press 2009, vol. 13, Issue: 5, pp. 10-13.

[62] European Network and Information Security Agency (Enisa), “Cloud Computing Benefits, risks and recommendations for information security”, November 2009.

[63] Arnold S., “Cloud Computing and the issues of privacy”, July 2009, KM World, pp.14-22

[64] Whitepaper, A, “Enterprise Cloud Computing: Transforming IT”, Platform Computing, viewed 13 March 2010, pp.6.

[65] Global Netoptex Incorporated, “Demystifying the cloud. Important opportunities, crucial choices”, 13 December, 2009, pp. 4-14., [Online]. Available from: http://www.gni.

[66] Kuyoro S.O., "Cloud Computing Security Issues and Challenges", Proc. International Journal of Computer Networks (IJCN), 2011, vol. 3, Issue: 5.

[67] KavithaV. and Subashini S.,“A survey on security issues in service delivery models of cloud”, International Journal of Network and Computer Applications, January 2011, vol. 34 Issue 1, pp.1-11

[68] Brodkin J., “Gartner: Seven cloud- computing security risks”, NetworkWorld, April 2013, [Online]. Available from: http://www.idi.ntnu.no/emner/tdt60/papers/Cloud_Computing_Security_Risk.pdf

[69] Okuhara M. et al- FUJITSU, “Security Architecture for Cloud Computing”, vol. 46, no 4, October 2010, Sci.Tecch.J., pp.397- 402].

[70] Min Y., Shin H., Bang Y., “Cloud Computing Security Issues and Access Control Solutions”, Journal of Security Engineering, February 2012, vol. 9, no2.

[71] National Institute of Standards and Technology, “Cloud Computing Synopsis and Recommendations”, May 2012, Special Publication 800-146.

[72] Gellman R., “Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing”, World Privacy Forum February 2009, [Online]. Available from: http://www.scribd.com/doc/12805751/ Privacy-in-Cloud-Computing-World-Privacy-Council-Feb-2009, [accessed November 2013].

[73] Chadwick W.D. and Fatema K., "A privacy preserving authorization system for the cloud", November 2012.

[74] European Network and Information Security Agency, “Cloud Computing benefits, risks and recommendations for information security”, 2009.

[75] Morsy M. Al., Grundy J. and Müller I., “An Analysis of the Cloud Computing Security Problem”, Proc. APSEC 2010 Cloud Workshop, Sydney, Australia, 2010.

[76] Karadsheh L. “Applying security policies and service level agreement to IaaS service model to enhance security and transition ”Computers & Security, vol. 31, Issue 3, May 2012, pp. 315-326.

[77] Cheng F., and Lai W., “The impact of Cloud Computing Technology on Legal Infrastructure within Internet-Focusing on the Protection of Information Privacy”, Proc International Workshop on Information and Electronics Engineering, Elsevier Ltd Press 2012, vol.29, pp.241-251, doi: 10.1016/j.proeng.2011.12.701

[78] Vaquero M., Rodero-Merino L., and Moran D., “ Locking the Sky: A Survey on IaaS Cloud Security Computing”. Springer. Press, January 2011, vol. 91, Number 1, pp. 93-118. doi: 10.1007/s00607-010-0140-x

[79] European Commission. “Official Journal of the European Union On Data protection guidelines for the Early Warning and Response System”, 9 February 2012 L 36/31.

[80] [26] Pearson S. and Charlesworth A., “Accountability as a Way Forward for Privacy Protection in the Cloud”, HP Laboratories HPL-2009-178, Proc. 1st CloudCom, Beijing, Springer LNCS Press, December 2009.

[81] European Commission, “Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21th Century” COM (2012), 25 January 2012, article 9 final Brussels.

[82] Jaeger P.T., Lin J. and Grimes J.M., “Cloud Computing and Information Policy: Computing in a Policy Cloud?”, Forthcoming in the Journal of Information Technology and Politics (ITI 2008), vol. 5, no. 3, pp. 269-283.

[83] National Institute of Standards & Technology – “Cloud Computing Standards Roadmap” Special Publication 500-291, Version 2, [Online]. http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=913661

[84] Cloud Security Alliance , “Security as a Service Implementation Guidance” 2012 , [Online] Available from https://cloudsecurityalliance.org/group/security-as-a-service/#_downloads

[85] Cloud Security Alliance, “Security Guidance for Critical Areas of focus in Cloud Computing” V3.0 .Available from: https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/csaguide.v3.0.pdf

[86] Cloud Security Alliance “The Treacherous Twelve Cloud Computing Top Threats in 2016” [Online]. Available from: https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1-july-2014/

[87] European Union Agency for Network and Information Security (ENISA),, “Good practice guide for Securing Deploying Governmental clouds”, 15 November 2013. [Online]. Available from: https://www.enisa.europa.eu/publications/good-practice-guide-for-securely-deploying-governmental-clouds

[88] European Union Agency for Network and Information Security (ENISA), “Security Framework for Governmental Clouds”, February 2015. [Online] Available from: https://www.enisa.europa.eu/publications/security-framework-for-governmental-clouds

[89] Fernandes, Diogo A., Liliana F. Soares, João V. Gomes, Mário M. Freire, and Pedro R. Inácio. 2014. “Security Issues in Cloud Environments: A Survey.” Int. J. Inf. Secur. 13 (2): 113–170. doi:10.1007/s10207-013-0208-

[90] Madhan Kumar Srinivasan, K. Sarukesi, Paul Rodrigues, M. Sai Manoj, and P. Revathy. 2012. “State-of-the-Art Cloud Computing Security Taxonomies: A Classification of Security Challenges in the Present Cloud Computing Environment.” In Proceedings of the International Conference on Advances in Computing, Communications and Informatics, 470–476. ICACCI ’12. New York, NY, USA: ACM. doi:10.1145/2345396.2345474.

[91] European Union Agency for Network and Information Security (ENISA), “Glossary — ENISA". https://www.enisa.europa.eu/topics/csirts-in-europe/glossary, July 2009.[Retrieved 2013-11-05].

[92] National Information Assurance Glossary. Available from: http://jitc.fhu.disa.mil/pki/documents/committee_on_national_security_systems_instructions_4009_june_2006.pdf …

[93] ISO/IEC, "Information technology - Security techniques-Information security risk management" ISO/IEC FIDIS 27005:2008

[94] Technical Standard Risk Taxonomy ISBN 1-931624-77-1 Document Number: C081 Published by The Open Group, January 2009.

[95] National Institute of Standards & Technology. “Risk Management Guide for Information Technology Systems”. Available from: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

[96] ISACA https://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf

[97] European Union Agency for Network and Information Security (ENISA), “Benefits, risks and recommendations for information security”, November 2009

[98] European Union Agency for Network and Information Security (ENISA),” ENISA Threat Landscape 2015”, January 2016

[99] Cloud Security Alliance – CSA, Top Threats Working Group (2013). The Notorious Nine - Cloud Computing Top Threats in 2013. [Online]. Available from : http://www.cloudsecurityalliance.org/topthreats

[100] European Commission Digital Agenda, ”Use of Cloud Services. [Online] Available from: ec.europa.eu/newsroom/dae/document.cfm?doc_id=9967

[101] ISACA “Cloud Computing: Business Benefits with Security, Governance and Assurance Perspectives”, White Paper Information Systems Audit and Control Association, 2009

[102] Glenn Brunette and Rich Mogull "Security Guidance for Critical Areas of Focus in Cloud Computing", Technical Report, Cloud Security Alliance, 2009

[103] Radha Krishna Reddy, S. Pavan Kumar Reddy, G.Sireesha and U.Seshadri "The Security Issues of Cloud Computing Over Normal & IT Sector" , International Journal of Advanced Research in Computer Science and Software Engineer, Vol.2, Issue 3, March 2012

[104] S.Ramgovid M., M. Eloff , E. Smith "The Management of Security in Cloud Computing" in proc. 2010 IEEE International Conference on Cloud Computing 2010

[105] Jon Brodkin " Gartner: Seven cloud-computing security risks" Infoworld, 2008

[106] Dimitra Georgiou and Costas Lambrinoudakis "A Security Policy for Cloud Providers The Software-as-a-Service-Problem", ICIMP 2014 : The Ninth International Conference on Internet Monitoring and Protection

[107] Goodwin, L. Courtney, K. Kirby, D. and M. A. Iannacchione (2002). "A pilot study: Patients' perceptions about the privacy of their medical records." Online Journal of Nursing Informatics, 6(3)

[108] Flynn, H. Marcus, S. Kerber, K. and N. Alessi (2003). "Patients' concerns about and perceptions of electronic psychiatric records." Psychiatric Services, 54(11), 1539–1541.

[109] Silber D. (2003). European Commission, Information Society, eHealth Conference. Atlanta, Belgium [Online]. Available from: www.openclinical.org/e-Health.html

[110] A Framework of Authentication and Authorization for e-Health Services

[111] H. Oh, C. Rizo, M. Enkin, and A. Jadad, "What is eHealth (3): a systematic review of published definitions," Journal of medical Internet research, vol. 7, no. 1, 2005.

[112] R.E. Scott, M.F.U. Chowdhury, S. Varghese, "Telehealth policy: looking for global complementarity", J. Telemed. Telecare 8 (2002) 55—57.

[113] F/P/T Advisory Committee on HealthInfostructure," Blueprint and Tactical Plan for a pan-Canadian Health Infostructure"—A Report on F/P/T Collaboration for the Planning of the Canadian Health Infostructure. Office of Health and the Information Highway, Health Canada, Ottawa, December 2000.

[114] "Gematik - gesellschaft fur telematikanwendungen der gesundheitskarte." http://www.gematik.de, 2011.

[115] C. Chatman, "How cloud computing is changing the face of health care information technology," J Health Care Compliance, vol. 12, pp. 37–70, 2010.

[116] J. T. Dudley, Y. Pouliot, R. Chen, A. A. Morgan, and A. J. Butte, "Translational bioinformatics in the cloud: an affordable alternative," Genome Med, vol. 2, p. 51, 2010.

[117] J. Kabachinski, "What's the forecast for cloud computing in healthcare?, "Biomed Instrum Technol, vol. 45, pp. 146–50, 2011.

[118] Meingast M, Roosta T and Sastry S. Security and privacy issues with health care information technology. Conf Proc IEEE Eng Med Biol Soc 2006; 1: 5453–5458.

[119] Shmatikov V. Anonymity is not privacy: technical perspective. Commun ACM; 2011; 54: 132–132.

[120] Reynolds B, Venkatanathan J, Gonçalves J and Kostakos V. Sharing ephemeral information in online socialnetworks: privacy perceptions and behaviours. Proc of Interact 2011; 3: 204–215.

[121] De Vimercati SDC, Foresti S, Livraga G and Samarati P. Protecting privacy in data release. In: Aldini A and Gorrieri R (eds) FOSAD VI. Berlin: Springer, 2011, pp.1–34.

[122] Karl A. Stroetmann, Jörg Artmann, Veli N. Stroetmann, Denis Protti, Jos Dumortier, Sarah Giest, Uta Walossek and Diane Whitehouse , "European countries on their journey towards national eHealth

infrastructures" European Commission ,Information Society [Online]. Available from www.ehealth-strategies.eu/report/report.html

[123] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, COM(2012) 736 final: e Health Action Plan 2012–2020-Innovative healthcare for the 21st century{SWD (2012) 413 final} {SWD(2012)414 final} Brussels European Commission; 2012.

[124] Communication from the Commission to the Council the European Parliament ,the European Economic and Social Committee and the Committee of the Regions, COM(2004) 356: e-Health—making health care better for European citizens: an action plan for a European e-Health Area {SEC(2004) 539} Brussels:EuropeanCommission;2004.

[125] Commission Staff Working Document on the applicability of the existing EU legal framework to telemedicine services, SWD (2012) 414 final—accompanying the document Communication from the Commission to the Council the European Parliament ,the European Economic and Social Committee and the Committee of the Regions, e Health Action Plan 2012–2020 innovative healthcare for the 21st century {COM(2012)736 final}{SWD (2012)413 final} Brussels: European Commission; 2012.

[126] Action77:Foster EU-wide standards, interoperability testing and certification of eHealth: digital Agenda for Europe. Available from: [http://ec.europa.eu/digital-agenda/en/pillar-vii-ict-enabled-benefits-eu-society/action-77-foster-eu-wide-standards-interoperability] [cited 28.08.14].

[127] Dobrev Alexander, Jones Tom, Stroetmann Veli, Stroetmann Karl, Vatter Yvonne, Peng K. Interoperable eHealth is worth it. Securing benefits from electronic health records and ePrescribing. Study report. Bonn/Brussels: European Commission; 2010.

[128] EU activities in the field of e Health interoperability and standardization: an overview [press release]. European Commission; 2013.

[129] "Europe's Information Society eHealth portal". [Online] Available from: http://europa.eu.int/information_society/activities/health.

[130] eHealth—making healthcare better for European Citizens: an action plan for a European eHealth area. Brussels: European Commission; 2004

[131] European Commission. (2012). eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century. URL: http://ec.europa.eu/health/ehealth/docs/com_2012_736_en.pdf (visited on 12/12/2014)

[132] European Parliament, Council of the European Union. Decision on adopting a programme of Community action on health monitoring within the framework of action in the field of public health (1997–2001) (1400/97/EC). Off J EurCommunities 1997;40:1–10.

[133] European Parliament, Council of the European Union. Decision on adopting a programme of Community action in the field of public health (2003–2008) (1786/2002/EC). Off J Eur Union 2002; 45:1–11.

[134] European Parliament, Council of the European Union. Decision on establishing a second programme of Community action in the field of health (2008–13) (1350/2007/EC). Off J Eur Union 2007; 50:3–13.

[135] eHealth Industries Innovation, "What is e Health?," e Health Industries Innovation (ehi2) Centre, [Online]. Available from: http://www.ehi2.swan.ac.uk/en/what-is-ehealth.htm. [Accessed 3 Apr 2014].

[136] European Commission. (2012). eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century. URL: http://ec.europa.eu/health/ehealth/docs/com_2012_736_en.pdf (visited on 12/12/2014)

[137] Khazaei H, Misic J, Misic V: Performance analysis of cloud computing centers using M/G/m/m+r. queuing systems. IEEE Trans Parallel Distributed Syst 2012, 23:5.

[138] Wang L, von Laszewski G, Younge A, He X, Kunze M, Tao J, Fu C: Cloud computing: A perspective study. New Generation Comput 2010,28:137–146.

[139] Kleinrock L: Queueing Systems: Theory, vol. 1. Wiley-Interscience, 1975.Published in Russian, 1979. Published in Japanese, 1979. Published in Hungarian, 1979. Published in Italian 1992.

[140] Mao M, Li J, Humphrey M: Cloud auto-scaling with deadline and budget constraints. In Grid Computing (GRID), 2010 11th IEEE/ACM International Conference; 2010:41–48.

[141] Barham P, Dragovic B, Fraser K, Hand S, Harris T, Ho A, Neugebauer R, Pratt I, Warfield A: Xen and the art of virtualization. SIGOPS Oper Syst Rev2003, 37(5):164–177.

[142] WMWare Staff: Virtualization overview. White paper. [Online]. Available from: [http://www.vmware.com/pdf/virtualization.pdf]. 2012-08-25.

[143] The OpenStack Project: OpenStack: The open source cloud operating system. Available from: [http://www.openstack.org/software/]. 2012-08-25.

[144] Mell P, Grance T: The NIST definition of cloud computing. Gaithersburg: NIST Special Publication 800-145; 2011. 20899-8930.