Πανεπιστήμιο Πειραιώς

Τμήμα Ψηφιακών Συστημάτων

Π.Μ.Σ. "Τεχνοοικονομική Διοίκηση & Ασφάλεια Ψηφιακών Συστημάτων"

Κατεύθυνση «Ασφάλεια Ψηφιακών Συστημάτων»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Διαχείριση ασφαλείας πληροφοριακού συστήματος Γενικού Νοσοκομείου με ευαίσθητα προσωπικά δεδομένα.

Μίχα Μαρία, MTE14017

Επιβλέπων: κ.Λαμπρινουδάκης Κωνσταντίνος, Αναπληρωτής Καθηγητής

Πειραιάς, Απρίλιος 2016

Εξεταστική Επιτροπή

……

Κωνσταντίνος Λαμπρινουδάκης
Αναπληρωτής Καθηγητής
Πανεπιστήμιο Πειραιώς

Πρόλογος -Ευχαριστίες

Η παρούσα διπλωματική εργασία εκπονήθηκε στο Τμήμα Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς, στα πλαίσια του μεταπτυχιακού διπλώματος ασφάλεια ψηφιακών συστημάτων.

Αντικείμενο της παρούσας διπλωματικής εργασίας είναι η ανάλυση και διαχείριση επικινδυνότητας των πληροφοριακών συστημάτων ενός Νοσοκομείου της Ελλάδας με ευαίσθητα δεδομένα. Για λόγους μη αποκάλυψης των δεδομένων του Νοσοκομείου θα διατηρηθεί η ανωνυμία των στοιχείων τους. Η ανάλυση και διαχείριση κινδύνων των ΠΣ του ΓΝ υλοποιείται με την μεθοδολογία MAGERIT και το λογισμικό Pilar. Σύμφωνα με αυτήν γίνεται αποτίμηση των επιπτώσεων, των απειλών και των τρωτοτήτων για τα δεδομένα που διαχειρίζονται τα πληροφοριακά συστήματα του Νοσοκομείου.

Στο σημείο αυτό θα ήθελα να ευχαριστήσω τον επιβλέποντα αναπληρωτή καθηγητή $κ_ο$ Λαμπρινουδάκη Κωνσταντίνο ο οποίος με βοήθησε να ασχοληθώ με το θέμα αυτό και με στήριξε κατά τη διάρκεια της εκπόνησης της διπλωματικής μου εργασίας.

Τέλος, θέλω να ευχαριστήσω την οικογένεια μου για την υπομονή τους και την ενθάρρυνση που μου έδωσαν καθ’ όλη τη διάρκεια των μεταπτυχιακών μου σπουδών.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Περίληψη

Οι ολοένα μεταβαλλόμενες απειλές των σύγχρονων πληροφοριακών συστημάτων έχουν αυξήσει τους κινδύνους και κατ' επέκταση την ανάγκη για ασφάλεια στα συστήματα επικοινωνιών και πληροφορικής.

Αντικείμενο της διπλωματικής εργασίας αυτής είναι η ανάλυση και διαχείριση κινδύνων πληροφοριών και συγκεκριμένα η **σύγκριση οκτώ από τις επικρατέστερες μεθοδολογίες** – **εργαλεία.** Μέσω αυτής της διαδικασίας αναδείχθηκαν τα πλεονεκτήματα και μειονεκτήματα των μεθοδολογιών και η ανάγκη χρήσης τους σε συγκεκριμένες περιπτώσεις.

Εν συνεχεία, περιγράφεται μια μελέτη περίπτωσης ανάλυσης και διαχείρισης επικινδυνότητας Το σύστημα που χρησιμοποιήθηκε ως **μελέτη περίπτωσης ασφαλείας των Πληροφοριακών Συστημάτων(ΠΣ) είναι ένα υπαρκτό ενός Γενικού Νοσοκομείου** της Ελλάδας. Η μελέτη έγινε με τη **ποσοτική ανάλυση επικινδυνότητας** της μεθοδολογίας **Metodologia de Analysis y Gestion de Riesgos de los Sistemas de Informacion (Magerit)** μέσω του περιβάλλοντος ανάλυσης κινδύνου Environment for the Analysis of Risk **(EAR) /Pilar.**

Σε αυτή τη διπλωματική αρχικά, προσδιορίζονται τα κρίσιμα περιουσιακά στοιχεία του εν λόγω ΠΣ-ΓΝ και αποτιμούνται. Εν συνεχεία, προσδιορίζονται οι απειλές που θεωρούμε ότι υφίστανται τα στοιχεία αυτά. και αποτιμούνται. Ετσι, καθορίσαμε υφιστάμενα αντίμετρα για να υπολογιστεί η εναπομείνασα επίπτωση Με βάση αυτήν, **υπολογίστηκε η εναπομείνασα επικινδυνότητα** για κάθε μια απειλή, αξιολογήθηκε η κρισιμότητα του κινδύνου και αποφασίστηκε η διαχείριση του.

Ακολούθως, παρουσιάζεται **ένα συνοπτικό σχέδιο ασφαλείας για το Νοσοκομείο**, το οποίο συμπεριλαμβάνει τα μέτρα ασφαλείας από την ανάλυση και διαχείριση επικινδυνότητας που αντιμετωπίζουν τις απειλές στα συγκεκριμένα περιουσιακά στοιχεία και την πολιτική ασφαλείας του Νοσοκομείου.

Στο τελευταίο κεφάλαιο, γίνεται μια **αποτίμηση και συμπεράσματα για βελτιώσεις** της μεθόδου MAGERIT και του περιβάλλοντος ανάλυσης κινδύνων EAR/Pilar όσον αφορά την καταλληλότητα και τα πλεονεκτήματα που προσφέρει για το εν λόγω ΠΣ-ΓΝ

Λέξεις-κλειδιά :

Περιουσιακά Στοιχεία, Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα, Απειλή, Επίπτωση, Ανάλυση Κινδύνου, Διαχείριση Κινδύνου, Αντίμετρο, Σχέδιο Ασφαλείας, Πολιτική Ασφαλείας, MAGERIT, EAR/PILAR, OCTAVE, EBIOS, CallioSecura, CCS Risk Manager, Cloud Assurance, CRAMM, COBRA.

Abstract

The threats of the contemporary information systems have increased the dangers and further more the need for security of the information systems.

The scope of this master thesis is the risk analysis and management of information, and specifically the comparison of eight of the contemporary methods and tools. Through this procedure the advantages and disadvantages of the methodologies are revealed and the need of their use was evaluated.

Consequently, a security study of risk analysis and management of a Greek Hospital's information system was performed. The study used the quantitative risk analysis methodology MAGERIT and the environment for the Analysis of Risk EAR/Pilar.

To begin with, in this security study the critical elements were defined of the specific information system and they were valued via interviews. Next, threats were defined for the specific assets and they were valued. After that, the dependencies were valued so as the remaining risk was calculated. Consequently, the remaining risk was calculated for every threat for every asset. Finally, priorities of safeguards were defined and the decisions from management for the protection of assets was taken.

Consequently, we presented a **summary of the security plan for the Hospital**, which includes the security procedures suitable for these threats.

At the last chapter, we present the suitability of the Magerit method for the specific system and the advantage offered for the risk management of the specific information system. Finally, there are some thoughts for improvement for the specific implementation for the risk management of the information system of the Greek hospital.

Keywords:

Assets, Confidentiality, Integrity, Availability, Threat, Impact, Vulnerability, Risk Analysis, Safeguards, Risk Management, Security Plan, Security Policy, MAGERIT, EAR/PILAR, OCTAVE, EBIOS, CallioSecura, CCS Risk Manager, Cloud Assurance, CRAMM, ISO31000, COBRA.

1. Κεφάλαιο 1: Εισαγωγή

1.1 Σκοπός

Η συγκεκριμένη διπλωματική εργασία αποσκοπεί στην εκπόνηση μελέτης ανάλυσης και διαχείρισης κινδύνων με την μεθοδολογία **MAGERIT** και το αυτοματοποιημένο εργαλείο ανάλυσης και διαχείρισης κινδύνων **EAR/Pilar** για το πληροφοριακό σύστημα(ΠΣ) ενός Γενικού Νοσοκομείου (ΓΝ) της Ελλάδας.

Είναι αποδεκτό ότι όλες οι τεχνολογικές εξελίξεις βοηθούν έναν μεγάλο Οργανισμό όπως είναι το νοσοκομείο να εφαρμόσει συστήματα με αρχιτεκτονικές ασφαλείας για την καλύτερη παροχή υπηρεσιών προς τους πολίτες. [1],[2],[3] Παρόλα αυτά τα στοιχεία των πρόσφατων επιθέσεων αποκαλύπτουν ότι οι ευπάθειες υφίστανται στα περιουσιακά στοιχεία σε ανεπαρκείς αρχιτεκτονικές ασφαλείας και σε περιπτώσεις μη ορθής εφαρμογή τους. Έτσι, το συνολικό κόστος των διαρροών έχει ανέβει δραματικά, καθώς οι οργανισμοί αντιμετωπίζουν κόστη αρκετών εκατομμυρίων για την αντιμετώπιση των διαρροών, την διόρθωση τους, την απώλεια της φήμης, των ευαίσθητων προσωπικών δεδομένων, καθώς και μηνύσεις και απώλεια αξιοπιστίας παροχής υπηρεσιών. Για να επιτευχθεί αυτό, πολλές εταιρείες υιοθέτησαν καινούργιες τεχνικές στους παραδοσιακούς περιορισμούς της έλλειψης εξειδίκευσης, χρόνου και χρημάτων.

Ο κύριος στόχος της πολιτικής ασφαλείας δεν είναι μόνο να προστατεύσει τα περιουσιακά στοιχεία του οργανισμού αλλά και να διασφαλίσει την προστασία του Νοσοκομείου.

1.2 Δομή Διπλωματικής

Συνοπτικά, παρουσιάζεται η δομή της διπλωματικής εργασίας η οποία χωρίζεται σε τέσσερα μέρη (εισαγωγή, σύγκριση μεθοδολογιών-εργαλείων, μελέτη περίπτωσης ΠΣΓΝ και σχέδιο ασφαλείας) με επιμέρους κεφάλαια:

Στο **πρώτο κεφάλαιο** γίνεται συνοπτική αναφορά στην ορολογία των βασικών εννοιών της ανάλυσης και διαχείρισης κινδύνου.

Στο **δεύτερο κεφάλαιο** αναλύονται οι σύγχρονες μεθοδολογίες που χρησιμοποιούνται **COBRA (Consultative, Objective and Bi-functional Risk Analysis), OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), Callio Secura 17799 της Callio Technologies Software Informer,** (**Expression des Besoins et Identification des Objectifs de Sécurité), MAGERIT με εργαλείο EAR/Pilar, CRAMM** από την **Insight Consulting** μέθοδος **CloudeAssurance** της **eFortresses, Inc**. Συμπερασματικά, γίνεται μια σύγκριση [4] μεταξύ των εργαλείων αυτών.

Στο **τρίτο κεφάλαιο** καθορίζονται λεπτομερέστατα τα κρίσιμα συστήματα του ΠΣ-ΓΝ, η αποτίμηση τους σύμφωνα με την μεθοδολογία MAGERIT. Επίσης, παρουσιάζονται τα σενάρια των απειλών σε αυτά και η αποτίμηση τους. Ακολούθως, αναλύεται η μεθοδολογία υπολογισμού του βαθμού επικινδυνότητας για κάθε περιουσιακό στοιχείο και η τελική αποτίμηση του. Συμπερασματικά, καταγράφονται οι κυριότερες κατηγορίες μέτρων από τις οποίες προκύπτουν τα απαραίτητα μέτρα ασφαλείας και συμπεριλαμβάνονται στο σχέδιο ασφαλείας για το συγκεκριμένο του ΠΣ-ΓΝ.

Στο **τέταρτο κεφάλαιο** παρουσιάζεται μια αποτίμηση της διαχείρισης επικινδυνότητας και του σχεδίου ασφαλείας του συγκεκριμένου ΠΣ του ΓΝ. Επίσης, αναφέρονται κάποιες προτάσεις για βελτιώσεις.

1.3 **Εννοιες - Ορισμοί**

Στην παρούσα διπλωματική αναφέρεται η ακόλουθη ορολογία:

Βασικές Έννοιες	**Ορισμοί**
Πληροφοριακό Σύστημα	Ένα οργανωμένο σύνολο αλληλεπιδρώντων στοιχείων (εφαρμογές, υπηρεσίες, άνθρωποι, δεδομένα, περιουσιακά στοιχεία της τεχνολογίας της πληροφορίας, λογισμικό, υλικός εξοπλισμός, διαδικασίες), το οποίο επεξεργάζεται δεδομένα και παράγει πληροφορίες για λογαριασμό μιας επιχείρησης ή ενός οργανισμού.
Ασφάλεια Πληροφοριακού Συστήματος	Το οργανωμένο πλαίσιο από έννοιες, αρχές, διαδικασίες, τεχνικές και μέτρα που απαιτούνται, για να προστατευθούν τόσο τα στοιχεία του ΠΣ όσο και ολόκληρο το ΠΣ από τυχαία ή σκόπιμη απειλή.
Περιουσιακά Στοιχεία ή Αγαθά (Assets)	Πληροφορίες, δεδομένα ή υπολογιστικοί πόροι που έχουν αξία, άρα σπουδαιότητα εκφραζόμενη σε χρηματικούς ή άλλους όρους.
Εμπιστευτικότητα (C*onfidentiality)*	Η διασφάλιση της μη αποκάλυψης ή διαθεσιμότητας της πληροφορίας σε μη εξουσιοδοτημένες οντότητες**.**
Ακεραιότητα *(Integrity)*	Διασφάλιση ότι ένα ισχύον χαρακτηριστικό μιας οντότητας είναι αληθές. Αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας.
Διαθεσιμότητα (*Availability)*	Διασφάλιση της πρόσβασης και χρήσης όταν ζητηθεί από μια εξουσιοδοτημένη οντότητα Αποφυγή προσωρινής ή μόνιμης άρνησης διάθεσης της πληροφορίας ή των υπολογιστικών πόρων σε νόμιμα εξουσιοδοτημένους χρήστες.
Αυθεντικοποίηση (Authenticity)	Η εξακρίβωση της γνησιότητας μίας πληροφορίας ή της γνησιότητας της ταυτότητας ενός χρήστη ή ενός υπολογιστικού συστήματος.
Ευπάθεια-Αδυναμία (Vulnerability)	Τρωτότητα είναι η αδυναμία ενός περιουσιακού στοιχείου, η έλλειψη ελέγχων η οποία θα μπορούσε να διευκολύνει ή επιτρέψει να συμβεί μια απειλή.
Απειλή (Threat)	Η απειλή είναι η πιθανότητα για εκμετάλλευση της εσκεμμένης αδυναμίας φυσικής, τυχαίας η οποία περιλαμβάνει απώλεια περισσοτέρων του ενός των απαιτήσεων ασφαλείας της πληροφορίας δηλ. διαθεσιμότητα, ακεραιότητα, εμπιστευτικότητα.
Παραβίαση (Breach)	Ένα γεγονός το οποίο προσβάλλει μία ή περισσότερες από τις ακόλουθες ιδιότητες: αυθεντικότητα, διαθεσιμότητα, εμπιστευτικότητα, ακεραιότητα, εγκυρότητα.
Επίπτωση (Impact)	Η απώλεια μιας αξίας, η αύξηση του κόστους ή άλλη απώλεια που προκύπτει ως αποτέλεσμα μιας παραβίασης
Ανάλυση Κινδύνου	Ανάλυση κινδύνου ενός πληροφοριακού συστήματος είναι η διαδικασία αξιολόγησης των κινδύνων ασφαλείας που εισάγει το σύστημα καθώς και το κόστος.
Επικινδυνότητα-Κίνδυνος ασφαλείας	Κίνδυνος ασφαλείας ορίζεται η πιθανότητα που έχει ένα πληροφοριακό σύστημα να υποστεί εκμετάλλευση από κάθε είδους απειλές λόγω αδυναμιών που παρουσιάζει. Έχει τρεις παραμέτρους την επίπτωση, την απειλή και την αδυναμία.
Μέτρο Προστασίας-Αντίμετρο	Μέτρο (διοικητικό, οργανωτικό, τεχνικό) που εφαρμόζεται για την προστασία του πληροφοριακού συστήματος και την αντιμετώπιση των απειλών ή για να μειώσει τις δυνητικές επιπτώσεις. Τα μέτρα περιλαμβάνουν οποιαδήποτε διεργασία, πολιτική, συσκευή, πρακτική, ή άλλες ενέργειες οι οποίες τροποποιούν τον κίνδυνο.

Εναπομένων Κίνδυνος	Είναι ο συνολικός κίνδυνος μείον τους αλειφθέντες κινδύνους.
Διαχείριση κινδύνου	Η διαχείριση των στοιχείων και των προτεινόμενων μέτρων κατά τη διάρκεια κύκλου ζωής του Συστήματος.
Πολιτική Ασφαλείας	Το σύνολο των κανόνων, των μέτρων και των διαδικασιών που ορίζουν τα φυσικά, διαδικαστικά και προσωπικά μέτρα ασφαλείας, που λαμβάνονται κατά τη διαχείριση, τη διανομή και την προστασία των περιουσιακών στοιχείων.
Σχέδιο Ασφαλείας	Το έγγραφο που περιγράφει τα οργανωτικά και τεχνικά μέτρα, και τα μέτρα φυσικής ασφάλειας που εφαρμόζονται ή πρόκειται να εφαρμοστούν για την κάλυψη των βασικών αρχών και κανόνων που αναφέρονται στην πολιτική ασφαλείας . Συμπεριλαμβάνει τις απαραίτητες ενέργειες για την υλοποίηση

Πίνακας 1: Βασικές Έννοιες και ορισμοί

2. Κεφάλαιο 2^{ο} :Μεθοδολογία – Εργαλεία ανάλυσης κινδύνων.

2.1 Μεθοδολογία - Εργαλείο Consultative, Objective and Bi-Functional Risk Analysis (COBRA)

Η μεθοδολογία **COBRA [25]** αποτελεί και εργαλείο. Η χώρα προέλευσης του είναι το Ηνωμένο Βασίλειο. Η μεθοδολογία COBRA έχει αναπτυχθεί σε πλήρη συνεργασία με Οικονομικούς οργανισμούς, ιδρύματα και χρόνια έρευνας. Η πρώτη έκδοση του εργαλείου είναι το 1990 στα Αγγλικά από την εταιρεία C&A Security Systems Ltd. με σκοπό μια καλύτερη και πιο εμφανή επιστροφή των επενδύσεων τους.

Τα στάδια αξιολόγησης του κινδύνου είναι τα ακόλουθα:

• **Αναγνώριση Κινδύνου**: Καθορισμός απειλών συστήματος, ευπάθειες και ευάλωτα σημεία. Μέτρηση του βαθμού του πραγματικού κινδύνου για κάθε περιοχή ή πλευρά του συστήματος και σύνδεση με πιθανή επιχειρησιακή επίπτωση.

- Δημιουργεί τα κατάλληλα ερωτηματολόγια κινδύνου με διαφορετικές απαιτήσεις ασφαλείας προσαρμοσμένα για συγκεκριμένο οργανισμό, περιβάλλον και σύστημα υπό αξιολόγηση.
- Είναι ένα ερωτηματολόγιο βασιζόμενο σε σύστημα υπολογιστή χρησιμοποιώντας εξειδικευμένες αρχές και μια βάση δεδομένων.
- Καταγράφει τις απειλές συστημάτων, καταγράφει τον βαθμό του πραγματικού κινδύνου.
- Αξιολογεί τη σχετική σπουδαιότητα όλων των απειλών και τρωτοτήτων και δημιουργεί κατάλληλες προτάσεις και λύσεις.

• **Ανάλυση Κινδύνου:**

Υποστηρίζει την υποθετική δοκιμή. Υπάρχει δυνατότητα δυναμικής διαβεβαίωσης της επίπτωσης που έχουν συγκεκριμένοι επιπρόσθετοι έλεγχοι στο επίπεδο κινδύνου. Οι αναφορές που δημιουργεί είναι επαγγελματικές αναφορές κατάλληλες για ερμηνεία από τεχνικό προσωπικό και στελέχη. Το εργαλείο σύμβουλος κινδύνου είναι ένα ερωτηματολόγιο βασιζόμενο σε Windows PC εργαλεία που χρησιμοποιεί βάσεις δεδομένων.

• **Αξιολόγηση Κινδύνου:** Καθορισμός απειλών συστήματος, τρωτοτήτων. Παρέχει μια ολοκληρωμένη υπηρεσία ανάλυσης κινδύνων, συμβατή με τις περισσότερες αναγνωρισμένες μεθοδολογίες(ποσοτική και ποιοτική).

• **Θεραπεία Κινδύνου:** Λεπτομερής λύσεις και προτάσεις για την μείωση του κινδύνου. Προσφέρει λεπτομερής λύσεις και συστάσεις για να μειωθεί ο κίνδυνος. Παρέχει επιχειρησιακές και τεχνικές αναφορές.

• **Κοινοποίηση κινδύνου:** Παρέχει επιχειρησιακές και τεχνικές αναφορές.

Το εργαλείο COBRA είναι γενική μεθοδολογία, ανάλυσης και διαχείρισης κινδύνων. Το εργαλείο αυτό δίνει τη δυνατότητα να πραγματοποιηθεί ποιοτική ανάλυση, η αξιολόγηση των επιπτώσεων γίνεται βασιζόμενη σε κρίσιμα περιουσιακά στοιχεία, η αξιολόγηση του κινδύνου λαμβάνει υπ' όψιν την πιθανότητα, την τρωτότητα (απειλή, περιουσιακό στοιχείο) και την επίπτωση.

Οι δυνατότητες για εμπλοκή των χρηστών στη διαδικασία της αξιολόγησης είναι αρκετά υψηλή. Η δυνατότητα της μεθόδου να αναλύσει και να συνδυάσει διαφορετική συνολική γνώση είναι αρκετά καλή. Απαιτούνται βασικές γνώσεις για να πραγματοποιηθεί η υλοποίηση του εργαλείου και της μεθοδολογίας. Υπάρχει αυτοματοποιημένο εργαλείο το The SRM Toolkit.

Είναι απαραίτητη η συμμετοχή του χρήστη σε αυτήν με βασικά απαιτούμενα προσόντα. Αυτό δημιουργεί πολλά πλεονεκτήματα και διαμορφώνει κατάλληλα την ανάλυση. Η τιμή του είναι 2000Ευρώ. Η συμμόρφωση του εργαλείου αυτού είναι με το ISO7799.

2.2 Μεθοδολογία – εργαλείο Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)

Η μέθοδος ***Operationally Critical Threat, Asset and Vulnerability Evaluation*** **(Octave) [23]** αναπτύχθηκε για πρώτη φορά από το πανεπιστήμιο Carnegie Mellon από το CERT Coordination Center και είναι μια αρκετά διαδεδομένη μέθοδος ιδιαίτερα στις .Η.Π.Α.

Είναι μια δωρεάν προσέγγιση που βελτιώνει την διαδικασία λήψης αποφάσεων που αφορούν την προστασία και την διαχείριση των πόρων μιας εταιρείας. Είναι κατανοητή, συστηματική, καθοδηγούμενη από το περιβάλλον εξελισσόμενη.

Χρησιμοποιώντας αυτήν την μέθοδο, οι μικρές ομάδες ανάμεσα στις επιχειρησιακές μονάδες και στην μηχανογράφηση αντιμετωπίζουν μαζί την ανάγκη ασφαλείας του οργανισμού. Η μεθοδολογία αυτή μπορεί να προσαρμοστεί στο ιδιαίτερο επικίνδυνο περιβάλλον του οργανισμού, στους σκοπούς ασφαλείας και στο επίπεδο επιδεξιότητας. Η μεθοδολογία αυτή θέτει στον οργανισμό τον κίνδυνο και την τεχνολογία σε ένα περιβάλλον επιχείρησης.

Για μικρότερους οργανισμούς (λιγότερο από 100 άτομα) είναι υπό ανάπτυξη η μέθοδος OCTAVE-S, μια παραλλαγή της προσέγγισης , αλλά ακόμα δεν έχει ολοκληρωθεί.

Η μέθοδος OCTAVE χρησιμοποιεί μια προσέγγιση τριών φάσεων για να εξετάσει οργανωτικά και τεχνολογικά θέματα, συγκεντρώνοντας μια κατανοητή εικόνα των αναγκών για την ασφάλεια πληροφοριών του Οργανισμού.

Κάθε φάση αποτελείται από πολλές διεργασίες και κάθε διεργασία έχει μια ή περισσότερες ομάδες εργασίες καθοδηγούμενες από την ομάδα ανάλυσης. Κάποιες δραστηριότητες προετοιμασίας είναι απαραίτητες για την ομαλή ολοκλήρωση της αξιολόγησης.

Αυτές οι τρεις φάσεις είναι οι ακόλουθες:

Φάση 1: Ενσωματωμένα προφίλ απειλών με βάση τα δεδομένα. Έχει τέσσερις διεργασίες.

Διεργασία 1: Καθορισμός γνώσης διευθυντή.

Διεργασία 2: Καθορισμός γνώσεων Λειτουργικής Διαχείρισης.

Διεργασία 3: Καθορισμός γνώσεων προσωπικού.

Διεργασία 4: Δημιουργία προφίλ απειλών.

Φάση 2: Καθορισμός τρωτοτήτων υποδομής. Οι διεργασίες της φάσης 2 είναι:

Διεργασία 5: Καθορισμός βασικών στοιχείων.

Διεργασία 6 : Αξιολόγηση επιλεγμένων στοιχείων.

Φάση 3: Ανάπτυξη στρατηγικών και σχεδίων ασφαλείας. Οι διεργασίες της φάσης 3 είναι:

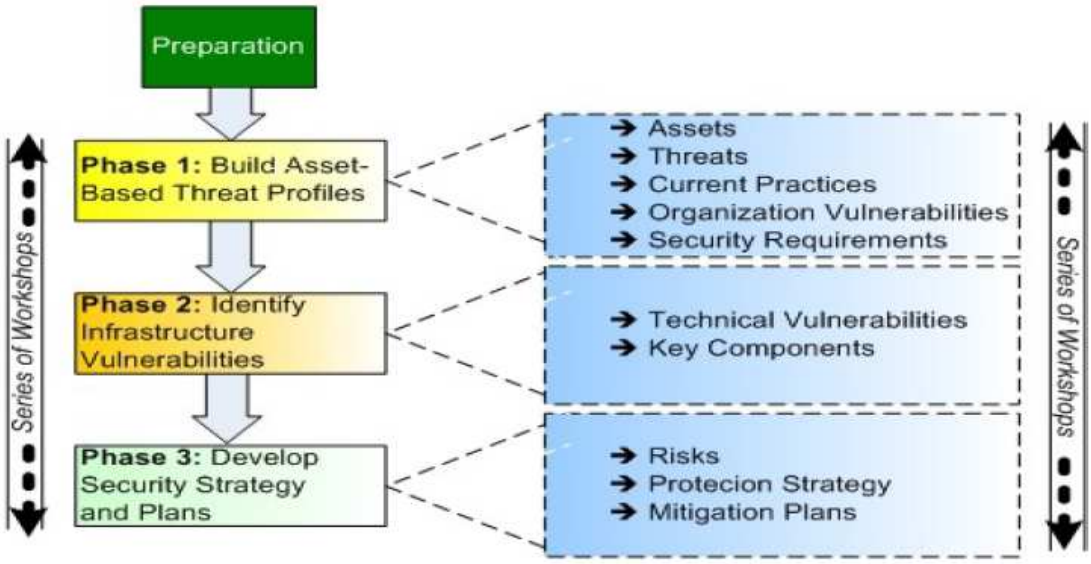
Διεργασία 7: Διεξαγωγή Ανάλυσης Κινδύνων. Πρέπει να σημειωθεί ότι η **OCTAVE** χρησιμοποιεί για την ανάλυση κινδύνων μια πρωταρχική προσέγγιση βασιζόμενη σε μια ποσοτική κλίμακα (υψηλή, μεσαία, χαμηλή). Η μεθοδολογία χρησιμοποιεί ένα πίνακα αναμενόμενης τιμής για να καθορίσει την αναμενόμενη τιμή κινδύνου.

Ο τύπος είναι:

Απώλεια = Επίπτωση/συνέπεια x Πιθανότητα.

Η μέθοδος δεν χρησιμοποιεί μαθηματικούς υπολογισμούς και συνεπώς θεωρείται απλοϊκή και χωρίς ακρίβεια. Επιπρόσθετα, η μέθοδος δεν ενσωματώνει μια προηγμένη τεχνική για την ανάλυση και τον συνδυασμό γνώσης που βρίσκεται στο συνολικό περιβάλλον. Έτσι, η πληροφορία διατρέχει μια μη επαρκή διεργασία για τον καθορισμό των συνολικών αποτελεσμάτων.

Διεργασία 8: Ανάπτυξη Στρατηγικής Προστασίας.



Εικόνα 1: Βήματα ανάλυσης κινδύνων OCTAVE

Η Octave **[9]** είναι μια γενική μεθοδολογία, δίνει τη δυνατότητα να πραγματοποιηθεί ποιοτική ανάλυση, η αξιολόγηση των επιπτώσεων γίνεται βασιζόμενη σε κρίσιμα περιουσιακά στοιχεία, η αξιολόγηση του κινδύνου λαμβάνει υπ' όψιν την πιθανότητα, την τρωτότητα (κρίσιμο περιουσιακό στοιχείο) και την επίπτωση (απειλή, περιουσιακό στοιχείο) .

Οι δυνατότητες για εμπλοκή των χρηστών στη διαδικασία της αξιολόγησης είναι μεσαία. Η δυνατότητα της μεθόδου να αναλύσει και να συνδυάσει διαφορετικά συνολικά δεδομένα φαίνεται να είναι χαμηλή. Απαιτούνται βασικές γνώσεις για να πραγματοποιηθεί η υλοποίηση του εργαλείου και της μεθοδολογίας. Υπάρχει ετήσια χρέωση για το εργαλείο OCTAVE το οποίο δεν θεωρείται εργαλείο αλλά βασίζεται σε φύλλα εργασίας.

Είναι εύκολα κατανοητή. Σε περίπτωση που το πληροφοριακό σύστημα είναι μικρό υλοποιείται ταχύτατα. Για μεγάλο Π.Σ. είναι δύσκολο να προσδιοριστεί το κρίσιμο περιουσιακό στοιχείο και να ολοκληρωθεί ο μεγάλος αριθμός φύλλων εργασίας. Επίσης δεν υπάρχει συμμόρφωση με κάποιο πρότυπο ασφαλείας.

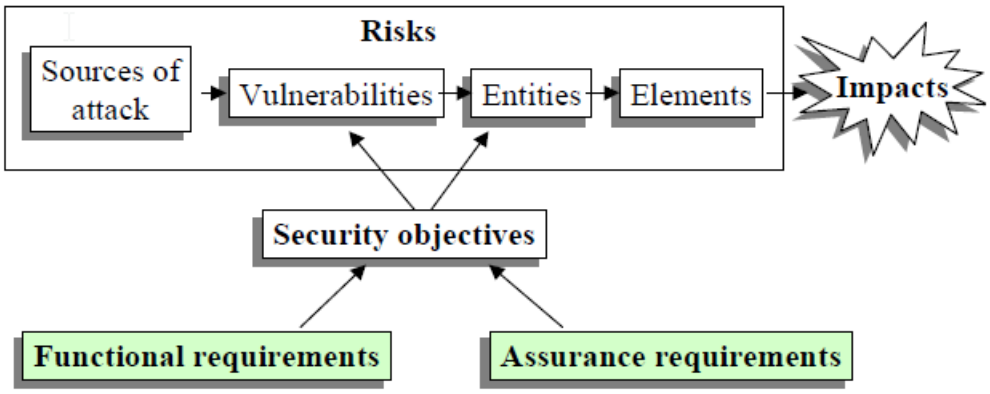
2.3 Μεθοδολογία – εργαλείο EBIOS

Η μεθοδολογία EBIOS (***Expression des Besoins et Identification des Objectifs de Sécurité*) [28]** αναπτύχθηκε από το γαλλικό κυβερνητικό οργανισμό DCSSI ***(Direction Centrale de la Sécurité des Systèmes d'Information, Premier Ministre)*** το 1995 στον οποίο συμμετέχει ένας σημαντικός αριθμός ιδιωτικών φορέων.

Έχει ως σκοπό την αξιολόγηση και διαχείριση των κινδύνων σχετιζομένων με την ασφάλεια πληροφοριών. Είναι μια εφαρμογή stand alone που βασίζεται σε τεχνολογίες java και xml.

Τα βήματα ανάλυσης και διαχείρισης κινδύνων καθορίζονται στα **5 στάδια του EBIOS**:

- **Αναγνώριση Κινδύνου:** Στο **πρώτο στάδιο** πραγματοποιεί ανάλυση του περιβάλλοντος όσον αφορά τις επιχειρησιακές απαιτήσεις με το πληροφοριακό σύστημα (συνεισφορά στο σύνολο, ακριβή καθορισμό περιμέτρου, ανάλυση σε ροή πληροφοριών και λειτουργιών).
- **Ανάλυση Κινδύνων**: Στα **στάδια 2 και 3** διεξάγονται η ανάλυση των αναγκών ασφαλείας και η ανάλυση κινδύνων. Το **EBIOS** είναι ένας συνδυασμός απειλής με τις απώλειες που μπορεί να προκαλέσει. Μειονέκτημα αποτελεί η απουσία ενός προηγμένου συστήματος υπολογισμού του κινδύνου για τον συσχετισμό και των καθορισμό των αποτελεσμάτων.
- **Διαχείριση Κινδύνων:** Στα **στάδια 4 και 5** γίνεται μια αντικειμενική διάγνωση των κινδύνων.



Εικόνα 2: Ανάλυση και διαχείριση EBIOS

Καλύπτει επαρκώς όλα τα βήματα αποτίμησης και διαχείρισης επικινδυνότητας ενώ παράλληλα παρέχει στους υπεύθυνους αναλυτές μια υψηλού επιπέδου προσέγγιση των κινδύνων βοηθώντας τους να εκτιμήσουν και να αντιμετωπίσουν τους κινδύνους.

Η μέθοδος EBIOS είναι μια γενική μεθοδολογία, δίνει τη δυνατότητα να πραγματοποιηθεί ποιοτική ανάλυση, η αξιολόγηση των επιπτώσεων γίνεται βασιζόμενη σε κρίσιμα περιουσιακά στοιχεία, η αξιολόγηση του κινδύνου λαμβάνει υπ' όψιν την πιθανότητα, την τρωτότητα (κρίσιμο περιουσιακό στοιχείο) και την επίπτωση (απειλή, περιουσιακό στοιχείο). Σε αντίθεση με προσεγγίσεις ανάλυσης κινδύνων βασιζόμενες σε σενάρια, η δομημένη προσέγγιση της μεθόδου EBIOS επιτρέπει να προσδιοριστούν τα δομικά στοιχεία του κινδύνου (οντότητες και ευπάθειες, μέθοδοι επιθέσεων και απειλές, ουσιαστικά στοιχεία και ευαισθησίες). Δεν φτάνει τόσο σε τεχνικό επίπεδο και εξαρτάται πολύ από τους χρήστες και συνεργασία που θα δείξουν.

Οι δυνατότητες για εμπλοκή των χρηστών στη διαδικασία της αξιολόγησης είναι μεσαία. Η μεθοδολογία συνδυάζει τα συνολικά δεδομένα με ένα αποτελεσματικό τρόπο βασιζόμενη σε μια ποιοτική προσέγγιση.

Το εργαλείο επιτρέπει στους χρήστες με χαμηλή εξειδίκευση και εμπειρία στην πληροφορική να αξιολογήσουν και να μειώσουν τους συνολικούς κινδύνους, περιλαμβάνει όλη την ανάλυση κινδύνων.

Η δυνατότητα της μεθόδου να αναλύσει και να συνδυάσει συνολικά τα διαφορετικά δεδομένα φαίνεται να είναι χαμηλή. Απαιτούνται βασικές γνώσεις για να πραγματοποιηθεί η υλοποίηση του εργαλείου και της μεθοδολογίας.

Είναι εύκολα κατανοητή. Η μέθοδος EBIOS μπορεί να εφαρμοστεί από ένα εύρος οργανισμών από κυβερνητικούς και μεγάλες εταιρείες σε μικρές και μεσαίες επιχειρήσεις. Τυποποιεί τις ευπάθειες και τις απειλές και καθορίζει τους συσχετιζόμενους κινδύνους για τον οργανισμό.

Η μεθοδολογία είναι εφαρμόσιμη τόσο σε μεγάλα έργα (επιχειρηματική συνέχεια, πολιτική ασφάλειας κ.α.) καθώς και σε μικρότερης εμβέλειας έργα (δίκτυα ιστοσελίδας, σύστημα ηλεκτρονικών μηνυμάτων κ.α.), καθώς παρέχεται μια σφαιρική θεώρηση για την λήψη αποφάσεων από τα ανώτερα διευθυντικά στελέχη. Είναι γρήγορη και επαναχρησιμοποιήσιμη.

Το εργαλείο που την υλοποιεί διατίθεται δωρεάν ενώ θα πρέπει να λάβουμε υπόψη μας ότι υλοποιείται με το εργαλείο αυτό και με ανοιχτό OpenEBIOS..

Υλοποιεί παρόλα αυτά, μια σειρά προτύπων όπως τα ISO/IEC IS 17799 ή ISO/IEC IS 27001: 2005, ISO/IEC 27002:2005, ISO14508, ISO/IEC 27005:2008, 15408, ISO/IEC IS 13335 και ISO/IEC IS 21827.

2.4 Μεθοδολογία – εργαλείο Callio Secura 17799

Το Callio Secura 17799 **[24]** είναι ένα προϊόν της Callie Technologies, δημιουργήθηκε στον Καναδά το 2001 και πλέον βρίσκεται στην δεύτερη έκδοση του που πραγματοποιήθηκε το 2005. Είναι ένα web-based εργαλείο με υποστήριξη βάσης δεδομένων, που επιτρέπει στο χρήστη να εφαρμόσει και να πιστοποιήσει ένα σύστημα διαχείρισης ασφάλειας πληροφοριών(ISMS). Περιλαμβάνει 3 φάσεις :

2.4.1 Αξιολόγηση Κινδύνου

α. Αναγνώριση Κινδύνου

Το πρόγραμμα δημιουργεί ένα web site στο οποίο μπορούν να έχουν πρόσβαση από παντού όσοι συμμετέχουν στην ανάλυση κινδύνων. Το πρόγραμμα διατηρεί βάση δεδομένων στον server με πλήρη δυνατότητα δικαιωμάτων και ομάδων χρηστών έτσι ώστε ο κάθε χρήστης να βλέπει ή να αλλάζει μόνο τα αρχεία εκείνα που τον αφορούν.

β. Ανάλυση Κινδύνου Είναι ένα πλήρες μοντέλο για να αξιολογηθεί ο παράγοντας έκθεσης exposure factor ενός κινδύνου, αλλά δεν υπολογίζει την επιχειρησιακή επίπτωση του κινδύνου. Δεν υποστηρίζει την ανάλυση κινδύνου αλλά μόνο την αξιολόγηση του κινδύνου.

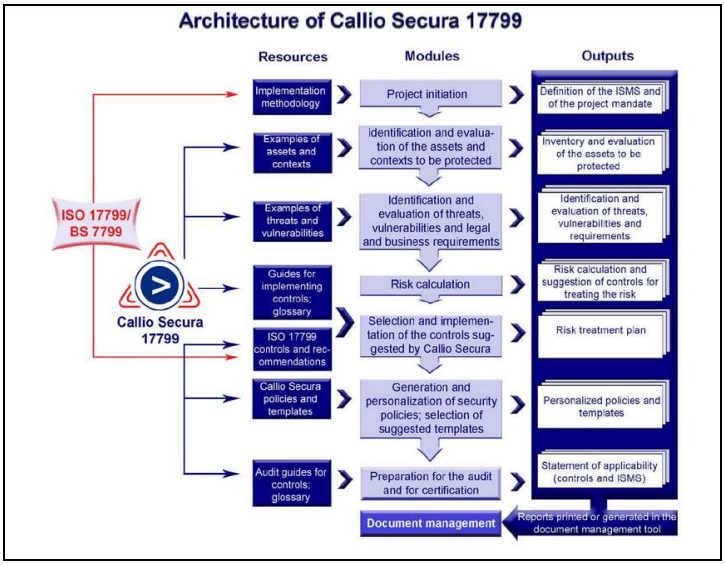
2.4.2. Διαχείριση Κινδύνου

Δημιουργεί πολιτικές ασφαλείας, αναφορές, υλοποιεί διαχείριση εγγράφων.

2.4.3. Κοινοποίηση Κινδύνου

Πραγματοποιεί διαχείριση αναφορών, έχει κέντρο ενημερωτικής πύλης.

Παρακάτω δίνεται ένα διάγραμμα που δείχνει τα εργαλεία που προσφέρει το Callio Secura 17799 για κάθε βήμα της ανάλυσης κινδύνων (και γενικότερα της διαχείρισης της ασφάλειας).



Εικόνα 3:Ανάλυση κινδύνωνCallioSecura

Η μέθοδος **Callio Secura 17799** είναι μια γενική μεθοδολογία, δίνει τη δυνατότητα να πραγματοποιηθεί ποιοτική ανάλυση, η αξιολόγηση των επιπτώσεων γίνεται βασιζόμενη σε κρίσιμα περιουσιακά στοιχεία, η αξιολόγηση του κινδύνου λαμβάνει υπ' όψιν την πιθανότητα, την τρωτότητα (κρίσιμο περιουσιακό στοιχείο) και την επίπτωση (απειλή, περιουσιακό στοιχείο).

Οι δυνατότητες για εμπλοκή των χρηστών στη διαδικασία της αξιολόγησης είναι μεσαίες. Η δυνατότητα της μεθόδου να αναλύσει και να συνδυάσει διαφορετικά συνολικά δεδομένα φαίνεται να είναι χαμηλή.

Απαιτούνται βασικές γνώσεις για να πραγματοποιηθεί η υλοποίηση του εργαλείου και της μεθοδολογίας. Η διεπαφή του προγράμματος είναι πολύ εύκολη και χρηστική και δεν χρειάζεται ειδική εκπαίδευση για την χρησιμοποίηση του.

Χρησιμοποιείται επίσης για την ενημέρωση και εκπαίδευση του προσωπικού για τα θέματα ασφαλείας, τις υπάρχουσες πολιτικές ασφαλείας, τις διαδικασίες κτλ. Η μεθοδολογία είναι εφαρμόσιμη σε μικρές εφαρμογές αλλά και για μεσαία δίκτυα. Υποστηρίζει πρότυπα όπως το ISO17799 και ISO 27001 (BS 7799-2) και παράγει τα έγγραφα που απαιτούνται για την πιστοποίηση.

2.5 Μεθοδολογία- εργαλείο Control Compliance Suite (CCS) 11 Risk Manager, CCS

Η CCS Risk Manager **[29]** δημιουργήθηκε στις Η.Π.Α από την εταιρεία **Symantec Corporation**, η μέθοδος επιτρέπει στους υπεύθυνους της ασφάλειας την καλύτερη κατανόηση των κινδύνων.

Υποστηρίζει τρεις φάσεις:

2.5.1 Αξιολόγηση Κινδύνου

α. Αναγνώριση κινδύνου : Χρησιμοποιώντας τεχνικά πρότυπα και προδιαγραφές (π.χ. ISO 27001, 27002).

β. Ανάλυση κινδύνου : Η CCS Risk Manager παρέχει ισχυρά εργαλεία που επιτρέπουν στους οργανισμούς τη μέτρηση, τον μετριασμό και την αποκατάσταση των κινδύνων των πληροφοριακών συστημάτων τους καθώς και την κοινοποίηση των κινδύνων αυτών. Επίσης παρέχει υποστήριξη σε όλους τους τομείς της επιχείρησης και σε όλα τα επίπεδα για την βέλτιστη λειτουργία του Π.Σ τους. Χρησιμοποιεί μια προσέγγιση βασισμένη στον κίνδυνο, όπου οι διαχειριστές χρησιμοποιούν τον Διαχειριστή κινδύνου να καθορίσει ένα περιουσιακό στοιχείο και κατόπιν απεικονίζουν τον κίνδυνο. Αυτό ελέγχει και τεκμηριώνει τα περιουσιακά στοιχεία για να δώσει πληροφορία για ενέργεια για τη μείωση του κινδύνου.

γ. Αξιολόγηση Κινδύνου : Συνδυάζει όλα αυτά με συμπληρωματικά δεδομένα από τη Symantec ή και μη Symantec λύσεις, παρέχοντας ένα πλούσιο σύνολο διαθέσιμων πληροφοριών για την καλύτερη ανάλυση και τη λήψη αποφάσεων. Το αποτέλεσμα είναι μια πραγματικά πολυδιάστατη άποψη των κινδύνων που συνδέονται με οποιαδήποτε επιχειρηματική διαδικασία, ομάδα ή λειτουργία. Το στοιχείο Risk Manager είναι σχεδιασμένο να βοηθήσει τους Διευθυντές να καθορίσουν το επίπεδο του κινδύνου που παρουσιάζονται από τις υποδομές πληροφοριακών συστημάτων.

2.5.2. Διαχείριση Κινδύνου:

Οι διαχειριστές δημιουργούν τις δικές τους πολιτικές χρησιμοποιώντας πρότυπα και τροποποιώντας αυτές τις πολιτικές για να καλύψουν τις συγκεκριμένες ανάγκες. Αυτές συνδέονται με τα κατάλληλα μέτρα

.2.5.3. Κοινοποίηση Κινδύνου:

Μέσω dashboards για συγκεκριμένα ακροατήρια όπως επίσης έχει συγκεκριμένες μορφές αναφορών και δυνατότητες εξαγωγής δεδομένων.

Εικόνα 4: Dashboards CCS Risk Manager

Η μέθοδος CCS Risk Manager είναι μια σπονδυλωτή λύση, αποτελούμενη από πέντε βασικά στοιχεία. Έχει δυνατότητες που περιλαμβάνουν λογισμικό για την ανάλυση μεγάλων όγκων δεδομένων, τροποποιημένους πίνακες και αναφορές web-based. Επίσης, χρησιμοποιείται για να εκτελεί end –to-end αξιολόγηση τρωτοτήτων σε εφαρμογές Web, βάσεων δεδομένων, εξυπηρετητών, και δικτυακών συσκευών καταγράφοντας τις απειλές ασφαλείας.

Οι δυνατότητες για εμπλοκή των χρηστών στη διαδικασία της αξιολόγησης είναι μεσαία. Η δυνατότητα της μεθόδου να αναλύσει και να συνδυάσει διαφορετικά συνολικά δεδομένα φαίνεται να είναι μεσαία. Απαιτούνται βασικές γνώσεις για να πραγματοποιηθεί η υλοποίηση του εργαλείου και της μεθοδολογίας.

Η **μέθοδος CCS Risk Manager συμμορφώνεται με τα IT πρότυπα :**

- TIER IV SCAP 1.2

- Open Vulnerability and Assessment Language (OVALR) 5.10.1, Common Configuration Enumeration (CCE.) 5, Common Platform Enumeration (CPE.) 2.3, Common Vulnerabilities and Exposures (CVER), Common Vulnerability Scoring System (CVSS) 2.0, Asset Identification 1.1, Asset Reporting Format (ARF) 1.1

- ISO 27001-2013, NIST Cyber security Framework in SCU 2014-1, and PCI DSS v3.0 in SCU 2014-1.

2.6 Μεθοδολογία – εργαλείο CloudeAssurance

Η μέθοδος CloudeAssurance **[30]** δημιουργήθηκε στις Ηνωμένες Πολιτείες από την εταιρεία eFortresses, Inc, τον Μάρτιο του 2012 ενώ αυτή την στιγμή βρίσκεται στην έκδοση 1.3 η οποία πραγματοποιήθηκε το 2014. Είναι μια μέθοδος αξιολόγησης ασφάλειας βασισμένη σε «σύννεφο», που δίνει την δυνατότητα για αξιολόγηση, τάσεις, συγκριτική αξιολόγηση ή συνεχή παρακολούθηση καθώς αποτελεί και εκπαιδευτική πλατφόρμα.

2.6.1 Αξιολόγηση Κινδύνου:

α. Αναγνώριση κινδύνου : Χρησιμοποιώντας τεχνικά πρότυπα και προδιαγραφές η μέθοδος Cloud eAssurance (αλγόριθμος συστήματος rating) προστατεύει τους πελάτες μετρώντας και διασφαλίζοντας την ικανότητα των παρόχων υπηρεσιών cloud να παραδώσουν ασφαλώς υπηρεσίες cloud σύμφωνα με τις καλές πρακτικές, τα πρότυπα και την συμμόρφωση των κανονισμών της βιομηχανίας για cloud.

β. Ανάλυση κινδύνου : Η Cloud eAssurance παρέχει ισχυρά εργαλεία που επιτρέπουν στους οργανισμούς τη μέτρηση, την ετοιμότητα, τις τάσεις(trending) και τις αναφορές benchmark. Επίσης παρέχει μια ολιστική προσέγγιση για διασφάλιση υποστηρίζοντας παραπάνω από 20 εθνικά και παγκόσμια αποδεκτά πρότυπα και κινδύνους, απειλές και βαθμολογίες ωριμότητας που επιτρέπουν στις επιχειρήσεις να μετρήσουν αποτελεσματικά, να παρακολουθήσουν τους κινδύνους εταιριών πέρα από την συνήθη προσέγγιση συμμόρφωσης.

γ. Αξιολόγηση Κινδύνου : Συνδυάζει όλα αυτά, τις συστάσεις, την βάση δεδομένων και τις βιβλιοθήκες και το αποτέλεσμα είναι μια πραγματικά πολυδιάστατη άποψη των κινδύνων που συνδέονται με οποιαδήποτε επιχειρηματική διαδικασία, ομάδα ή λειτουργία.

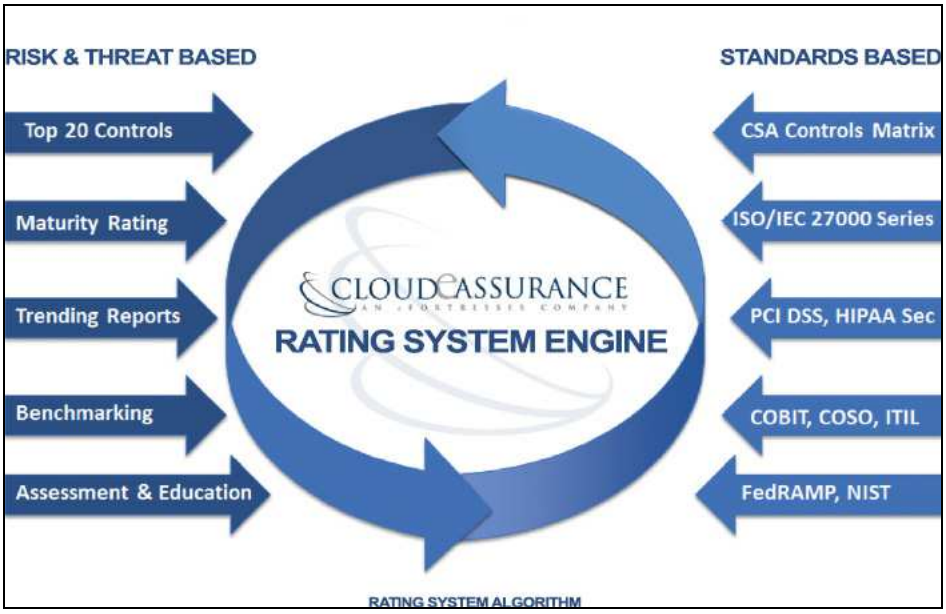
2.6.2. Διαχείριση Κινδύνου:

Υποστηρίζει τις φάσεις εκτίμησης κινδύνου, θεραπείας κινδύνου, αποδοχής κινδύνου.

2.6.3. Κοινοποίηση Κινδύνου:

Η μέθοδος Cloud eAssurance είναι η πρώτη αξιολόγηση βαθμολογίας κινδύνου, συνεχούς λήψης στοιχείων με συνεχές σύστημα παρακολούθησης, διασφαλίζοντας την ασφάλεια , του κινδύνου και τη συμμόρφωση.

Παρέχει αλυσίδα διαχείρισης κινδύνων εταιριών και αλυσίδας υποστήριξης: Διαδικασία 3 βημάτων που οδηγεί σε βαθμολογία αξιολόγησης διασφάλισης Cloud.



Εικόνα 5: Cloud Assurance

Η μέθοδος Cloud eAssurance **[29]** είναι μια γενική μεθοδολογία, δίνει τη δυνατότητα να πραγματοποιηθεί ποιοτική ανάλυση, η αξιολόγηση των επιπτώσεων γίνεται βασιζόμενη σε κρίσιμα περιουσιακά στοιχεία, η αξιολόγηση του κινδύνου λαμβάνει υπ' όψιν την πιθανότητα, την τρωτότητα (κρίσιμο περιουσιακό στοιχείο) και την επίπτωση (απειλή, περιουσιακό στοιχείο).

Οι δυνατότητες για εμπλοκή των χρηστών στη διαδικασία της αξιολόγησης είναι μεσαία. Η δυνατότητα της μεθόδου να αναλύσει και να συνδυάσει διαφορετική συνολική γνώση φαίνεται να είναι μεσαία. Απαιτούνται ειδικές γνώσεις για να πραγματοποιηθεί η υλοποίηση του εργαλείου και της μεθοδολογίας.

Είναι εύκολα κατανοητή. Οι πελάτες μπορούν να γνωρίζουν ποιοι από τους παρόχους Cloud έχουν την πιο υψηλή βαθμολογία Cloud και να έχουν μια μέτρηση εμπιστοσύνης Cloud στην οποία μπορούν να βασίζονται.

Η μέθοδος Cloud eAssurance συμμορφώνεται με τα IT πρότυπα :

- 2011 CSA GRC Stack and HISPI CAAP Top 20 Controls - CSA CCM 1.2 and CAIQ 1.1
- 2012 HISPI CAAP Top 20 ISO/IEC 27001:2005 Annex A Controls and EU Safe Harbor - May 2013 Matrix
- FedRAMP Baseline Controls - September 2013 Matrix
- ISO/IEC 21827:2008 Process Areas and Base Practices Controls - July 2013 Matrix
- ISO/IEC 27001:2005 Annex A Controls HISPI CAAP Top 20 Controls and EU Safe Harbor - May 2013 Matrix

- ISO/IEC 27001:2005 ISMS HISPI CAAP Top 20 Controls - September 2012 Matrix
- ISO/IEC 27001:2005 ISMS including Annex A Controls HISPI CAAP Top 20 Controls and EU Safe Harbor - May 2013 Matrix
- ISO/IEC 27001:2005 ISMS including Annex A Controls HISPI CAAP Top 20 Controls Cybersecurity Framework 1st Draft and EU Safe Harbor - September 2013 Matrix
- ISO/IEC 27001:2013 ISMS including Annex A Controls HISPI CAAP Top 20 Controls -January 2014
- NIST Cybersecurity Framework 1st Draft HISPI CAAP Top 20 - September 2013
- NIST Cybersecurity Framework 2nd Draft HISPI CAAP Top 20 Controls - December 2013 Matrix
- NIST SP 800-53r3
- NIST SP 800-53r4
- NIST SP 800-53r4 - and PM Controls
- PCI DSS 2.0 HISPI CAAP Top 20 Controls - May 2013 Matrix
- PCI DSS 3.0 HISPI CAAP Top 20 Controls - December 2013 Matrix

2.7 Μεθοδολογία Magerit - εργαλείο EAR/PILAR

Η Magerit **[27]** μια μεθοδολογία που δημιουργήθηκε και αναπτύχθηκε από το Ισπανικό Υπουργείο Δημόσιας Διοίκησης και η οποία διατίθεται ανοιχτά στα Ισπανικά και τα Αγγλικά. Η πρώτη εκδοχή (version) της μεθόδου v.1 δημοσιεύτηκε το 1997, ενώ η δεύτερη εκδοχή ήρθε αρκετά χρόνια αργότερα το 2005.

2.7.1 Αξιολόγηση Κινδύνου:

α. Αναγνώριση κινδύνου : Η διαδικασία θα πρέπει να χωριστεί να περιλαμβάνει προπαρασκευαστική φάση(1-2ΠΜ), την ομάδα εργασίας των μετόχων(1) και την φάση της σύνθεσης (0.5 PM).

Πραγματοποιεί αναγνώριση περιουσιακών στοιχείων, σχέσεις μεταξύ τους, αποτίμηση για τον οργανισμό, αναγνώριση απειλών και εκτίμηση κινδύνων. Η γνώση που εισάγεται προέρχεται από γνώση του περιβάλλοντος του συστήματος, από αναφορές από παρόμοιες αποφάσεις, από στατιστικά όπου είναι εφαρμόσιμα. Η διαθεσιμότητα των δεδομένων φαίνεται καλύτερα με την αναπαράσταση σε ποσοτική πληροφορία.

Οι δυσκολίες στην συλλογή των δεδομένων προέρχονται από σπάνια γεγονότα και από τα μεμονωμένα συστήματα που έχουν δημιουργηθεί και δεν λαμβάνονται υπ' όψιν στη βάση για την λήψη αποφάσεων.

Η εισαγωγή των δεδομένων για την ποιοτική ανάλυση είναι ο καθορισμός των σεναρίων και για την ποσοτική είναι οι κλίμακες κατηγοριών, το κόστος των δεδομένων. Έχει τη δυνατότητα να μετατρέψει τα ποσοτικά δεδομένα, να υιοθετηθούν ή να αναπαρασταθούν σε ποιοτικά δεδομένα χρησιμοποιώντας κατά προσέγγιση κλίμακες. Τα στοιχεία που λαμβάνει υπ' όψιν για την αποτίμηση είναι η Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα, Αυθεντικότητα και καταλογισμός ευθυνών.

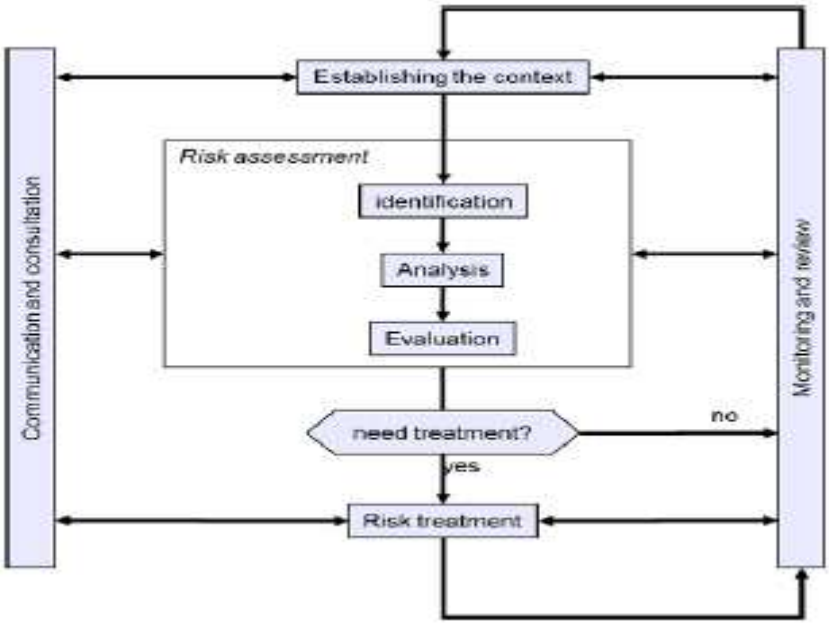
β. Ανάλυση κινδύνου : Υπολογίζει την επίπτωση και τον κίνδυνο. Πιθανές και εναπομείναντες αξίες. Ποσοτικά και ποιοτικά, συγκεντρωτικά (accumulated) και αντανακλώμενα (deflected). Πραγματοποιεί **βασική ανάλυση κινδύνου**. Ο ορισμός του κινδύνου βασίζεται σε τρεις παραμέτρους όπου η μια είναι το σενάριο της απειλής, η δεύτερη είναι η πιθανότητα, και η τρίτη η συνέπεια (πολυδιάστατη, τυπικά μετρήσιμη χρησιμοποιώντας κλίμακες κατηγοριών). Η πιθανότητα είναι σχετική με μια περίοδο αξιολόγησης που είναι τυπικά ο χρόνος που διαρκούν οι επενδύσεις ~ 40 χρόνια). Η μεθοδολογία δέχεται ποιοτικά και ποσοτικά δεδομένα. Παρέχει ένα Παράρτημα περιλαμβάνοντας πιθανούς τύπους ζημίας επεκτάσιμο για τις ανάγκες του χρήστη. Η πιθανότητα συμβάντων περιλαμβάνεται ως στοιχείο που περιγράφει τους κινδύνους. Οι διαστάσεις των συνεπειών συνήθως δεν γίνονται ως σύνολο.

γ. Αξιολόγηση Κινδύνου : Θέτει προτεραιότητες στα αποτελέσματα και αυτά παρουσιάζονται στους διευθυντές για επιχειρησιακή αξιολόγηση. Η βασική μέθοδος ανάλυσης κινδύνων υποστηρίζεται από δημιουργία σεναρίων (στην πράξη «βασιζόμενα στα γεγονότα») και η εκτίμηση των συνεπειών και των πιθανοτήτων(συχνότητες) που σχετίζονται με σενάρια. Οι κλίμακες συνεπειών είναι συνήθως κλιμακούμενες ανά κατηγορίες. Η μέτρηση κινδύνου παρέχει μια διαβάθμιση με σειρά των εναλλακτικών λύσεων.

δ. Αποθήκευση Περιουσιακών στοιχείων και αποτίμηση : Ποιοτική και ποσοτική.

ε. Ανάλυση Επιχειρησιακής Επίπτωσης : Αποτιμάται το κόστος της Υπηρεσίας. Δίνει δεδομένα για την ανάπτυξη των σχεδίων ανάκτησης από καταστροφές.

2.7.2. Διαχείριση Κινδύνου:



Εκόνα 6: Ανάλυση Κινδύνων Magerit

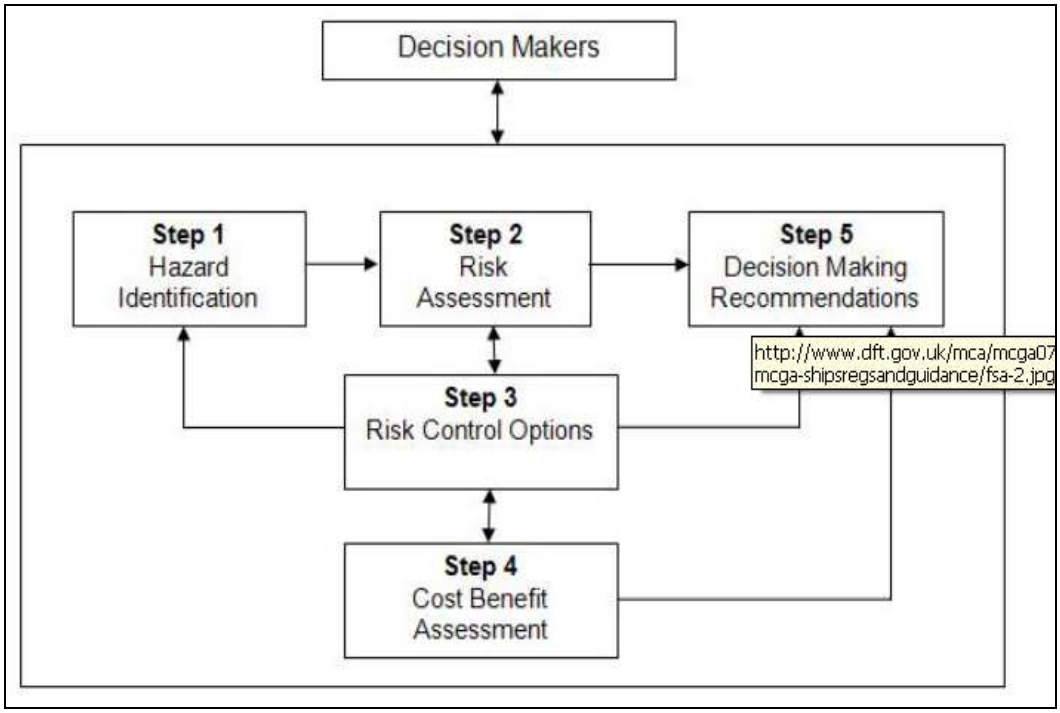
2.7.2.1 Αξιολόγηση κινδύνου: Αναγνώριση, ανάλυση και αξιολόγηση. Εναλλακτικές λύσεις προτείνονται σύμφωνα με το ποσό της μείωσης που έχει επιτευχθεί (ή εναπομείναν κίνδυνος). Ο κίνδυνος καθορίζεται ως μια λειτουργία πιθανών ποσών απώλειας και είναι συσχετιζόμενος με πιθανές απώλειες με συγκεκριμένες πιθανότητες. Οι απώλειες μετρούνται συνήθως με διαφορετικές μονάδες.

2.7.2.2 Θεραπεία Κινδύνου: Χρησιμοποιεί πολιτικές με δυνατότητα προσθήκης και άλλων ειδικών συμφωνιών του οργανισμού. Επίσης, διαθέτει διαδικασίες για εκτίμηση ωριμότητας εφαρμογής μέτρων.

2.7.2.3 Αποδοχή κινδύνου: Αποτυπώνει την εναπομείνασα επίπτωση και κίνδυνο. Συγκεντρωτικές αποτιμήσεις σε τεχνικά περιουσιακά στοιχεία και ανακλώμενης (deflected) αξίας σε επιχειρησιακές διεργασίες.

2.7.2.4 Κοινοποίηση Κινδύνου: Προσφέρει επίσης πολλές αναφορές. Αναλυτικές εκθέσεις και γραφικές αναφορές, δυνατότητα εξαγωγής σε άλλες ενότητες.

Η έξοδος της ανάλυσης κινδύνων, δίνει μοντέλο τιμών, τις εξαρτήσεις ανάμεσα σε διαφορετικά στοιχεία και το ποσό των απειλών στις οποίες εκτίθενται τα στοιχεία. Αξιολόγηση της αποτελεσματικότητας των υφιστάμενων μέτρων. Ταξινόμηση των μέτρων για τον κίνδυνο. Σχέδιο Ασφαλείας - Σύνολο προγραμμάτων ασφαλείας που θέτουν σε εφαρμογή τις αποφάσεις για την διαχείριση κινδύνων.



Εικόνα 7: Βήματα λήψης αποφάσεων

Η μέθοδος **Magerit** είναι μια γενική μεθοδολογία που δίνει τη δυνατότητα να πραγματοποιηθεί ποιοτική και ποσοτική ανάλυση. Η αξιολόγηση των επιπτώσεων γίνεται βασιζόμενη σε κρίσιμα περιουσιακά στοιχεία, η αξιολόγηση του κινδύνου λαμβάνει υπ' όψιν την πιθανότητα, την τρωτότητα (κρίσιμο περιουσιακό στοιχείο) και την επίπτωση (απειλή, περιουσιακό στοιχείο).

Οι δυνατότητες για εμπλοκή των χρηστών στη διαδικασία της αξιολόγησης είναι χαμηλή. Η δυνατότητα της μεθόδου να αναλύσει και να συνδυάσει διαφορετικά συνολικά δεδομένα φαίνεται να είναι μεσαία. Πραγματοποιεί σύνθεση των σεναρίων. Η μέθοδος έχει μεσαία πολυπλοκότητα και απαιτεί καλή προπαρασκευαστική εργασία για την ελαχιστοποίηση παρερμηνεύσεων από τους μετόχους.

Απαιτούνται ειδικές γνώσεις για να πραγματοποιηθεί η υλοποίηση του εργαλείου και της μεθοδολογίας.

- Η μεθοδολογία εφαρμόζεται ως τυπική διαδικασία από την ακαδημαϊκή κοινότητα, και η εφαρμογή γίνεται σε προβλήματα πολύπλοκων αποφάσεων όπου ο κίνδυνος είναι ένα επαρκές μέτρο για να διακριθεί η απόδοση των εναλλακτικών λύσεων. Μπορεί να χρησιμοποιηθεί σε πολλές διαφορετικές περιπτώσεις και υλοποιείται εύκολα με εργαλεία λογισμικού.
- Η μεθοδολογία αυτή βρίσκει εφαρμογή σε συστήματα πληροφορικής, τηλεματικής των μέσων ενημέρωσης και γενικότερα στην χρήση ηλεκτρονικών που παρουσιάζουν πολλούς κινδύνους και χρήζουν προστασίας μέσα από τα κατάλληλα αντίμετρα.
- Μέσω της **Magerit** μπορούμε πλέον να ποσοτικοποιήσουμε υπηρεσίες και πληροφορίες που μπορεί να βρίσκονται σε κίνδυνο ορίζοντας τους κάποιες τιμές.

Υποστηρίζεται από εργαλεία όπως RIGER, Pilar και όλη την οικογένεια των εργαλείων EAR και έχει ένα κόστος 2500 Ευρώ.

Είναι συμβατό με τα ακόλουθα πρότυπα: ISO/IEC 13335:2004, ISO/IEC 17799:2005, ISO/IEC 15408:2005, ISO/IEC 27001:2005. Επίσης, οι διαχειριστές δημιουργούν τις δικές τους πολιτικές χρησιμοποιώντας πρότυπα και τροποποιώντας αυτές τις πολιτικές για να καλύψουν τις συγκεκριμένες ανάγκες. Αυτές συνδέονται με τα κατάλληλα μέτρα.

2.8 CRAMM

Το CRAMM **[26]** είναι ένα εργαλείο ποιοτικής και ποσοτικής ανάλυσης κινδύνων που αναπτύχθηκε από το CCTA (Central Computer and Telecommunications Agency) της βρετανικής κυβέρνησης το 1985 ώστε να εφοδιάσει τα διάφορα τμήματα της κυβέρνησης με μια κοινή μέθοδο ανάλυσης κινδύνων πληροφοριακών συστημάτων. Το πρόγραμμα, το οποίο έχει υποστεί σημαντικές αναθεωρήσεις και βρίσκεται σήμερα στην έκδοση 5, δεν υποστηρίζεται πλέον από την εμπορική εταιρία Insight Consulting που έχει έδρα στην Αγγλία.

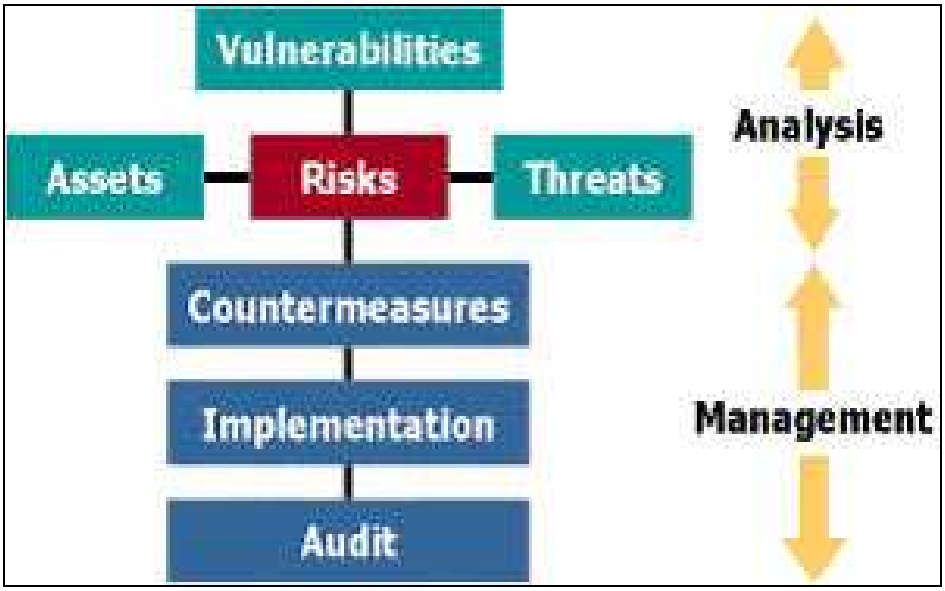
- Η μεθοδολογία CRAMM έχει τρεις κυρίως φάσεις:

2.8.1. Καθορισμός και αξιολόγηση περιουσιακών στοιχείων.- Κατόπιν καθορισμού των αντικειμενικών σκοπών όσο και των ορίων, τα φυσικά και τα περιουσιακά στοιχεία του οργανισμού καθορίζονται και αξιολογούνται μέσω συνεντεύξεων. Στηρίζεται σε ένα πολύ απλοϊκό μοντέλο του πληροφοριακού συστήματος. Εστιάζει ουσιαστικά μόνο στα δεδομένα και λαμβάνει υπόψη τους ανθρώπους μόνο ως πηγές απειλών.

2.8.2. Αξιολόγηση απειλών και τρωτοτήτων- Αυτό περιλαμβάνει την αναγνώριση και ανάλυση πιθανών απειλών στο σύστημα, αξιολογώντας την τρωτότητα των συστημάτων και τελικά χρησιμοποιώντας τες για τον υπολογισμό των κινδύνων.

2.8.3 Επιλογή μέτρων ασφαλείας και συστάσεις. Τεράστια βάση αντιμέτρων (3000 αντίμετρα) που καλύπτει όλες τις πτυχές της ασφάλειας πληροφοριακών συστημάτων. Εργαλεία για την δημιουργία σχεδίων επιχειρησιακής συνέχειας. Παρέχει οδηγούς για την δημιουργία πολιτικών ασφαλείας.

Οδηγούς για την δημιουργία αναφορών με δυνατότητες χάραξης πινάκων και γραφημάτων και εξαγωγής σε διάφορες μορφές αρχείων.



Εικόνα 8:Ανάλυση Κινδύνων CRAMM

Η μέθοδος είναι μια γενική μεθοδολογία, δίνει τη δυνατότητα να πραγματοποιηθεί ποιοτική ανάλυση, η αξιολόγηση των επιπτώσεων γίνεται βασιζόμενη σε κρίσιμα περιουσιακά στοιχεία, η αξιολόγηση του κινδύνου λαμβάνει υπ' όψιν την πιθανότητα, την τρωτότητα (κρίσιμο περιουσιακό στοιχείο) και την επίπτωση (απειλή, περιουσιακό στοιχείο).

Δυνατότητα προσαρμογής του προγράμματος στις ανάγκες του κάθε οργανισμού (σε συνεννόηση με την εταιρία).

Οι δυνατότητες για εμπλοκή των χρηστών στη διαδικασία της αξιολόγησης είναι μέτρια. Η CRAMM στηρίζεται σε μεγάλο βαθμό στη συνεργασία με τους χρήστες και τη διοίκηση του οργανισμού και τις δικές τους (υποκειμενικές απόψεις).

Η δυνατότητα της μεθόδου να αναλύσει και να συνδυάσει διαφορετικά συνολικά δεδομένα φαίνεται να είναι χαμηλή.

Τέλος, υπάρχει και η έκδοση CRAMM Express η οποία δεν περιλαμβάνει όλα τα εργαλεία σαν την κανονική έκδοση αλλά είναι πιο απλή στην χρήση και οδηγεί σε πιο γρήγορα αλλά λιγότερο αναλυτικά αποτελέσματα.

Απαιτούνται ειδικές γνώσεις για να πραγματοποιηθεί η υλοποίηση του εργαλείου και της μεθοδολογίας. Η χρήση του δεν είναι τόσο απλή, με αποτέλεσμα να απαιτείται εκπαίδευση και εξοικείωση για να επιτευχθούν τα βέλτιστα αποτελέσματα. Έχει υψηλό κόστος εφαρμογής (χρόνος και ανθρώπινη προσπάθεια). Το CRAMM έχει μεγάλο κύρος, καθώς χρησιμοποιείται σε παραπάνω από 500 οργανισμούς σε 23 χώρες, συμπεριλαμβανομένου και του ΝΑΤΟ.

Το πρόγραμμα ακολουθεί την δική του μέθοδο, η οποία αποτιμά και βοηθάει τους οργανισμούς να επιτύχουν συμμόρφωση με το διεθνές πρότυπο ISO17799/BS7799.

Η ανανέωση του εργαλείου έχει παύσει από το 2008.

2.9 Συμπεράσματα- Σύγκριση των εργαλείων Μειονεκτήματα-Πλεονεκτήματα

Τα κριτήρια που χρησιμοποιούνται **[5], [8], [10], [11]** για τη σύγκριση των οκτώ μεθοδολογιών είναι τα ακόλουθα.

Κ1: Μέθοδος ή Εργαλείο

Κ2: Εμβέλεια χρήσης: Γενική Μεθοδολογία (ΓΜ) ή Στοχευόμενη

Κ3: Υποστήριξη Ανάλυσης Κινδύνων (ΑΚ)/ Διαχείρισης Κινδύνων (ΔΚ)

Κ4: Κλίμακα αξιολόγησης: Ποσοτική ή Ποιοτική

Κ5: Αξιολόγηση επιπτώσεων: Κάθε προσέγγιση που υιοθετείται στις μεθόδους για να καθορίσει το επίπεδο επίπτωσης. Κάθε μέθοδος υιοθετεί διαφορετικά σενάρια, παράγοντες επιρροής, παραμέτρους, και οδηγίες χρήσης για να καθορίσει την επίπτωση του γεγονότος.

Κ6: Αξιολόγηση κινδύνου: Η προσέγγιση που χρησιμοποιείται από τα διάφορα προϊόντα είναι των ακόλουθων τύπων:

Τύπος 1 = Κίνδυνος(Απειλή, Περιουσιακό Στοιχείο) = Πιθανότητα(Απειλή) x Τρωτότητα(Απειλή, Περιουσιακό Στοιχείο)χ Επίπτωση(Απειλή, Περιουσιακό Στοιχείο)

Τύπος 2 = Κίνδυνος(Απειλή, Περιουσιακό Στοιχείο, Ανάγκες) = Πιθανότητα(Απειλή, Ανάγκες) x Τρωτότητα(Απειλή, Περιουσιακό Στοιχείο)

Τύπος 3 = Κίνδυνος(Απειλή, Περιουσιακό Στοιχείο) = Ετήσια Αναμενόμενη Απώλεια (Απειλή, Περιουσιακό Στοιχείο) = Πιθανότητα(Απειλή, Περιουσιακά Στοιχεία) x Μέση Απώλεια(Απειλή, Περιουσιακό Στοιχείο)

Τύπος 4 = Κίνδυνος(Απειλή, Περιουσιακό Στοιχείο) = Επίπτωση (Απειλή, Περιουσιακό Στοιχείο) x Τρωτότητα (Κρίσιμο Περιουσιακό Στοιχείο)

Τύπος 5 = Κίνδυνος(Απειλή, Περιουσιακό Στοιχείο) = Πιθανότητα(Συμβάντος) x Συνέπειες (Περιστατικό, Περιουσιακό Στοιχείο)

Άλλος Τύπος

Κ7: Δυνατότητες για εμπλοκή των χρηστών στη διαδικασία της αξιολόγησης.

Κ8: Δυνατότητες υπολογιστικές, η δυνατότητα των μεθόδων να αναλύσουν και να συνδυάσουν διαφορετικά δεδομένα.

Κ9: Απαιτούμενη γνώση για να χρησιμοποιηθεί και να συντηρηθεί η μέθοδος.

. **Κ10:** Κόστος (Αδειοδότηση) / (Άδεια χρήσης μεθόδου).

Κ11: Αυτόματα εργαλεία που υλοποιούν την μέθοδο.

Κ12: Συμμόρφωση με τα πρότυπα.

	K1	K2	K3	K4	K5	K6	K7	K8	K9	K10	K11	K12
COBRA	Μ	ΓΜ	**ΑΚ/ΔΚ**	Ποιοτική	Βασιζόμενη σε κρίσιμα περιουσιακά στοιχεία	**Τύπος 1**	Μεσαία	Μεσαία	Βασική	Full Cobra Suite: **$1995** Cobra for ISO17799: **$895**	ΝΑΙ	***COBRA ISO17799***
OCTAVE	Μ	**ΓΜ**	**ΑΚ/ΔΚ**	Ποιοτική	Βασιζόμενη σε κρίσιμα περιουσιακά στοιχεία	**Τύπος 4**	Μεσαία	Χαμηλή	Βασική	**Για κάθε εφαρμογή :** 1500$ Διατίθεται δοκιμαστική έκδοση, Απαιτείται εγγραφή	ΝΑΙ	-
EBIOS	Μ/Ε	**ΓΜ**	**ΑΚ/ΔΚ**	Ποιοτική	Βασιζόμενη σε ανάγκες ασφαλείας	**Τύπος 2**	Μεσαία	Χαμηλή	Βασική	Δωρεάν	ΝΑΙ	ISO/IEC 27001:2005 ISO/IEC 27002:2005 ISO/IEC 27005:2008
CallioSecura		**ΓΜ**	**ΑΚ/ΔΚ**	Ποιοτική	Βασιζόμενη σε σενάρια ζημίας	**Τύπος 5**	Μεσαία	Χαμηλή	Βασική	$3.000	ΝΑΙ	ISO 27002:2005
CCS Risk Manager	Μ/Ε	**ΓΜ**	**ΑΚ/ΔΚ**	Ποιοτική	Βασιζόμενη σε απαιτήσεις ασφαλείας	**Άλλος Τύπος**	Χαμηλή	Μεσαία	Βασική	227,330: Άδεια για 500 χρήστες Κάθε επιπλέον χρόνο: € 27,330	ΝΑΙ	AS/NZS 4346, ISO/IEC 27002, ISO/IEC 27005, FRAP, Risk IT
Cloud e Assurance	Μ/Ε	**ΓΜ**	**ΑΚ/ΔΚ**	Ποιοτική	Βασιζόμενη σε απαιτήσεις ασφαλείας	**Άλλος Τύπος**	Μεσαία	Μεσαία	Βασική	Δωρεάν	ΝΑΙ	Βλέπε §(1)
EAR/Pilar	Μ/Ε	**ΓΜ**	**ΑΚ/ΔΚ**	Ποιοτική/ Ποσοτική	Βασιζόμενη σε σενάρια ζημίας	**Τύπος 5**	Χαμηλή	Χαμηλή	Ειδική	1500 € EAR +500 € Βάση	ΝΑΙ	ISO/IEC 27001:2005 ISO/IEC 27002:2005ISO/IEC 27005:2008
CRAMM	Μ/Ε	**ΓΜ**	**ΑΚ/ΔΚ**	Ποιοτική	Βασιζόμενη σε ανοιχτή ζημία	**Τύπος 1**	Χαμηλή	Χαμηλή	Ειδική	Εμπορικό	ΝΑΙ	ISO/IEC 27002:2005

Πίνακας 2: Αξιολόγηση μεθοδολογιών

Με βάση τα ανωτέρω η μέθοδος Pilar καλύπτει το μεγαλύτερο μέρος των κριτηρίων και έτσι κρίνονται καταλληλότερα για πληροφοριακό σύστημα που θα μελετηθεί.

3 Κεφάλαιο 3ο: Μελέτη Ανάλυσης και Διαχείρισης Κινδύνων ΠΣΓΝ

3.1 Σκοπός της Ανάλυσης

Η μελέτη ασφάλειας αφορά τα Πληροφοριακά Συστήματα και τα χειρόγραφα αρχεία που χρησιμοποιεί το ΓΝ. Χαρακτηριστικό των υπηρεσιών του Νοσοκομείου είναι ότι οι περισσότερες εφαρμογές λογισμικού που χρησιμοποιούνται έχουν αναπτυχθεί από τον ίδιο φορέα, επικοινωνούν με κοινή βάση και αποτελούν το Πληροφοριακό Σύστημα(ΠΣ) του Γενικού Νοσοκομείου.

3.2 Εμβέλεια της Ανάλυσης

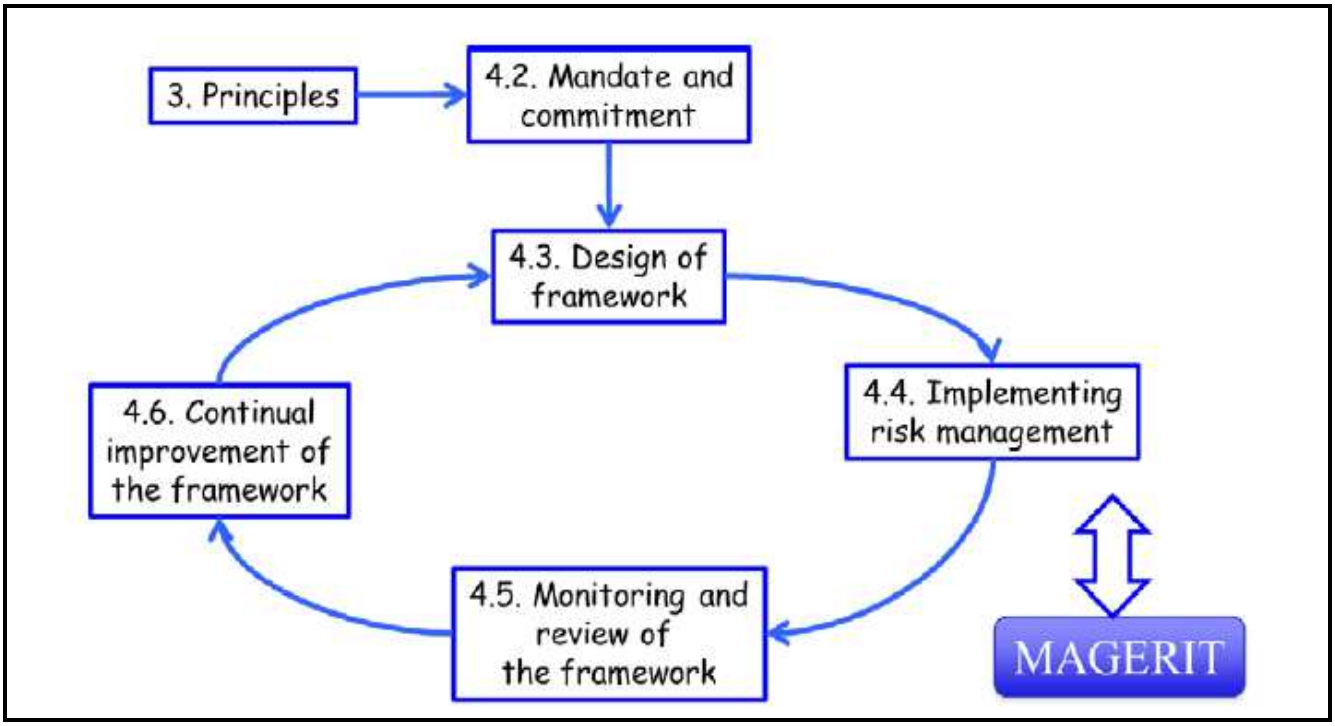
Το Πληροφοριακό Σύστημα του Νοσοκομείου απαρτίζεται από το ΠΣ του ΓΝ μαζί με τις υπόλοιπες τοπικές εφαρμογές και τα υπολογιστικά συστήματα που χρησιμοποιούνται.

3.3Μέθοδος και Εργαλεία

Η μεθοδολογία που υλοποιείται γι’ αυτή τη μελέτη ασφαλείας είναι η μεθοδολογία MAGERIT και η υλοποίηση θα γίνει μέσω του λογισμικού EAR/Pilar.

3.4. Επεξήγηση της μεθόδου MAGERIT (Περίληψη)

Σύμφωνα με την ορολογία του ISO31000 η MAGERIT υλοποιεί τη διαδικασία Ανάλυσης και Διαχείρισης Κινδύνων όπως φαίνεται ακολούθως:



Εικόνα 9: ISO31000 -Διαχείριση κινδύνου

Η μεθοδολογία MAGERIT πραγματοποιεί τους ακόλουθους στόχους:

1. Ενημέρωση των υπεύθυνων για τα πληροφοριακά συστήματα της ύπαρξης κινδύνων και της ανάγκης αντιμετώπισης τους.Προσφέρει μια συστηματική μέθοδο για την ανάλυση κινδύνων.

2. Προγραμματίζει για το Νοσοκομείο τις διαδικασίες αξιολόγησης, ελέγχου, πιστοποίησης.

Η μεθοδολογία ***MAGERIT*** **[6]** ακολουθεί τα εξής βήματα:

1.Χαρακτηρισμό των περιουσιακών στοιχείων που περιλαμβάνει:
   α. Αναγνώριση των περιουσιακών στοιχείων
   β. Συσχετίσεις μεταξύ τους
   γ. Αξιολόγηση των περιουσιακών στοιχείων

2.Χαρακτηρισμό των απειλών
   α. Καθορισμό των απειλών
   β. Αποτίμηση των απειλών

3.Προσδιορισμό αντιμέτρων ασφαλείας.

   α. Καθορισμό των σχετικών αντιμέτρων ασφαλείας
   β. Αξιολόγηση των αντιμέτρων ασφαλείας

4.Υπολογισμό κατάστασης κινδύνου.

   α. Υπολογισμό επίπτωσης.
   β. Υπολογισμό Κινδύνου

.

Η μεθοδολογία **διαχείρισης κινδύνων *της MAGERIT*** του ΠΣ του ΓΝ ακολουθεί τα εξής βήματα:

1. Αξιολόγηση- ερμηνεία της εναπομείνασας επίπτωσης και των τιμών κινδύνου.
2. Αποδοχή Κινδύνου.
3. Θεραπεία Κινδύνου

3.5 Περιουσιακά Στοιχεία

3.5.1 Μεθοδολογία

Πραγματοποιείται αναγνώριση των περιουσιακών στοιχείων του ΠΣΓΝ στις ακόλουθες κατηγορίες:

- **Δεδομένα (Data Assets):** Είναι όλα εκείνα τα δεδομένα που ανήκουν στις κατηγορίες προσωπικών στοιχείων, προσωπικών ευαίσθητων και ευαίσθητων δεδομένων τα οποία ανήκουν στις κατηγορίες των δεδομένων υπαλλήλων, των δεδομένων ασθενών και των δεδομένων μισθοδοσίας.
- **Υπηρεσίες (End User Services):** Είναι όλες εκείνες οι υπηρεσίες τελικού χρήστη που παρέχουν τις υπηρεσίες στον χρήστη.
- **Υλικά Στοιχεία:** Είναι όλα εκείνα τα υλικά στοιχεία τα οποία επεξεργάζονται τα δεδομένα για τα οποία πραγματοποιείται η ανάλυση επικινδυνότητας
- **Τοποθεσίες:** Ολες οι κτιριακές εγκαταστάσεις στις οποίες είναι εγκατεστημένος ο υλικός εξοπλισμός για του ΠΣ-ΓΝ.
- **Λογισμικό:** Περιλαμβάνει όλο το λογισμικό (λειτουργικό λογισμικό, λογισμικά εφαρμογών, λογισμικά υποστήριξης.

Επειδή τα περιουσιακά στοιχεία συσχετίζονται μεταξύ τους, δηλαδή τα δεδομένα με τις υπηρεσίες και τον εξοπλισμό ο οποίος τα επεξεργάζεται, η μεθοδολογία προσφέρει την δημιουργία μοντέλου συσχέτισης των ανωτέρω, για τον υπολογισμό των τιμών τους στην αξιολόγηση.

3.5.2 Αναγνώριση των περιουσιακών στοιχείων στο ΠΣΓΝ

Τα κύρια στοιχεία που συνθέτουν το σύστημα σε υλικό, λογισμικό, δεδομένα, διαδικασίες και το προσωπικό που μελετήθηκε ελήφθησαν από την μελέτη συγκεκριμένου Νοσοκομείου **[31]** και ήταν τα ακόλουθα :

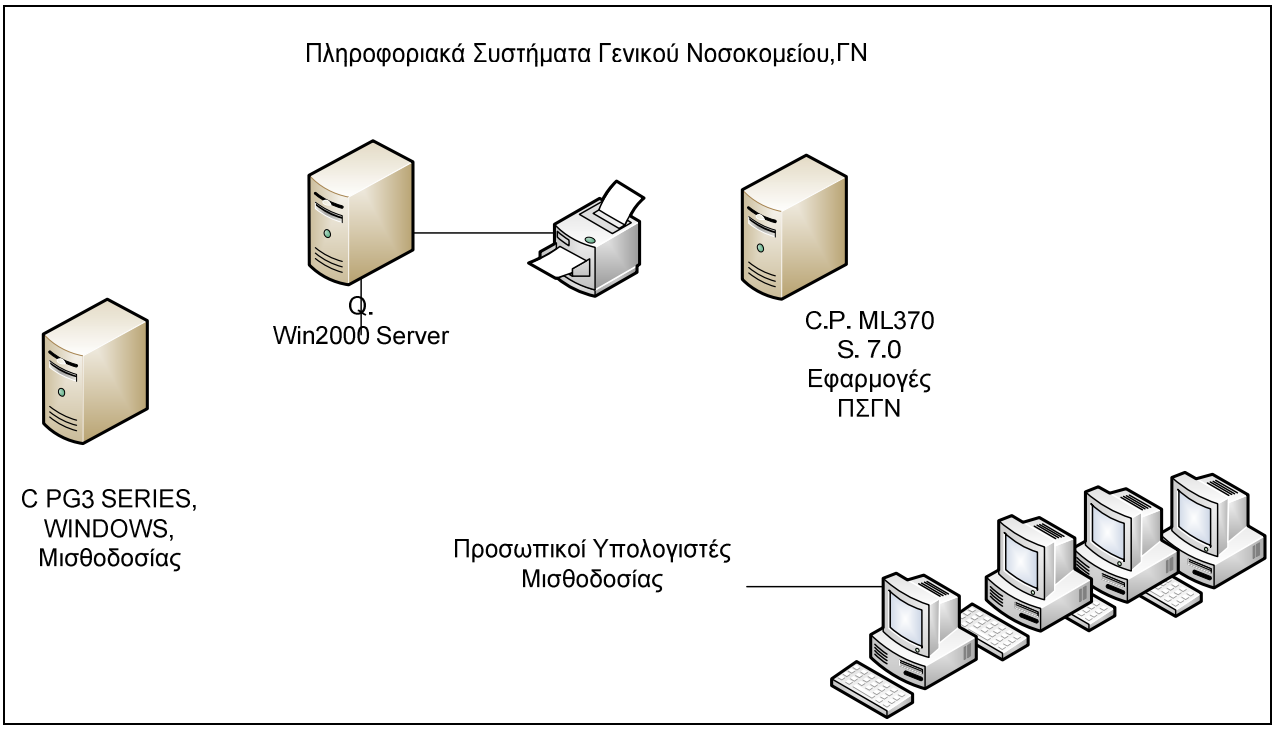
3.5.2.1.Δεδομένα

Η κατηγοριοποίηση των δεδομένων των ΠΣ-ΓΝ μπορεί να γίνει, με κριτήριο τη νομική τους υπόσταση, σε τρεις κατηγορίες. Στα *μη-προσωπικά δεδομένα*, στα *προσωπικά δεδομένα* και στα *ευαίσθητα προσωπικά δεδομένα*. Τα ευαίσθητα προσωπικά δεδομένα αποτελούν υποσύνολο των προσωπικών δεδομένων. Ειδικότερα, οι κύριες ομάδες δεδομένων που εξετάστηκαν είναι:

- ***Δεδομένα ασθενών***. Αφορούν την περίθαλψη των ασθενών και είναι **ευαίσθητα** δεδομένα. Περιλαμβάνουν δεδομένα που αφορούν τις επισκέψεις ασθενών στα εξωτερικά ιατρεία, δεδομένα χορήγησης φαρμάκων, καθώς και δεδομένα ιατρικών και εργαστηριακών εξετάσεων και δεδομένα της αιμοδοσίας. Ταυτόχρονα, τηρούνται και δεδομένα οικονομικής φύσης που απαιτούνται για την είσπραξη των νοσηλίων των ασθενών από τους ασφαλιστικούς φορείς.
- ***Δεδομένα εργαζομένων***. Τα δεδομένα αυτά περιλαμβάνουν **προσωπικά** και οικονομικά στοιχεία που αφορούν τους εργαζόμενους στο ΓΝ και σχετίζονται, κυρίως, με την καταβολή των αμοιβών τους καθώς και την καταβολή των μισθοδοτικών εισφορών.
- ***Οικονομικά και λογιστικά δεδομένα***. Σε αυτά περιλαμβάνονται τα **προσωπικά** και **οικονομικά** στοιχεία των συναλλασσόμενων με το ΓΝ, όπως είναι οι προμηθευτές του νοσοκομείου, τα στοιχεία που αφορούν τις οικονομικές συναλλαγές, τα στοιχεία του πρωτοκόλλου, καθώς και στοιχεία ισο-λογισμών και απολογισμών.

3.5.3Υλικός εξοπλισμός (hardware)

3.5.3.1Εξοπλισμός κεντρικών συστημάτων.



Εικόνα 10: Αρχιτεκτονική υποδομής

- Ένας (1) εξυπηρετητής *(server)* με λειτουργικό σύστημα Windows 2000 Server, που λειτουργεί η εφαρμογή **Ηλεκτρονικού Πρωτοκόλλου** της εταιρείας. Ο εξυπηρετητής αυτός στεγάζεται στους χώρους της Γραμματείας και το Πρωτόκολλο.
- Ένας (1) εξυπηρετητής με λειτουργικό σύστημα Solaris 7.0, ο οποίος στεγάζεται στο Τμήμα Πληροφορικής και Οργάνωσης του **ΓΝ**. Εκεί λειτουργούν οι εφαρμογές **ΓΝ,** τις οποίες έχει αναπτύξει το ΚΗΥΚΥ και χρησιμοποιούνται από το Τμήμα Εισαγωγών Ασθενών, το Φαρμακείο, το Γραφείο Υλικού, το Λογιστήριο, το Τμήμα Διατροφής, τη Γραμματεία Εξωτερικών Ιατρείων, τα Γραφεία Νοσηλίων, Ιματισμού και Υγειονομικού Υλικού.
- Ένας (1) εξυπηρετητής με λειτουργικό σύστημα Windows, με τις εφαρμογές του Τμήματος **Αιμοδοσίας** και είναι εγκατεστημένος στο Τμήμα αυτό.
- Προσωπικοί Υπολογιστές με λειτουργικό σύστημα Windows με την εφαρμογή της **Μισθοδοσίας** και βρίσκονται σε αυτό το τμήμα.
- Ένας (1) κεντρικός εκτυπωτής (Line Printer), για τον κεντρικό εξυπηρετητή που είναι εγκατεστημένος στο Τμήμα Πληροφορικής και Οργάνωσης.
- Δικτυακός εξοπλισμός των κεντρικών συστημάτων

***3.5.3.2 Σταθμοί εργασίας*.**

Οι σταθμοί εργασίας που λειτουργούν ως ***τερματικοί σταθμοί του κεντρικού συστήματος εφαρμογών*** του ΓΝ, εξυπηρετούν τους χρήστες των εφαρμογών το Φαρμακείο, το Γραφείο Υλικού, το Χρηματικό Γραφείο (Λογιστήριο), το Γραφείο Νοσηλίων, το Τμήμα Εισαγωγών Ασθενών, το Τμήμα Διατροφής, η Γραμματεία Εξωτερικών Ιατρείων, το Γραφείο Υγειονομικού και το Τμήμα Ιματισμού.

- Χρησιμοποιούνται επίσης **σταθμοί εργασίας** για χρήση των τοπικών εφαρμογών στο Σταθμό Αιμοδοσίας, στη Γραμματεία – Πρωτόκολλο, στο Γραφείο Μισθοδοσίας, στο γραφείο Προσωπικού και στο Γραφείο Προμηθειών.
- Ακόμη υπάρχουν ***Προσωπικοί υπολογιστές*** του ΓΝ, για επαγγελματική και επιστημονική χρήση του προσωπικού του σε όλα τα τμήματα του νοσοκομείου.
- Χρησιμοποιούνται επίσης δύο (2) **προσωπικοί υπολογιστές** στο χώρο του Τμήματος Πληροφορικής και Οργάνωσης για πρόσβαση στο Διαδίκτυο (Internet Room) από το προσωπικό του Νοσοκομείου.
- Υπάρχουν επίσης **Προσωπικοί υπολογιστές** στα Κέντρα Υγείας.
- Συνολικά το πλήθος των προσωπικών υπολογιστών που χρησιμοποιούνται στο ΓΝ είναι περίπου εκατόν είκοσι (120). Συνολικά, για το εσωτερικό δίκτυο του Νοσοκομείου λειτουργούν γύρω στις διακόσιες πενήντα (250) θέσεις εργασίες για τους χρήστες των Πληροφοριακών Συστημάτων.
- *Εξοπλισμός δικτύου*. Περιλαμβάνει τις συσκευές του δικτύου, όπως δρομολογητές, τερματικές συσκευές κλπ., που χρησιμοποιούνται για τη λειτουργία των Πληροφοριακών Συστημάτων του **ΓΝ.** Οι δικτυακές και τηλεπικοινωνιακές υπηρεσίες που παρέχονται από τρίτους φορείς (π.χ. ΟΤΕ), καθώς και ο αντίστοιχος εξοπλισμός, δεν περιλαμβάνονται. Λαμβάνονται, όμως, υπόψη στην παρούσα μελέτη ασφάλειας ως πιθανές πηγές απειλών και κινδύνων.

3.5.3.3 Σχετικά συστήματα

Τα ΠΣ του ΓΝ δε διασυνδέονται άμεσα με συστήματα άλλων οργανισμών ή υπηρεσιών. Πρόσβαση στα συστήματα αυτά έχουν (μέσω modem) οι εταιρείες που τα έχουν αναπτύξει και έχουν αναλάβει τη συντηρησή τους καθώς και οι εταιρείες τεχνικής υποστήριξης, ελήφθη, όμως, υπόψη και η δυνατότητα πρόσβασης χρηστών κάποιων εφαρμογών στο Διαδίκτυο μέσω modems.

3.5.3.4 Παρεχόμενες υπηρεσίες

Τα ΠΣ του ΓΝ υποστηρίζουν τις βασικές διαχειριστικές λειτουργίες του ΓΝ. Αναλυτικότερα, τα ΠΣ αυτά υποστηρίζουν τις εξής λειτουργίες:

- Οικονομική διαχείριση
- Λογιστική διαχείριση
- Παραλαβή και διάθεση φαρμακευτικού και υγειονομικού υλικού
- Διαχείριση προσωπικών και οικονομικών δεδομένων των εργαζομένων
- Παροχή υπηρεσιών προς νοσηλευόμενους και εξωτερικούς ασθενείς
- Νοσηλεία ασθενών
- Παροχή φαρμακευτικής περίθαλψης
- Παροχή αποτελεσμάτων εργαστηριακών εξετάσεων

3.6. Λογισμικό και εφαρμογές

Η παρούσα μελέτη ασφάλειας έχει συμπεριλάβει το ακόλουθο λογισμικό:

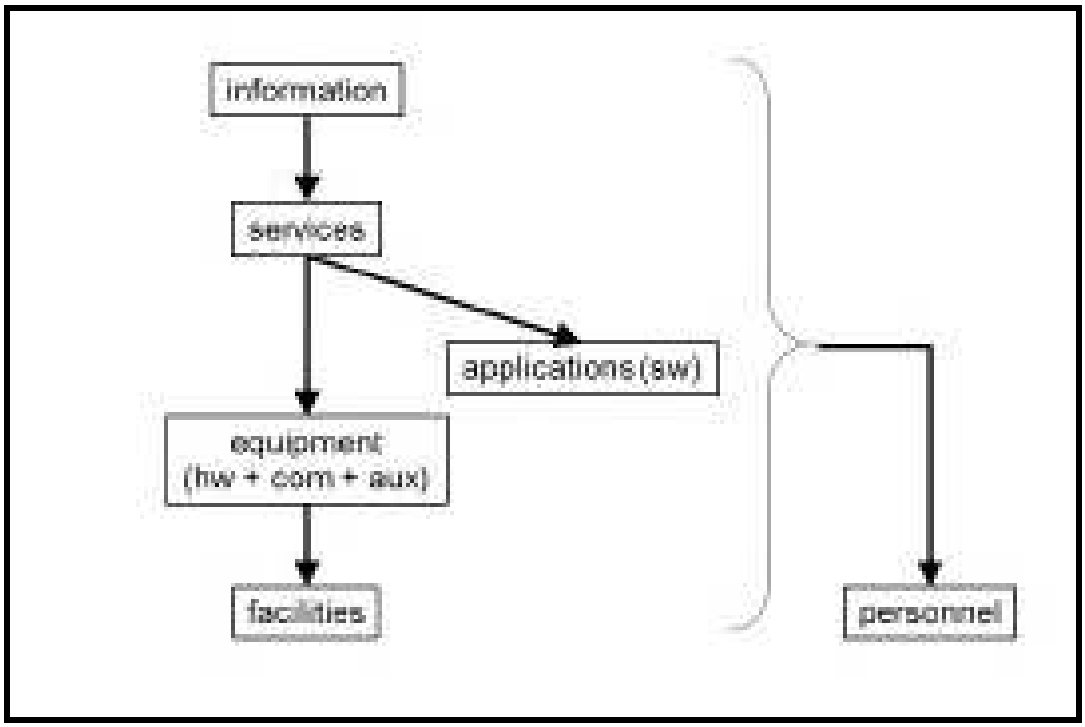
- *Λογισμικό συστημάτων και ανάπτυξης εφαρμογών.* αποτελούνται από τα λειτουργικά συστήματα των εξυπηρετητών και των σταθμών εργασίας (Windows, Solaris). Επίσης, περιλαμβάνουν βοηθητικό λογισμικό (π.χ. MS Office), λογισμικό βάσεων δεδομένων (Oracle), λογισμικό διαχείρισης ηλεκτρονικού ταχυδρομείου (e-mail) και λογισμικό για την ασφάλεια των Πληροφορικών Συστημάτων (McAfee Antivirus, Karspersky).
- *Εφαρμογές Διαχειριστικού Πληροφοριακού Συστήματος Νοσοκομείου (ΠΣΝ):* Συμπεριλαμβάνουν όλες τις εφαρμογές του Τμήματος Εισαγωγής Ασθενών, και τις υπόλοιπες εφαρμογές του νοσοκομείου.
- *Τοπικές εφαρμογές:* Συμπεριλαμβάνει όλες τις εφαρμογές της *Αιμοδοσίας* , τις εφαρμογές της *Μισθοδοσίας* και τις εφαρμογές *Ηλεκτρονικού Πρωτοκόλλου* εταιρείας.
- *Ειδικές εφαρμογές:* Ειδικό λογισμικό που χρησιμοποιείται για συγκεκριμένους σκοπούς, όπως το firewall.

3.7 Μοντέλο Συσχέτισης

Λόγω του γεγονότος ότι η διαχειριζόμενη πληροφορία και οι παρεχόμενες υπηρεσίες εξαρτώνται από περιουσιακά στοιχεία όπως εξοπλισμός, επικοινωνίες, η έννοια του βαθμού από τον οποίο εξαρτώνται από ένα περιστατικό ασφαλείας ένα υψηλότερου επιπέδου περιουσιακό στοιχείο από ένα χαμηλό είναι σημαντική.

Παρόλο που είναι απαραίτητο το ΓΝ να αναλυθεί ως ξεχωριστή περίπτωση σύμφωνα με τη μεθοδολογία, τα περιουσιακά στοιχεία μπορούν να παρουσιαστούν δομημένα σε επίπεδα όπου τα άνω επίπεδα εξαρτώνται από τα κάτω επίπεδα. Το μοντέλο συσχέτισης δίνει τις τιμές για την αποτίμηση των δεδομένων.

Στην συγκεκριμένη περίπτωση η συνολική αξία των περιουσιακών στοιχείων έγινε με βάση τις συσχετίσεις που φαίνονται στο **Παράρτημα Γ.**



Εικόνα 11:Ιεραρχία των Εξαρτήσεων

3.8 Αξιολόγηση περιουσιακών στοιχείων του ΠΣ-ΓΝ

3.8.1 Εισαγωγή

Στο κεφάλαιο αυτό περιγράφονται τα αποτελέσματα της αποτίμησης των δεδομένων που διαχειρίζεται το ΠΣΓΝ. Η ακολουθούμενη μεθοδολογία αποδίδει ιδιαίτερη βαρύτητα στα *δεδομένα* και λιγότερο στο *υλικό* και *λογισμικό*. Χρησιμοποιεί πολλαπλά χαρακτηριστικά για την αποτίμηση των δεδομένων ή ένα ανάλογα με το σενάριο. Στην περίπτωση μας πραγματοποιήθηκε ανάλυση για την αποτίμηση των δεδομένων σύμφωνα με τις επιπτώσεις της απώλειας της διαθεσιμότητας, της ακεραιότητας,της εμπιστευτικότητας.

3.8.2 Καθορισμός Δεδομένων

Η μεθοδολογία Magerit έχει δύο βασικούς τύπους δεδομένων του Π.Σ. Την πληροφορία που διαχειρίζεται και τις υπηρεσίες που παρέχει. Τα δεδομένα που αναλύθηκαν με τη μεθοδολογία Magerit παρουσιάζονται στον ακόλουθο Πίνακα.

Λογισμικό	***Δεδομένα***
Σύστημα Διαχείρισης Μισθοδοσίας	Μισθοδοσίας
Σύστημα Ασθενών-Πελατών	Οικονομικά
Σύστημα Διαχείρισης Προσωπικού	Οικονομικά

Πίνακας 3 : Δεδομένα Ανάλυσης

Σημειώνεται ότι το σύνολο των δεδομένων που διαχειρίζονται τα ΠΣ-ΓΝ διαχωρίστηκαν και μελετήθηκαν σε αντιπροσωπευτικές ομάδες, ανάλογα με τα χαρακτηριστικά και τις ανάγκες ασφάλειας που έχουν. Συγκεκριμένα, αποτιμήθηκαν οι συνέπειες για τις εξής ομάδες δεδομένων ***Δεδομένα Εργαστηρίων***, ***Δεδομένα Προσωπικού***, ***Δεδομένα Μισθοδοσίας.***

3.9 Αποτίμηση περιουσιακών στοιχείων του Π.Σ.

Η αποτίμηση των περιουσιακών στοιχείων του ΠΣ-ΓΝ έγινε από την ομάδα ανάλυσης κινδύνων πληροφοριών σε συνεργασία με τον διευθυντή πληροφορικής του Νοσοκομείου, όπου εξετάστηκαν **[6], [7]**, οι επιπτώσεις στην λειτουργία των ΠΣ για τις περιπτώσεις μη διαθεσιμότητας, μη ακεραιότητας, μη εμπιστευτικότητας λαμβάνοντας υπόψη το πιο απαισιόδοξο σενάριο.

Για την αποτίμηση του εναπομείναντος κινδύνου λάβαμε υπ' όψιν υφιστάμενα μέτρα ασφαλείας του ΠΣ-ΓΝ και τις επιπτώσεις που θα έχει η εταιρεία σε περίπτωση απειλών.

Η κατηγοριοποίηση των πιο κρίσιμων υπηρεσιών πραγματοποιήθηκε με βάση την γνώμη των αρμοδίων στελεχών της εταιρείας.

Η αξία καθορίστηκε για τα κρίσιμα περιουσιακά στοιχεία (πληροφορίες και υπηρεσίες) και καταγράφεται στον τομέα ασφαλείας(security domain). Η αξιολόγηση τους γίνεται με βάση τις πληροφορίες των τελικών χρηστών που δίνουν για τα ΠΣ του ΓΝ στην κλίμακα που έχει το Pilar.

Αφού εισήγαμε τα περιουσιακά στοιχεία στο λογισμικό Pilar και τις αλληλεξαρτήσεις τους, δημιουργήσαμε μια αναφορά με την αξιολόγηση των περιουσιακών στοιχείων. Για την υλοποίηση πήραμε τις συνεντεύξεις από τους διευθυντές, από τους αρμόδιους ανθρώπους για τα περιουσιακά στοιχεία, για τις υπηρεσίες, και για κάθε περιουσιακό στοιχείο καθορίστηκε μια περιγραφή με χαρακτηριστικά:

- Κωδικός
- Όνομα,περιγραφή.
- Τύπος που χαρακτηρίζει το περιουσιακό στοιχείο.
- Υπεύθυνο προσωπικό.
- Τεχνική ή γεωγραφική τοποθεσία.
- Ποσό, όπου είναι κατάλληλο, για παράδειγμα 300 Η/Υ γραφείου.
- Όρια μέσα στα οποία ένα περιουσιακό στοιχείο είναι σχετικό.
- Υπολογισμός της αξιολόγησης.
- Επεξήγηση της αξιολόγησης.
- Συνεντεύξεις.

Μη συμπληρωμένο υπόδειγμα των ερωτηματολογίων είναι στο **Παράρτημα Α.**

Τα αποτελέσματα της αποτίμησης είναι συνάρτηση της πληρότητας των εκτιμήσεων-απαντήσεων που δόθηκαν στους αναλυτές. Για την αποτίμηση ελήφθησαν υπ' όψιν, οι συνολικές τιμές (**accumulated values**) των αγαθών.

Η αποτίμηση πραγματοποιήθηκε με γνώμονα την ανάγκη προστασίας των περιουσιακών στοιχείων. Όσο πιο πολύτιμο δηλαδή, όσο πιο υψηλό ήταν το επίπεδο προστασίας που έχει ένα περιουσιακό στοιχείο τόσο πιο μεγάλη είναι η ανάγκη προστασίας του. Συνεπώς, τόσο πιο πολλά είναι τα αντίμετρα που απαιτούνται για να καλυφθούν οι απαιτήσεις ασφαλείας εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητας.

Η αποτίμηση έγινε λαμβάνοντας υπόψη το κόστος αντικατάστασης, το εργασιακό κόστος, την απώλεια εισοδήματος, την απώλεια λειτουργίας, τις ποινές μη νομικής συμμόρφωσης, την ζημία σε άλλα περιουσιακά, ή ανθρώπους και σε περιβαλλοντική ζημία. Συνεπώς, τα συμπεράσματα που προκύπτουν ανάγονται στο σύνολο των δεδομένων της κάθε ομάδας.

Το υλικό και λογισμικό αποτιμήθηκε με βάση το κόστος αντικατάστασής τους.

Η αξιολόγηση έγινε αριθμητικά σε κλίμακα (1) -(10) και οι τιμές που έχουν αποδοθεί προκύπτουν από τους **Πίνακες Αποτίμησης Δεδομένων** που συνοδεύουν τη μεθοδολογία MAGERIT και το εργαλείο λογισμικού Pilar (βλ. **Παράρτημα Γ**). Η αποτίμηση πραγματοποιήθηκε με βάση το Κεφάλαιο 4 του Καταλόγου των στοιχείων του βιβλίου ΙΙ της μεθοδολογίας Magerit.

Αξία		**Κριτήριο**
10	Πολύ υψηλή	Πολύ σοβαρή ζημιά στον οργανισμό
7-9	Υψηλή	Σοβαρή ζημιά στον Οργανισμό
4-6	Μεσαία	Σημαντική ζημιά στον Οργανισμό
1-3	Χαμηλή	Μικρή ζημιά στον Οργανισμό
0	Ελάχιστη	Άσχετη για πρακτικούς λόγους.

Πίνακας 4: Κλίμακα Αποτίμησης

Asset	[A]	[I]	[C]	[V]
[datalabpatients] datapatients	215K(1)	100K(2)	215K(3)	100K(6)
[dataemployees] dataemployees	1M(7)	215K(8)	215K(9)	215K(12)
[financial] finlogisticssubcontractor	215K(13)	1M(14)	215K(15)	100K(18)

Πίνακας 5: Αποτίμηση Δεδομένων

Στις ακόλουθες παραγράφους περιγράφεται αναλυτικά η αποτίμηση των επιπτώσεων από την παραβίαση της ασφάλειας των τριών ομάδων δεδομένων που αξιολογήθηκαν στο πλαίσιο της μελέτης. Όλα τα αντικείμενα που βαθμολογούνται ως πολύ υψηλά πρέπει να τα προστατέψουμε άμεσα.

3.9.1 Δεδομένα Ασθενών (Πελατών)

Περιεχόμενο: Τα Δεδομένα ασθενών αποτελούνται από προσωπικά στοιχεία των νοσηλευομένων, και μη, ασθενών που έχουν εξεταστεί από το εργαστήριο, καθώς και **ευαίσθητα** ιατρικά δεδομένα (π.χ. διαγνώσεις ασθενειών, αποτελέσματα εξετάσεων). Τα δεδομένα αυτά δεν περιλαμβάνουν στοιχεία που αφορούν σε μολυσματικές ασθένειες.

Σχετικό Σύστημα: Τα Δεδομένα των ασθενών είναι αποθηκευμένα στο σύστημα των αντίστοιχων εγκαταστάσεων κάθε Εργαστηρίου.

Παράλληλα, υπάρχει χειρόγραφο αρχείο Ασθενών στο οποίο φυλάσσονται παραπεμπτικά από κλινικές και αναλύσεις των εργαστηρίων. Ένα ποσοστό των στοιχείων αυτών καταστρέφεται έπειτα από τη χρήση τους, ενώ τα βιβλία αποθηκεύονται στο Αρχείο.

3.9.1.1 Απώλεια Διαθεσιμότητας Δεδομένων Ασθενών

Επιπτώσεις: Η μη διαθεσιμότητα των δεδομένων Ασθενών δε θα επιφέρει σημαντικές επιπτώσεις στην ομαλή λειτουργία του ΓΝ καθώς τηρούνται χειρόγραφα βιβλία. Επιπλέον, τα αποτελέσματα των εξετάσεων επιστρέφονται στην κλινική που τα ζήτησε και έπειτα τμήμα των δεδομένων καταστρέφεται.

Αποτίμηση: Συνεπώς, η συνέπεια της απώλειας διαθεσιμότητας για χρονικό διάστημα έως μία ημέρα αποτιμάται με βαθμό **τρία (3)**, στην κλίμακα 0-10.

3.9.1.2 Απώλεια ακεραιότητας Δεδομένων Ασθενών - Σκόπιμη Αλλοίωση Δεδομένων Εργαστηρίων

Επιπτώσεις: Η σκόπιμη αλλοίωση των αποτελεσμάτων των εξετάσεων των εργαστηρίων μπορεί να θέσει σε κίνδυνο τη ζωή και την ασφάλεια των εξετασμένων, καθώς τα δεδομένα των ασθενών καθορίζουν τις ενέργειες για την ιατρική παρακολούθηση των ασθενών. Συμπερασματικά, μια επιτυχής σκόπιμη αλλοίωση αυτών των δεδομένων ενδέχεται να βλάψει την ασφάλεια των ασθενών του ΓΝ.

Αποτίμηση: Σύμφωνα με το παραπάνω σενάριο, η συνέπεια σκόπιμης αλλοίωσης αποτιμάται με βαθμό **πέντε (5)**, σε κλίμακα 0-10**.**

3.9.1.3 Απώλεια Εμπιστευτικότητας

Επιπτώσεις: Τα Δεδομένα Ασθενών αποτελούν ευαίσθητα προσωπικά δεδομένα. Σύμφωνα με τον Ν. 2472/97 ενδεχόμενη αποκάλυψη τους μπορεί να επιφέρει ποινικές κυρώσεις και άμεσες επιπτώσεις στη δημόσια εικόνα και την αξιοπιστία του.

. Ο νόμος 2472/97 προβλέπει σημαντικά χρηματικά πρόστιμα, καθώς και ποινές φυλάκισης για τον υπεύθυνο επεξεργασίας που δε συμμορφώνεται, οι οποίες φτάνουν μέχρι τα δέκα (10) έτη σε εξαιρετικές περιπτώσεις.

Αποτίμηση: Η επίπτωση της **αποκάλυψης σε τρίτους** των δεδομένων υγείας των ασθενών αποτιμάται με βαθμό **έξι (6)** σε κλίμακα 0-10

Κατηγορία Επίπτωσης		**Επιπτώσεις στο Νοσοκομείο**	**Βαθμός Αποτίμησης**
Απώλεια Διαθεσιμότητας Δεδομένων	1 ημέρα	Οικονομική Απώλεια	3
Απώλεια Ακεραιότητας Δεδομένων	Αλλοίωση Δεδομένων	Ποινικές Κυρώσεις Καταστροφή καλής φήμης	5
Απώλεια Εμπιστευτικότητας	Αποκάλυψη των δεδομένων σε τρίτους	Ποινικές Κυρώσεις	6

Πίνακας 6: Αποτίμηση Δεδομένων Ασθενών

3.9. 2 Δεδομένα Προσωπικού

Περιεχόμενο: Τα Δεδομένα Προσωπικού περιλαμβάνουν προσωπικά δεδομένα των υπαλλήλων του ΓΝ και την επαγγελματική τους θέση, αλλά και στοιχεία αναρρωτικών αδειών τους. Επιπλέον, τα δεδομένα αυτά περιλαμβάνουν ευαίσθητα προσωπικά στοιχεία που αφορούν στο ποινικό μητρώο του κάθε υπαλλήλου.

Σχετικό Σύστημα: Τα Δεδομένα Προσωπικού τηρούνται στην εφαρμογή Προσωπικού που στεγάζεται στις εγκαταστάσεις του Τμήματος Πληροφορικής *(Computer Room)*, στο υπόγειο του ΓΝ. Επιπλέον, όλες οι σχετικές πληροφορίες (π.χ. προσωπικά στοιχεία και ποινικό μητρώο) είναι αποθηκευμένα και σε χειρόγραφη μορφή σε φυσικό αρχείο που στεγάζεται στο Τμήμα Προσωπικού στο ισόγειο του κεντρικού κτηρίου του ΓΝ.

3.9.2.1 Απώλεια Διαθεσιμότητας Δεδομένων Προσωπικού

Επιπτώσεις: Η μη διαθεσιμότητα των δεδομένων αυτών δε διακόπτει την εύρυθμη λειτουργία του τμήματος Προσωπικού. Οι επιπτώσεις από την απώλεια διαθεσιμότητας των δεδομένων Προσωπικού δεν είναι σημαντικές, καθώς γίνεται χρήση των χειρόγραφων φακέλων.

Αποτίμηση: Η επίπτωση της μη διαθεσιμότητας των δεδομένων αυτών αποτιμάται με βαθμό **τρία (3)** για διάστημα έως μία ημέρα, σε κλίμακα 0-10.

3.9.2.2 Απώλεια Μερικής Ακεραιότητας Δεδομένων - Σκόπιμη Αλλοίωση Δεδομένων Προσωπικού

Επιπτώσεις: Η εσφαλμένη εισαγωγή των δεδομένων που έχουν εισαχθεί έπειτα από τη λήψη του τελευταίου εφεδρικού αντιγράφου, ή η απώλεια στα δεδομένα, έχει ως επίπτωση την εκ νέου εισαγωγή τους. Άλλη επίπτωση σε αυτήν την περίπτωση αφορά στο κόστος που προκύπτει από τις αντίστοιχες ανθρωποώρες που απαιτείται για την επανεισαγωγή των δεδομένων. Μεγαλύτερη επίπτωση προκύπτει από τη λανθασμένη εισαγωγή στοιχείων ποινικού μητρώου, που μπορεί να καθορίσει δυσμενώς την επαγγελματική εξέλιξη των εργαζομένων.

Αποτίμηση: Η συνέπεια από απώλεια της ακεραιότητας των δεδομένων σύμφωνα με τα παραπάνω αποτιμάται με βαθμό **τρία (3).**

3.9.2.3 Απώλεια Εμπιστευτικότητας(Αποκάλυψη) Δεδομένων Προσωπικού

Επιπτώσεις: Η αποκάλυψη των προσωπικών δεδομένων των εργαζομένων σε άλλους εργαζομένους ή τρίτους, θα είχε ως επίπτωση ενδεχόμενα προσωπικά, οικονομικά και άλλα οφέλη γι' αυτούς. Στην περίπτωση αυτή το ΓΝ υπόκειται στις διατάξεις του νόμου που ορίζει ο νόμος για την απώλεια της εμπιστευτικότητας των προσωπικών στοιχείων, στις οποίες περιλαμβάνονται τόσο χρηματικές συνέπειες όσο και ποινικές συνέπειες για αυτό. Επιπροσθέτως, το ΓΝ συμπεριλαμβάνει και τα ευαίσθητα προσωπικά δεδομένα του ποινικού μητρώου κάθε εργαζομένου, η ενδεχόμενη αποκάλυψη αποτελεί σοβαρή παράβαση του Ν. 2472/97 με τις αντίστοιχες ποινικές κυρώσεις.

Αποτίμηση: Η επίπτωση της αποκάλυψης των Δεδομένων Προσωπικού σε τρίτους αποτιμάται με βαθμό **έξι (6)**.

Κατηγορία Επίπτωσης		Επιπτώσεις στο Νοσοκομείο	Βαθμός Αποτίμησης
Απώλεια Διαθεσιμότητας Δεδομένων	1 ημέρα	Οικονομική Απώλεια	3
Απώλεια Ακεραιότητας Δεδομένων	Αλλοίωση Δεδομένων	Ποινικές Κυρώσεις Καταστροφή καλής φήμης	5
Απώλεια Εμπιστευτικότητας	Αποκάλυψη των δεδομένων σε τρίτους	Ποινικές Κυρώσεις	6

Πίνακας 7: Αποτίμηση Δεδομένων Προσωπικού

3.9.3 Δεδομένα Μισθοδοσίας

Περιεχόμενο: Τα δεδομένα περιλαμβάνουν προσωπικά(όπως άδειες, αλλά κυρίως οικονομικά στοιχεία που αφορούν τους εργαζόμενους στο ΓΝ καθώς και δεδομένα δανείων που λαμβάνουν εργαζόμενοι μέσω του ΓΝ.

Σχετικό Σύστημα: Τα Δεδομένα Μισθοδοσίας τηρούνται στην *εφαρμογή Μισθοδοσίας* που στεγάζεται στις εγκαταστάσεις του Τμήματος Μισθοδοσίας στο ισόγειο του ΓΝ.

3.9.3.1 Απώλεια Διαθεσιμότητας Δεδομένων Μισθοδοσίας

Επιπτώσεις: Η *απώλεια της διαθεσιμότητας* των δεδομένων μισθοδοσίας έχει ως συνέπεια την στάση πληρωμών η οποία μπορεί να οδηγήσει σε μηνύσεις ενάντια στην εταιρεία και σε παραίτηση προσωπικού Οι επιπτώσεις που θα προκύψουν αφορούν κυρίως τη δυσκολία έκδοσης των μισθοδοτικών καταστάσεων και τις επιπλέον ανθρωποώρες που απαιτούνται. Η μη διαθεσιμότητα των στοιχείων αυτών δε θα εμποδίσει την ομαλή λειτουργία του Τμήματος Μισθοδοσίας.

Αποτίμηση: Λόγω του γεγονότος ότι οι μισθολογικές καταστάσεις μπορούν να συμπληρωθούν με χρήση των χειρόγραφων στοιχείων, η λειτουργία του τμήματος μπορεί να διεξαχθεί ομαλά αν η εφαρμογή δεν είναι διαθέσιμη για αρκετές ημέρες. Η επίπτωση της μη διαθεσιμότητας των δεδομένων αυτών αποτιμάται με βαθμό **τρία (3)** για διάστημα μιας εβδομάδος και πλέον, σε κλίμακα **0-10**.

3.9.3.2 Απώλεια Ακεραιότητας ή Μερική Καταστροφή Δεδομένων Μισθοδοσίας

Επιπτώσεις: Η αλλοίωση των Δεδομένων Μισθοδοσίας, περιλαμβανομένων και των εφεδρικών αντιγράφων, απαιτεί την εκ νέου εισαγωγή των δεδομένων στην εφαρμογή, βάσει των αυθεντικών στοιχείων που τηρούνται στο φυσικό αρχείο Μισθοδοσίας. Σημαντικές επιπτώσεις μπορεί να έχει η εισαγωγή σφαλμάτων με οικονομικές απώλειες για το Νοσοκομείο. Επιπλέον προβλήματα προκύπτουν αναφορικά με τα στοιχεία δανείων των εργαζομένων (οφειλές, δόσεις κλπ.) που προκαλεί επιπλέον κόστος αποκατάστασης των στοιχείων αυτών, από τον αντίστοιχο πιστωτικό φορέα.

Αποτίμηση: Κατά συνέπεια, εκτιμάται ότι θα υπάρξει οικονομικό κόστος που αφορά τις ανθρωποώρες που απαιτούνται για την εισαγωγή των δεδομένων. Η επίπτωση του ενδεχομένου μερικής καταστροφής των στοιχείων αποτιμάται με βαθμό **τρία (3)**, σε κλίμακα 0-10.

3.9.3.3 Απώλεια Εμπιστευτικότητας - Αποκάλυψη Δεδομένων Μισθοδοσίας

Επιπτώσεις: Τα στοιχεία μισθοδοσίας είναι γενικά, εμπιστευτικής φύσης. Η μη εξουσιοδοτημένη δημοσιοποίησή τους σε άλλους εργαζομένους ή τρίτους, θα είχε ως συνέπεια ενδεχόμενα προσωπικά, οικονομικά και άλλα οφέλη γι' αυτούς. Συνεπώς έχει ως επίπτωση την παραβίαση της νομοθεσίας λόγω του γεγονότος ότι τα δεδομένα είναι ευαίσθητα.

Στην περίπτωση αυτή το ΓΝ θα υποστεί τις αντίστοιχες συνέπειες που ορίζει ο νόμος για την απώλεια της εμπιστευτικότητας των προσωπικών στοιχείων, οι οποίες περιλαμβάνουν τόσο χρηματικά πρόστιμα όσο και ποινικές συνέπειες.

Αποτίμηση: Με βάση τα παραπάνω, η συνέπεια της αποκάλυψης των στοιχείων αυτών αποτιμάται με βαθμό **τρία (3)**, σε κλίμακα 0-10.

Κατηγορία Επίπτωσης		**Επιπτώσεις στο Νοσοκομείο**	**Βαθμός Αποτίμησης**
Απώλεια Διαθεσιμότητας Δεδομένων	1 ημέρα	Οικονομική Απώλεια	3
Απώλεια Ακεραιότητας Δεδομένων	Αλλοίωση Δεδομένων	Ποινικές Κυρώσεις Καταστροφή καλής φήμης	5
Απώλεια Εμπιστευτικότητας	Αποκάλυψη των δεδομένων σε τρίτους	Ποινικές Κυρώσεις	3

Πίνακας 8:Αποτίμηση Δεδομένων Μισθοδοσίας

¤	**Απώλεια· διαθεσιμότητας¤**	**Απώλεια· ακεραιότητας¤**	**Αποκάλυψη·σε·τρίτους¤**
	1·ημέρα¤	Ολική· καταστροφή¤	Αποκάλυψη·των· δεδομένων·σε·τρίτους¤
Δεδομένα¶ Ασθενών¤	3¤	**5¤**	**6¤**
Δεδομένα· Μισθοδοσίας¤	1¤	3¤	3¤
Δεδομένα· Λογιστηρίου¤	**5¤**	**6¤**	1¤

Πίνακας 9: Συνολική Αποτίμηση

3.10 Αποτίμηση Υλικού

Στη συνέχεια γίνεται αποτίμηση της αξίας των υλικών με βάση τη χρηματική τους αξία σε περίπτωση αντικατάστασης τους.

Περιουσιακό στοιχείο	**Ποσότητα**	**Βαθμός Αποτίμησης**	**Κόστος Αντικατάστασης**
Σταθμός εργασίας	**250**	**4**	1000
Δρομολογητής/Μεταγωγέας	**6**	**4**	5800
Εκτυπωτής	**5**	**2**	1500
Εξυπηρετητής εφαρμογής Μισθοδοσίας	**4**	**2**	4500
Εξυπηρετητής εφαρμογής Πελάτών	**1**	**3**	2200
Εξυπηρετητής Βάσεων Δεδομένων	**2**	**3**	2200

Πίνακας 10: Αποτίμηση Υλικού

3.11 Αποτίμηση Λογισμικού

Για την αποτίμηση του λογισμικού ακολουθήθηκε ο τρόπος αποτίμησης με βάση το κόστος αντικατάστασης τους που φαίνεται ως ακολούθως:

Καταστροφή Λογισμικού	**Συνέπεια για την εταιρεία**	**Βαθμός Αποτίμησης**
Λογισμικό του Συστήματος Ασθενών	Οικονομική Απώλεια	**8**
Λογισμικό του Συστήματος Μισθοδοσίας	Οικονομική Απώλεια	**9**
Λογισμικό του Συστήματος Διαχείρισης Προσωπικού	Οικονομική Απώλεια	**4**

Πίνακας 11: Αποτίμηση Λογισμικού

3.12 Αξιολόγηση Επιπτώσεων

3.12.1 Αναγνώριση των απειλών στο ΠΣΓΝ

Παρακάτω, φαίνονται τα περιουσιακά στοιχεία:

Απειλή	Απαιτήσεις σχετικές με ασφάλεια
Πλαστοπροσωπία	Αυθεντικοποίηση
Μη εξουσιοδοτημένη χρήση εφαρμογής	Έλεγχος Εξουσιοδότησης
Εισαγωγή Ιομορφικού Λογισμικού	Μηχανισμοί πρόληψης εισαγωγής Ιομορφικού Λογισμικού
Διήθηση – Παρεμβολές Επικοινωνιών	Εμπιστευτικότητα - Ακεραιότητα - Διαθεσιμότητα
Βλάβη Εξυπηρετητή	Τεχνική Υποστήριξη
Βλάβη Εξυπηρετητή Διαχείρισης Δικτύου ή Συσκευής ή Πύλης Δικτύου	Τεχνική Υποστήριξη
Λάθος Χειρισμού ή Χρήστη	Εκπαίδευση Προσωπικού
Διακοπή Ηλεκτροδότησης	Τροφοδοτικά Αδιάλειπτης Λειτουργίας
Βλάβη Κλιματισμού	Τεχνική Υποστήριξη
Αστοχία Λογισμικού Συστήματος και Λογισμικού Δικτύου	Ποιότητα Λογισμικού
Αστοχία Λογισμικού Εφαρμογών	Δοκιμές και Ποιότητα Εφαρμογών
Σφάλμα Συντήρησης Υλικού	Τεχνική Υποστήριξη
Σφάλμα Συντήρησης Λογισμικού	Τεχνική Υποστήριξη
Φωτιά	Μηχανισμοί Πρόληψης Πυρκαγιάς
Πλημμύρα	Μηχανισμοί Πρόληψης Πλημμύρας
Φυσική Καταστροφή	Σχέδιο Συνέχισης Λειτουργιών
Έλλειψη Προσωπικού	Σχέδιο Συνέχισης Λειτουργιών
Κλοπή	Προστασία ενάντια σε κλοπές
Ηθελημένη πρόκληση βλάβης - βανδαλισμός	Έλεγχος Προσωπικού

Πίνακας 12: Απειλές στο ΠΣΓΝ

Για την υλοποίηση της μεθοδολογίας Magerit δημιουργήθηκαν πολλά σενάρια που λαμβάνουν υπόψη τις απειλές σε όλα τα περιουσιακά στοιχεία του ΠΣ-ΓΝ. Στα περισσότερα από τα σενάρια αυτά η απειλή ενδέχεται να εμφανιστεί περισσότερες από μια φορές και σε διαφορετικό βαθμό.

3.12.2 Αξιολόγηση των απειλών στο ΠΣΓΝ

3.12.2.1 Μεθοδολογία

Όταν ένα περιουσιακό στοιχείο είναι ευπαθές δεν σημαίνει ότι επηρεάζονται όλες οι διαστάσεις ασφαλείας του στον ίδιο βαθμό. Πρέπει λοιπόν να καθοριστεί ότι η απειλή μπορεί να βλάψει ένα περιουσιακό στοιχείο, με το ότι η έκθεση του στοιχείου σε αυτήν έχει δύο παραμέτρους:

-Ζημία(Degradation) :Το ποσό της ζημίας που γίνεται στην αξία του περιουσιακού στοιχείου.

-Πιθανότητα(Likelihood): Πόσο συχνά συμβαίνει η απειλή.

Όταν οι απειλές δεν είναι εσκεμμένες αρκεί να γνωρίζουμε το μέρος της φυσικής ζημίας του περιουσιακού στοιχείου για να μετρήσουμε την απώλεια της αξίας. Σε περίπτωση εσκεμμένης πρόθεσης, ο επιτιθέμενος μπορεί να προκαλέσει μεγαλύτερη ζημία έμμεσα.

Η πιθανότητα εμφάνισης είναι πιο πολύπλοκη. Καμιά φορά μοντελοποιείται ποσοτικά με βάση την ακόλουθη κλίμακα.

VH	Πολύ υψηλή	Σχεδόν Βέβαιη	Εύκολα
H	Υψηλή	Πολύ υψηλή	Μεσαία
M	Μεσαία	Πιθανή	Δύσκολα
L	low	Μη πιθανή	Πολύ δύσκολη
VL	Πολύ χαμηλή	Πολύ σπάνια	Εξαιρετικά δύσκολη

Πίνακας 13: Τιμές ζημίας(Degradation)

Όταν ένα περιουσιακό στοιχείο υποστεί μια απειλή, χάνει μέρους της αξίας του. Η ζημία αυτή μπορεί να είναι ανάμεσα από 0% έως 100% και λαμβάνει τιμές από 0.0 έως 1.0. Καμιά φορά, η πιθανότητα είναι αριθμητικά μοντελοποιημένη ως ποσοστό συμβάντων. Είναι σύνηθες, να χρησιμοποιείται ο ένας χρόνος ως αναφορά, έτσι ώστε η εμφάνιση να γίνεται ως ετήσιο ποσό ως μέτρηση της πιθανότητας ότι κάτι συμβαίνει.

Τυπικές τιμές είναι:

100	Πολύ συχνά	Καθημερινά
10	Συχνά	Μηνιαία
1	Κανονικά	Ετησίως
1/10	Όχι συχνά	Κάθε λίγα χρόνια

Πίνακας 14 Τιμές πιθανότητας(Likelihood)

Η ακόλουθη κλίμακα είναι ένα εργαλείο για να βαθμολογήσουμε τα περιουσιακά στοιχεία, το μέγεθος της επίπτωσης.

		degradation		
impact		1%	10%	100%
value	VH	M	H	VH
	H	L	M	H
	M	VL	L	M
	L	VL	VL	L
	VL	VL	VL	VL

Πίνακας 15: Τιμές επίπτωσης(Impact)

- **VL:** very low
- **L:** low
- **M:** medium
- **H:** high
- **VH:** very high

Υπόμνημα

3.12.2.2 Καθορισμός της πιθανής επίπτωσης(potential impact).

Η επίπτωση είναι η μέτρηση της ζημίας ανά περιουσιακό στοιχείο που προκύπτει από την εμφάνιση της απειλής. Γνωρίζοντας την αξία των περιουσιακών στοιχείων (για διάφορες απαιτήσεις ασφαλείας) και την απώλεια που προκαλείται από τις απειλές, την επίπτωση τους πάνω στο σύστημα μπορεί αυτή άμεσα να εξαχθεί ως συμπέρασμα.

Αρχικά, υπολογίζεται η πιθανή (potential) επίπτωση ανά περιουσιακό στοιχείο η οποία δεν λαμβάνει υπόψη τα υφιστάμενα μέτρα ασφαλείας τα οποία έχουμε καθορίσει και αξιολογήσει στο προηγούμενο στάδιο.

3.12.2.3 Συνολική Επίπτωση(Accumulated impact).

Η **συνολική επίπτωση** μετριέται για κάθε περιουσιακό στοιχείο, για κάθε απειλή και για κάθε διάσταση αξιολόγησης.

Οσον αφορά ένα περιουσιακό στοιχείο μετράμε την συνολική αξία (την δική του επιπλέον της συνολικής αξίας των περιουσιακών στοιχείων που εξαρτώνται από αυτό). Η συνολική αξία υπολογίζεται ως η **υψηλότερη αξία των τιμών** που περιλαμβάνονται μεταξύ του περιουσιακού στοιχείου που αποτιμούμε και όλων αυτών που εξαρτώνται από πάνω στη σειρά και τις συνολικές απειλές στις οποίες εκτίθεται.

Η **συνολική επίπτωση της απειλής** σε ένα περιουσιακό στοιχείο είναι η μέτρηση της συνολικής απώλειας της αξίας. Αν ένα περιουσιακό στοιχείο έχει συνολική αξία vx και η τιμή της μείωσης είναι **d** τότε η τιμή της συνολικής επίπτωσης της απειλής είναι

$$\textbf{Επίπτωση} = V_{round}(x_x\ d).$$

Όσο μεγαλύτερη είναι η συνολική αποτίμηση ενός περιουσιακού στοιχείου και η ζημία (degradation) του επιτιθέμενου περιουσιακού στοιχείου τόσο μεγαλύτερη είναι η επίπτωση. Πρέπει να λάβουμε υπ' όψη τις αλληλεξαρτήσεις μεταξύ των περιουσιακών στοιχείων. Συχνά, η αξία του πληροφοριακού συστήματος είναι στις υπηρεσίες που παρέχει και στα δεδομένα που χειρίζεται ενώ οι απειλές συνήθως εμφανίζονται στα αλληλοεξαρτώμενα περιουσιακά στοιχεία.

3.12.2.4 Ανακλώμενη επίπτωση(Deflected Impact)

Η ανακλώμενη (deflected) επίπτωση υπολογίζεται για κάθε περιουσιακό στοιχείο, για κάθε απειλή και για κάθε απαίτηση ασφαλείας έχοντας ως λειτουργία την πραγματική αξία και την ζημία (degradation) που έχει προκληθεί.

Αν ένα περιουσιακό στοιχείο Α εξαρτάται από ένα περιουσιακό στοιχείο Β, οι απειλές του Β θα επηρεάσουν το στοιχείο Α. Εάν το Β υπόκειται μια μείωση "d", αυτή θα συμβεί και στο "Α" και η επίπτωση στο Α θα είναι η απώλεια της βασικής αξίας. Εάν η τιμή του Α είναι «V» τότε η τιμή της επίπτωσης είναι :

$$\textbf{Επίπτωση} = v_x\ d_x\ \textbf{degree(AB)}$$

Η ανακλώμενη επίπτωση υπολογίζεται για κάθε περιουσιακό στοιχείο.

3.12.2.5 Καθορισμός της εναπομείνασας επίπτωσης(Residual impact).

Υπολογίζεται η εναπομείνασα επίπτωση ανά περιουσιακό στοιχείο λαμβάνοντας υπόψη τα υφιστάμενα μέτρα ασφαλείας του συστήματος. Ο υπολογισμός γίνεται με βάση τη μεθοδολογία Magerit.

3.12.2.6 Αποτελέσματα Αποτίμησης Απειλών.

Για την αξιολόγηση των απειλών απαντήθηκαν σενάρια κατόπιν συνεντεύξεων. Η διαδικασία που διεξήχθη ολοκληρώθηκε σε αρκετές συναντήσεις με τους υπεύθυνους πληροφορικής.

Αρχικά, επιλέξαμε από τις **προτεινόμενες απειλές** τις πιο κατάλληλες για την περίπτωση του ΓΝ, κατόπιν από το μενού των επιλογών opitons επιλέξαμε να εισάγουμε χειροκίνητα τις τιμές αποτίμησης των απειλών και όχι αυτόματα όπως φαίνεται από τις παραμέτρους της κάτωθι εικόνας. Σύμφωνα με τις προεπιλεγμένες παραμέτρους των τιμών για το αρχείο **threats.tsv** το οποίο έχει στοιχεία για την αποτίμηση των απειλών, της συχνότητας για κάθε απαίτηση ασφαλείας, για κάθε περιουσιακό στοιχείο. Δηλαδή, για παράδειγμα για την απειλή E2 με συχνότητα 1.0, εφαρμόζεται η απαίτηση ασφαλείας D με ζημία 20%, όπως αυτά αντιστοιχούν στο security domain:base που επιλέξαμε ως ακολούθως:

threats.tsv	meaning
<?xml version="1.0" encoding="UTF-8" ?> <threat-standard-values> <family F="HW"> <threat Z="E.2" f="1.0" s="6h"> <set D="D" deg="0.2"/> <set D="I" deg="0.2"/> <set D="C" deg="0.2"/> </threat> <threat Z="E.23" f="1.0" s="1d"> <set D="D" deg="0.1"/> </threat> <threat Z="E.24" f="10.0" s="30m"> <set D="D" deg="0.5"/> </threat> <threat Z="E.25" f="1.0" s="2d"> <set D="D" deg="1.0"/> <set D="C" deg="0.5"/> </threat> <threat Z="A.6" f="1.0"> <set D="I" deg="0.1"/> <set D="C" deg="0.5"/> </threat>	format: XML for every asset of class HW … apply threat E.2 with frequency 1.0 apply to dimension D, degradation 20% … and so on … please, notice that security dimensions are in Spanish D for availability I for integrity C for confidentiality A for authenticity T for accountability

Εικόνα12: Βαθμολογία Απειλών

Πιο αναλυτικά φαίνεται η αντιστοιχία στον ακόλουθο Πίνακα:

applicable	family	threat	likelihood	step	D=D	D=I	D=C	D=A	D=T	D=V
	arch.ip	E.15	1			10%				
	arch.ip	E.18	1	1d	10%					
	arch.ip	E.19	1				10%			
	arch.ip	A.5	1			50%	50%	50%		
	arch.ip	A.11	1			50%	50%			
	arch.ip	A.15	1			50%				
	arch.ip	A.18	1	5d	50%					
	arch.ip	A.19	1				50%			
	D	E.1	10	2h	10%	10%	10%			
	D	E.2	1	6h	20%	20%	20%			
	D	E.15	1			1%				
	D	E.18	1	1d	1%					
	D	E.19	1				10%			
	D	A.5	10			10%	50%	100%		
	D	A.6	10	1d	1%	10%	50%			
	D	A.11	100			10%	50%			
	D	A.15	10			100%				
	D	A.18	10	2d	50%					
	D	A.19	10				100%			
	D.conf	E.4	1			1%				

Πίνακας 17: Βαθμολογία Απειλών

Επίσης, κατεβάσαμε από την ιστοσελίδα του NIST https://nvd.nist.gov τα αρχεία **CVE-2015-5434, CVE-2015-6860** με τις ευπάθειες. Εισάγαμε τα αρχεία αυτά με τις τιμές της αποτίμησης των ευπαθειών στο μενού τεχνικές ευπάθειες(cve) για το υλικό των υπολογιστών(server, compaqproliantml370,personal computer) του υπό ανάλυση συστήματος. Βαθμός ευπάθειας είναι πόσο εύκολα μπορεί να συμβεί η χειρότερη περίπτωση σε ένα περιουσιακό στοιχείο.

Συγκεντρωτικά, τα αποτελέσματα της αποτίμησης των απειλών φαίνονται στο **Παράρτημα Δ**.

Τα συνοπτικά αποτελέσματα από τη διαδικασία αυτή της αξιολόγησης των απειλών φαίνονται ακολούθως:

Απειλή	Περιουσιακό Στοιχείο	Πιθανότητα Απειλής
Πλαστοπροσωπία από Εσωτερικούς Χρήστες	Λογισμικό του Συστήματος Ασθενών	Πολύ Υψηλή
	Λογισμικό του Συστήματος Μισθοδοσίας	Πολύ Υψηλή
	Λογισμικό του Συστήματος Διαχείρισης Προσωπικού	Μέτρια
Πλαστοπροσωπία από Παρόχους Υπηρεσιών	Λογισμικό του Συστήματος Ασθενών	Πολύ Χαμηλή
	Λογισμικό του Συστήματος Μισθοδοσίας	Πολύ Χαμηλή
	Λογισμικό του Συστήματος Διαχείρισης Προσωπικού	Πολύ Χαμηλή
Πλαστοπροσωπία από Εξωτερικούς Χρήστες	Λογισμικό του Συστήματος Ασθενών	Υψηλή
	Λογισμικό του Συστήματος Μισθοδοσίας (εξυπηρετητής βάσεων δεδομένων)	Υψηλή
	Λογισμικό του Συστήματος Διαχείρισης Προσωπικού	Υψηλή
Διακοπή Ηλεκτροδότησης	Υλικό του Συστήματος Ασθενών	Πολύ Υψηλή
	Υλικό του Συστήματος Μισθοδοσίας	Πολύ Υψηλή
	Υλικό του Συστήματος Διαχείρισης Προσωπικού	Πολύ Υψηλή
Αστοχία Κλιματισμού	Υλικό του Συστήματος Ασθενών	Μέτρια
	Υλικό του Συστήματος Μισθοδοσίας	Υψηλή
	Υλικό του Συστήματος Διαχείρισης Προσωπικού	Υψηλή
Αστοχία Λογισμικού Εφαρμογών	Εξυπηρετητής Εφαρμογής Μισθοδοσίας	Πολύ Υψηλή
	Εφαρμογές Προσωπικού	Πολύ Υψηλή
	Εφαρμογές Ασθενών	Πολύ Υψηλή
Σφάλμα Συντήρησης Υλικού	Υλικό του Συστήματος Ασθενών	Πολύ Υψηλή
	Υλικό του Συστήματος Μισθοδοσίας	Χαμηλή
	Υλικό του Συστήματος Διαχείρισης Προσωπικού	Χαμηλή
Σφάλμα Συντήρησης Λογισμικού	Υλικό του Συστήματος Ασθενών	Χαμηλή
	Υλικό του Συστήματος Μισθοδοσίας	Χαμηλή
	Υλικό του Συστήματος Διαχείρισης Προσωπικού	Χαμηλή
Λάθος Χρήστη	Λογισμικό του Συστήματος Ασθενών	Μεσαία
	Λογισμικό του Συστήματος Μισθοδοσίας (Εξυπηρετητής Βάσεων Δεδομένων)	Μεσαία
	Λογισμικό του Συστήματος Διαχείρισης Προσωπικού	Μεσαία
Φωτιά	Κεντρικό κτήριο	Πολύ Χαμηλή
	Κτήριο 2	Πολύ Χαμηλή
	Κτήριο 3	Πολύ Χαμηλή
Πλημμύρα	Κεντρικό κτήριο	Πολύ Χαμηλή
	Κτήριο 2	Πολύ Χαμηλή
	Κτήριο 3	Πολύ Χαμηλή
Κλοπή από Εσωτερικούς Χρήστες	Σταθμοί Εργασίας	Χαμηλή
	Δρομολογητές (Switches)	Χαμηλή
	Εκτυπωτές	Πολύ Χαμηλή

Πίνακας18: Βαθμολογία Απειλών

3.12.2.7 Σχολιασμός των αποτελεσμάτων

Από τον παραπάνω Πίνακα 18 φαίνεται ότι ορισμένες απειλές είναι πιο σημαντικές σε επίπεδο κρισιμότητας από άλλες.

Οι απειλές με βαθμολογία Υψηλή, Πολύ Υψηλή και άνω πρέπει να ληφθούν σοβαρά υπόψη και να αντιμετωπιστούν κατάλληλα ως οι πιο κρίσιμες. Επειδή όμως οι απειλές με την χαμηλότερη βαθμολογία μπορεί να προκαλέσουν το ευάλωτο σημείο ολόκληρου του ΠΣΓΝ πρέπει να ληφθούν υπόψη σε προτεραιότητα.

Τα σημεία που κρίνονται κρίσιμα στους σταθμούς εργασίας για μια ημέρα είναι τα ακόλουθα:

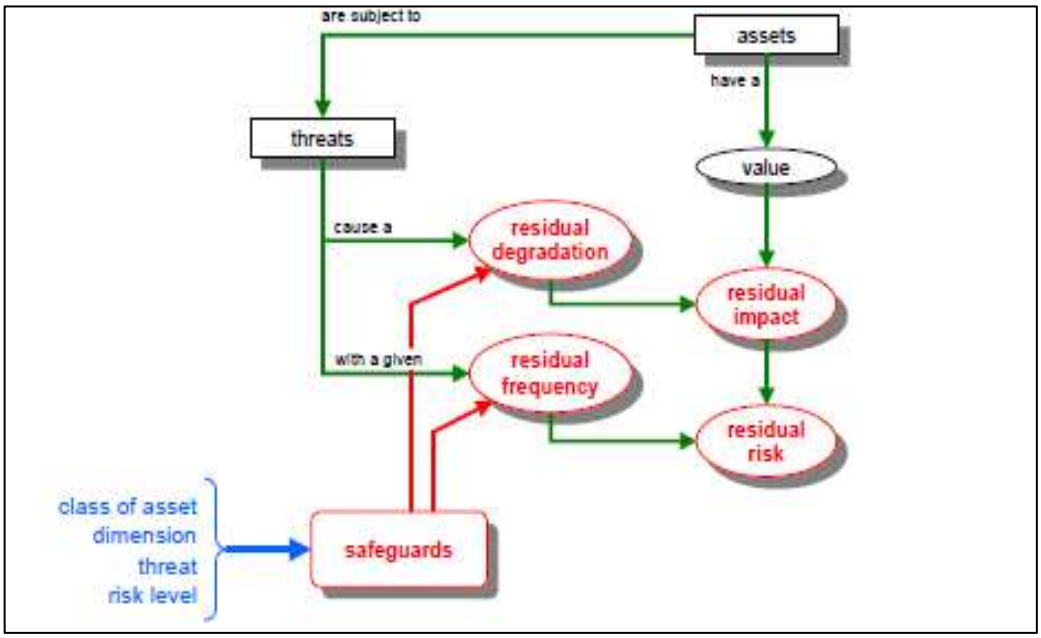
- Ιομορφικού Λογισμικού
- Πλαστοπροσωπία από Εσωτερικούς Χρήστες
- Πλαστοπροσωπία από Εξωτερικούς Χρήστες
- Αστοχία Λογισμικού Συστήματος και Λογισμικού Δικτύου (αφορά την εφαρμογή Μισθοδοσίας)
- Αστοχία Λογισμικού Εφαρμογών
- Λάθος του Χρήστη
- Διακοπή Ηλεκτροδότησης
- Κλοπή εγγράφων ή άλλων αγαθών του ΠΣ (από άτομα εκτός του ΓΝ)

Οι ανωτέρω απειλές βαθμολογήθηκαν με υψηλή βαθμολογία άρα πρέπει να δοθεί μεγάλη προσοχή και προτεραιότητα στην υλοποίηση των μέτρων αντιμετώπισης τους λόγω του γεγονότος ότι έχουν μεγάλο αντίκτυπο στο ΠΣΓΝ. Αυτό όμως δεν θα πρέπει να σημαίνει ότι δεν θα λαμβάνουμε υπόψη και τις υπόλοιπες απειλές. Παρόλο που όλες οι απειλές πρέπει να αντιμετωπίζονται με τη βαρύτητα που τους αναλογεί είναι γνωστό ότι η ισχυρή ασφάλεια του συστήματος είναι όση και η ασφάλεια του αδύναμου σημείου της.

3.13 Υπολογισμός του κινδύνου του ΠΣΓΝ

3.13.1 Μεθοδολογία

Η μεθοδολογία Magerit υπολογίζει την επικινδυνότητα ως ακολούθως:



Εικόνα18: Υπολογισμός Απειλών

Ο κίνδυνος υπολογίζεται ως συνάρτηση της επίπτωσης και της συχνότητας:

Κίνδυνος = (επίπτωση, συχνότητα)

Ο κίνδυνος είναι μια πραγματική τιμή μεγαλύτερη του μηδενός. Οι τιμές είναι σε Ευρώ και η συχνότητα μετράει ετήσια συμβάντα. Εάν 0.1 σημαίνει μια φορά κάθε 10 χρόνια για ένα περιουσιακό στοιχείο που έχει αξία 900.000 τότε ο εκτιμώμενος κίνδυνος θα είναι 900.000χ 0.1=90000.

Η συχνότητα των Απειλών

Η συχνότητα των απειλών περιγράφεται από μια σειρά από συμβολικές τιμές.

Μια απειλή έχει j σημεία συχνότητας ώστε η συνολική συχνότητα να είναι fj.Η συχνότητα μοντελοποιείται από μια απλή κλίμακα.

risk		frequency			
		PF	FN	F	MF
impact	VH	H	VH	VH	VH
	H	M	H	VH	VH
	M	B	M	H	VH
	L	VL	L	M	H
	VL	VL	VL	L	M

- VF: very frequent (daily)
- F: frequent (monthly)
- NF: normal frequency (yearly)
- I: infrequent (every few years)

Πίνακας 19 : Υπολογισμός Κινδύνου

Η υπολογιζόμενη επίπτωση είναι το κόστος που απορρέει από την απειλή και ο στόχος (Target) υπολογίζεται ως ο κίνδυνος για τις ετήσιες απώλειες.

3.13.2 Καθορισμός του θεωρητικού κινδύνου.

Η επικινδυνότητα είναι η μέτρηση της πιθανής ζημίας στο σύστημα. Γνωρίζοντας την επίπτωση των απειλών στα περιουσιακά στοιχεία, ο κίνδυνος μπορεί να υπολογιστεί άμεσα λαμβάνοντας υπ' όψιν τη πιθανότητα εμφάνισης τους. Υψηλή επίπτωση και πολύ υψηλή πιθανότητα παράγει υψηλό κίνδυνο. Ο πιθανός κίνδυνος στον οποίο υπόκειται το σύστημα, λαμβάνει υπόψη την αξία των περιουσιακών στοιχείων και την αξιολόγηση των απειλών αλλά όχι τα αντίμετρα που έχουν χρησιμοποιηθεί.

3.13.3 Καθορισμός του εναπομείναντος (residual) κινδύνου.

Πραγματοποιείται επιλογή των υφιστάμενων μέτρων ασφαλείας με τη δήλωση Εφαρμογής(**Statement of Applicability**) και κατόπιν η αποτίμηση τους. Εν συνεχεία, πραγματοποιείται μια αξιολόγηση της καταλληλότητας των αντίμετρων(**Safeguards**), της ποιότητας εφαρμογής τους, της εκπαίδευσης των χρηστών στη χρήση τους.

Κατόπιν, ο εναπομείναν κίνδυνος λαμβάνει υπόψη την εναπομείνασα επίπτωση και την αποτελεσματικότητα των μέτρων που έχουν υλοποιηθεί. Υπολογίζεται δηλαδή ο κίνδυνος από την εναπομείνασα συχνότητα και την εναπομείνασα επίπτωση.

Εναπομείναντας κίνδυνος = (Εναπομείνασα_επίπτωση, Εναπομείνασα _συχνότητα)

- Λόγω του ότι η ανακλώμενη επίπτωση υπολογίζεται στα περιουσιακά στοιχεία που έχουν αποτιμηθεί με την δική τους τιμή, επιτρέπει τον καθορισμό των συνεπειών σε τεχνικά περιστατικά. Τα αποτελέσματα αυτής της αποτίμησης λοιπόν βοηθάνε καλύτερα τη διοίκηση για τη λήψη κρίσιμων αποφάσεων στην ανάλυση κινδύνων πληροφοριών: ν**α κάνει αποδεκτό ένα συγκεκριμένο επίπεδο κινδύνου.**

3.13.4 Αποτελέσματα Αποτίμησης επικινδυνότητας.

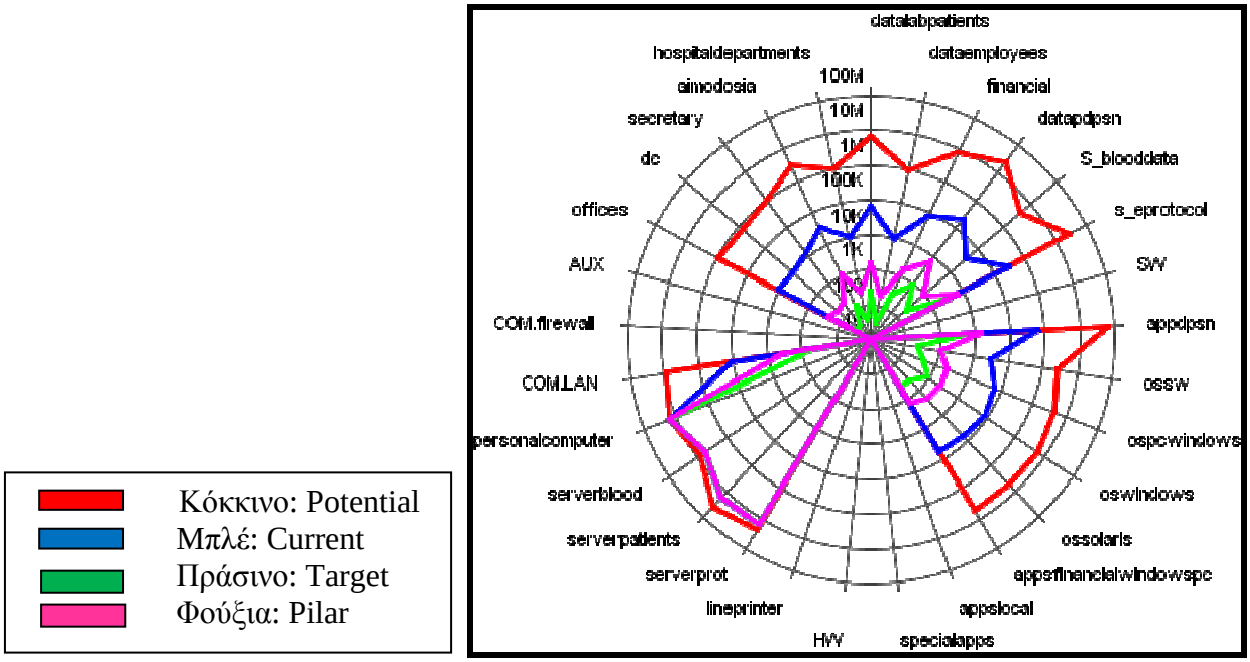
Στον Πίνακα 17 και στην Εικόνα 14 που ακολουθεί φαίνεται η αποτίμηση της επικινδυνότητας για τα κρίσιμα περιουσιακά στοιχεία του ΠΣΓΝ. Κατά τη διαδικασία της ερμηνείας των αποτελεσμάτων έγινε μια προτεραιότητα στα περιουσιακά στοιχεία που υπόκεινται στη μεγαλύτερη επίπτωση και στο μεγαλύτερο κίνδυνο.Το λογισμικό Pilar υπολογίζει αυτόματα τον βαθμό κινδύνου αφού ολοκληρωθούν τα προηγούμενα στάδια αξιολόγησης των περιουσιακών στοιχείων, των απειλών. Το Pilar υπολογίζει αυτόματα τον κίνδυνο ως το ποσό το οποίο πρέπει να ληφθεί υπόψη για τις ετήσιες απώλειες. Στον ακόλουθο πίνακα φαίνεται η αποτίμηση του ανακλώμενου(deflected) κινδύνου σε συνάρτηση με τις απειλές οι οποίες έχουν πιθανότητα **likelihood 10% και η επίπτωση στο Νοσοκομείο είναι 50%.**

Father	Child	Threat	Risk	Current	Target	PILAR
[dataemployees] dataemployees	[appdpsn] appdpsnsolarisml370	[E.2] System / Security administrator errors	2,00E+13	1,68E+11	7,43E+08	4,65E+09
[financial] finlogisticssubcontractor	[s_eprotocol] s_eprotocol	[E.2] System / Security administrator errors	2,00E+13	2,12E+11	2,55E+09	4,38E+09
[dataemployees] dataemployees	[appdpsn] appdpsnsolarisml370	[A.11] Unauthorised access	1,04E+13	1,32E+11	7,13E+08	2,17E+09
[dataemployees] dataemployees	[datapdpsn] datadpsn	[E.2] System / Security administrator errors	1,00E+13	7,87E+10	3,70E+08	2,78E+09
[dataemployees] dataemployees	[appdpsn] appdpsnsolarisml370	[E.2] System / Security administrator errors	4,30E+12	4,41E+10	4,68E+08	9,35E+08
[dataemployees] dataemployees	[appdpsn] appdpsnsolarisml370	[E.2] System / Security administrator errors	4,30E+12	4,05E+10	2,69E+08	8,70E+08
[financial] finlogisticssubcontractor	[s_eprotocol] s_eprotocol	[E.2] System / Security administrator errors	4,30E+12	3,61E+10	1,59E+08	1,02E+09
[financial] finlogisticssubcontractor	[s_eprotocol] s_eprotocol	[E.2] System / Security administrator errors	4,30E+12	4,05E+10	2,69E+08	8,76E+08
[dataemployees] dataemployees	[serverpatients] compaqproliantml370	[A.24] Denial of service	2,43E+12	3,00E+10	1,02E+08	1,08E+09
[dataemployees] dataemployees	[datapdpsn] datadpsn	[E.2] System / Security administrator errors	2,15E+12	1,52E+10	7,67E+07	4,74E+08
[dataemployees] dataemployees	[datapdpsn] datadpsn	[E.2] System / Security administrator errors	2,15E+12	1,52E+10	7,67E+07	4,74E+08
[dataemployees] dataemployees	[datapdpsn] datadpsn	[E.2] System / Security administrator errors	2,15E+12	1,52E+10	7,67E+07	4,75E+08
[dataemployees] dataemployees	[appdpsn] appdpsnsolarisml370	[E.2] System / Security administrator errors	2,15E+12	1,66E+10	7,72E+07	3,94E+08
[dataemployees] dataemployees	[appdpsn] appdpsnsolarisml370	[A.11] Unauthorised access	2,09E+12	2,48E+10	8,46E+07	4,34E+08
[financial] finlogisticssubcontractor	[serverprot] questwinerserver	[A.22] Software manipulation	1,22E+12	1,61E+10	7,70E+07	4,80E+08
[financial] finlogisticssubcontractor	[oswindows] oswindows200serve	[A.22] Software manipulation	1,22E+12	1,52E+10	7,70E+07	6,31E+08
[dataemployees] dataemployees	[serverpatients] compaqproliantml370	[I.6] Power interruption	1,05E+12	1,37E+10	4,67E+07	3,65E+08
[dataemployees] dataemployees	[aimodosia] workingroomaimodosia	[A.27] Enemy over-run	1,00E+12	1,30E+10	4,44E+07	5,63E+08
[dataemployees] dataemployees	[ossolaris] solaris	[A.8] Malware diffusion	9,70E+11	1,05E+10	3,58E+07	1,33E+08
[dataemployees] dataemployees	[appsfinancialwindowspc] logisticsexternalpatients	[A.8] Malware diffusion	9,70E+11	1,05E+10	3,58E+07	1,33E+08
[financial] finlogisticssubcontractor	[serverprot] questwinerserver	[A.8] Malware diffusion	9,70E+11	1,05E+10	3,57E+07	1,48E+08
[financial] finlogisticssubcontractor	[oswindows] oswindows200server	[A.8] Malware diffusion	9,70E+11	1,05E+10	3,58E+07	1,33E+08
[dataemployees] dataemployees	[serverpatients] compaqproliantml370	[E.25] Equipment loss	1,15E+11	1,48E+09	5,96E+06	4,47E+07
[dataemployees] dataemployees	[dc]	[A.27] Enemy over-	1,00E+11	1,30E+09	4,44E+06	5,63E+07

	datacenterpliroforikhsorganwsis	run				
[dataemployees] dataemployees	[offices] workingroomisthodosias	[A.27] Enemy over-run	1,00E+11	1,30E+09	4,44E+06	5,63E+07
[financial] finlogisticssubcontractor	[s_eprotocol] s_eprotocol	[E.2] System / Security administrator errors	1,00E+11	7,70E+08	3,57E+06	1,95E+07
[dataemployees] dataemployees	[hospitaldepartments] hospitaldepartments	[A.27] Enemy over-run	1,00E+10	1,30E+08	0,00E+00	5,65E+06
[dataemployees] dataemployees	[hospitaldepartments] hospitaldepartments	[N.1] Fire	1,00E+10	1,31E+08	0,00E+00	5,06E+06
[dataemployees] dataemployees	[aimodosia] workingroomaimodosia	[N.2] Water	1,00E+10	1,77E+08	0,00E+00	5,50E+06
[dataemployees] dataemployees	[aimodosia] workingroomaimodosia	[N.1] Fire	1,00E+10	1,31E+08	0,00E+00	5,06E+06

Πίνακας 17: Συνολικός Κίνδυνος

Αναλυτικά, το σύνολο της αποτίμησης της ανακλώμενης επικινδυνότητας πραγματοποιήθηκε για πιθανότητα (likelihood) 10% και επίπτωση 10%. Η αποτίμηση των απειλών για τα συγκεκριμένα αγαθά φαίνεται στο **Παράρτημα Ε.**



Εικόνα14: Ανακλώμενη Επικινδυνότητα

1. Ο κίνδυνος υπολογίστηκε συνολικά υπό συγκεκριμένες συνθήκες [12],[13],[14],[15],16],[17],[18], [19], [20], [21]:

2. Σύμφωνα με τη μεθοδολογία Magerit ο ανακλώμενος κίνδυνος υπολογίστηκε σε διαφορετικά περιουσιακά στοιχεία.

3. Υπολογίστηκε ο συνολικός κίνδυνος των περιουσιακών στοιχείων που δεν έχουν αλληλεξάρτηση και τίποτα κοινό με υψηλότερα στην ιεραρχία των εξαρτήσεων περιουσιακά στοιχεία.

4. Υπολογίστηκε ο κίνδυνος προερχόμενος από διαφορετικές απειλές στο ίδιο περιουσιακό στοιχείο όπως επίσης και ο κίνδυνος μιας απειλής με διαφορετικές απαιτήσεις ασφαλείας.

5. Δεν αθροίστηκε ο συνολικός κίνδυνος από εξαρτώμενα περιουσιακά στοιχεία.

3.13.5 Σχολιασμός των αποτελεσμάτων

.Ο εναπομένων βαθμός της επικινδυνότητας υποδεικνύει ποιά περιουσιακά στοιχεία πρέπει να προστατευθούν λαμβάνοντας υπόψη τα υφιστάμενα μέτρα στο πληροφοριακό σύστημα. Ο ανακλώμενος κίνδυνος έχει λάβει υπόψη του τις αλληλεξαρτήσεις μεταξύ του κάθε κρίσιμου περιουσιακού στοιχείου και αυτών που εξαρτώνται από αυτό. Αυτό σημαίνει ότι, κάποιο περιουσιακό στοιχείο παραμένει με υψηλό βαθμό επικινδυνότητας και δεν αντιμετωπίζεται ικανοποιητικά από τα υφιστάμενα μέτρα προστασίας. Επειδή, το Νοσοκομείο δεν είχε όλους τους πόρους να εξετάσει όλους τους κινδύνους προσδιορίστηκαν κάποιοι κίνδυνοι να εξεταστούν σε μεγαλύτερο βαθμό και περισσότερο. Η βαθμολογία του κινδύνου είναι ενδεικτική επειδή έχει υπολογιστεί με υποκειμενικό τρόπο αλλά είναι πολύ χρήσιμη για το ποιες προτεραιότητες θα πρέπει να δοθούν στην αντιμετώπιση των κινδύνων.

Η αποτίμηση έχει λάβει υπ' όψιν την συνολική αποτίμηση όλων των περιουσιακών στοιχείων που αλληλοεξαρτώνται μεταξύ τους, και στα μέτρα ασφαλείας.

3.14. Αντίμετρα

3.14.1Μεθοδολογία

Η Ανάλυση Επικινδυνότητας των Πληροφοριακών Συστημάτων του ΓΝ, τα αποτελέσματα της οποίας παρουσιάστηκαν στο προηγούμενο κεφάλαιο, καταδεικνύει τη δυνατότητα να εντοπιστούν οι τομείς που απαιτούν τη λήψη μέτρων προστασίας - αντιμέτρων και να προσδιοριστεί το επίπεδο προστασίας που απαιτείται. Έτσι επιλέχθηκε μια στρατηγική για να μειωθεί η επίπτωση και ο κίνδυνος και καθορίστηκαν τα κατάλληλα αντίμετρα για τον παραπάνω στόχο. Καθορίστηκε η ποιότητα που απαιτούν αυτά τα αντίμετρα και **σχεδιάστηκε ένα *Σχέδιο Ασφάλειας* για την μείωση της επίπτωσης και του κινδύνου σε ανεκτά επίπεδα το σύνολο των αντίμετρων(μέτρων προστασίας) και την Πολιτική Ασφάλειας**.

Για την διαχείριση κινδύνου πληροφοριών στο Νοσοκομείο, ακολουθήθηκε η μεθοδολογία MAGERIT για την λήψη αποφάσεων.

Η δεξαμενή των μέτρων είναι το ISO27001 και το λογισμικό προσφέρει τη δυνατότητα να επιλέγονται ποια μέτρα εφαρμόζονται στη συγκεκριμένη διαχείριση κινδύνων με την Δήλωση Εφαρμοσιμότητας(Statement of Applicability). Επίσης, υπάρχει μια προτεινόμενη βαθμολογία για προτεραιότητα που δηλώνει την κρισιμότητα των αντίμετρων αυτών(Safeguard Evaluation) που παρουσιάζονται στο Παράρτημα ΣΤ σύμφωνα με την οποία επιλέξαμε την υφιστάμενη κατάσταση της εφαρμογής των αντίμετρων και του στόχου του επιπέδου στο οποίο θέλουμε να φτάσουμε. Αυτό μας βοήθησε να υπολογίσουμε τον εναπομείναντα κίνδυνο. Το γεγονός ότι **το λογισμικό περιλαμβάνει τα επίπεδα ωριμότητας** είναι σημαντικό για τον προγραμματισμό των χρονοδιαγραμμάτων υοποίησης του έργου.

Σύμφωνα με αυτήν, οι επιπτώσεις και οι κίνδυνοι που εκτίθεται το σύστημα καθορίζουν έναν αριθμό αποφάσεων εξαρτώμενο από πολλούς παράγοντες. Λάβαμε υπόψη τις νομικές υποχρεώσεις στις οποίες υπόκειται το Νοσοκομείο, που επιβάλλονται από εσωτερικούς κανονισμούς, και από συμβόλαια. Επίσης, στη φάση της διαχείρισης επικινδυνότητας θεωρήθηκε ότι **το Νοσοκομείο πρέπει να λάβει υπόψη του ορισμένες επιπτώσεις για την δημόσια εικόνα του (θέματα φήμης) εσωτερικής πολιτικής, σχέσεις με τους υπαλλήλους, την ικανότητα να προσλάβουν ικανό προσωπικό,** κλπ.

Ως προτεραιότητα, το σύστημα πρέπει να έλαβε υπόψη του τα προληπτικά αντίμετρα που διασφαλίζουν ότι η απειλή δεν θα συμβεί ή ότι η ζημία είναι μικρή. Έτσι αυτά μπορούν να αποτρέψουν περιστατικά ή επιθέσεις. **Το κόστος ανά ώρα υπολογίζεται για κάθε σενάριο. Ελήφθησαν υπόψη ο εναπομείναν κίνδυνος, το κόστος των αντίμετρων, το ετήσιο κόστος συντήρησης των αντίμετρων, τη βελτίωση της παραγωγικότητας.** Η αξιολόγηση για την εφαρμογή ή όχι των αντίμετρων προκύπτει από ένα συνδυασμό του τύπου των περιουσιακών στοιχείων, των απειλών στις οποίες εκτίθεται, της απαίτησης ασφαλείας που πρέπει να αντιμετωπίσει και της αποτίμησης του κινδύνου.

Η έννοια του σοβαρού καθορίστηκε ως **ότι απαιτεί προσοχή, ότι έχει ουσία** επειδή απαιτεί περαιτέρω εξέταση και **ότι δεν απαιτεί άλλες ενέργειες** για να μετρηθεί ο κίνδυνος.Τα ανωτέρω είναι σημαντικά, για να καθοριστεί ποιό σημείο κινδύνου είναι ποιό σημαντικό, και ποιό είναι κρίσιμο από την άποψη ότι απαιτεί επείγουσα προσοχή. Η **ταξινόμηση των κινδύνων** καθόρισε τη σχετική προτεραιότητα των διαφορετικών πράξεων.

Η επικινδυνότητα ελήφθη υπόψη με προσοχή και τεκμηριωμένα. **Οι λόγοι** που καθιστούν **δυνατή την αποδοχή** είναι οι εξής: η εναπομείνασα επίπτωση και ο εναπομείναν κίνδυνος έχει υπολογιστεί και **το κόστος των μέτρων χρονικά** είναι δυσανάλογο εάν συγκριθεί με την εναπομείνασα επίπτωση και επικινδυνότητα.

Η αποτελεσματικότητα του σχεδίου ασφάλειας προϋποθέτει την συνεχή, πιστή και συνολική εφαρμογή του. Τα αντίμετρα που προτείνονται βρίσκονται σε αλληλεξάρτηση και η αποτελεσματικότητα ενός αντιμέτρου είναι συνάρτηση της ορθής υλοποίησης ενός άλλου. Για παράδειγμα, **κανένα τεχνικό αντίμετρο δεν πρόκειται να αποδώσει τα αναμενόμενα αποτελέσματα, χωρίς την παράλληλη εφαρμογή μιας κατάλληλης οργάνωσης και ενός προγράμματος εκπαίδευσης και ενημέρωσης.**

Η **επιλογή μόνο των πιο "κρίσιμων" ή "άμεσης προτεραιότητας" αντίμετρων ενέχει σοβαρούς κινδύνους τα στοιχεία στα οποία βασίζονται** να είναι απλά στατιστικά δεδομένα τα οποία μπορεί να είναι γνωστά στον επιτιθέμενο. Τότε θα επιλέξει τρόπους επίθεσης που αντιστοιχούν σε στατιστικά λιγότερο πιθανές απειλές. Έτσι, αμέσως η πιθανότητα εμφάνισης ή όχι των απειλών διαφοροποιείται.

3.14.2 Αντίμετρα για το ΠΣΓΝ

Στη συνέχεια αναφέρονται, ομαδοποιημένα, τα σημαντικότερα σημεία του Σχεδίου Ασφάλειας. Η λεπτομερής αξιολόγηση των αντίμετρων παρουσιάζεται στο **Παράρτημα Ζ.**

Όλα τα προτεινόμενα αντίμετρα έχουν στόχο να προσφέρουν υψηλότερο όφελος σε σχέση με το κόστος εφαρμογής τους *(cost-effective)*. **Πολλά από τα μέτρα είναι χαμηλού κόστους και πραγματοποιούνται με απλές ρυθμίσεις και αλλαγές στην οργάνωση.** Επίσης, σύμφωνα με την καλή πρακτική τα αντίμετρα κατά την υλοποίηση τους θα πρέπει να είναι αδιαφανή στο χρήστη.

Ως σημαντικότερα από τα προτεινόμενα αντίμετρα θεωρούνται: η υλοποίηση ενός οργανωτικού σχήματος ασφαλείας με **την ανάθεση του ρόλου του Υπεύθυνου Ασφάλειας ΠΣ σε στέλεχος με τα κατάλληλα προσόντα, η υιοθέτηση της Πολιτικής Ασφάλειας ΠΣ και του Κώδικα Δεοντολογίας, η διαμόρφωση κατάλληλου χώρου στέγασης των βασικών υπολογιστικών συστημάτων και η κατάλληλη εκπαίδευση – κατάρτιση του προσωπικού.** Στα μέτρα με άμεση προτεραιότητα περιλαμβάνεται η αποδοχή της Πολιτικής Ασφάλειας ΠΣ από τη Διοίκηση του ΓΝ, καθώς και η εφαρμογή του Κώδικα Δεοντολογίας. Επίσης, ιδιαίτερα κρίσιμη είναι **η διαμόρφωση κατάλληλου χώρου εξυπηρετητών *(server room)* για τις βασικές εφαρμογές του ΠΣ του ΓΝ** και ειδικότερα για τους εξυπηρετητές των εφαρμογών ΠΣ του ΓΝ και της Μισθοδοσίας. Απαιτείται επίσης, **η ανάπτυξη διαδικασιών εσωτερικής και εξωτερικής εποπτείας και ελέγχου *(audit)*.** Είναι σημαντικό να διασφαλιστεί **η συνέχιση λειτουργίας και η αντιμετώπιση έκτακτων περιστατικών και ιδιαίτερα στη λήψη και διαχείριση των εφεδρικών αντιγράφων δεδομένων**.

Επιπλέον, απαιτείται **η υλοποίηση των αντίμετρων της φυσικής ασφάλειας των χώρων όπου φυλάσσονται αρχεία με ιατρικά δεδομένα και γενικότερα ευαίσθητα προσωπικά δεδομένα**, όπως τα βιβλία που τηρούν οι ιατροί στις κλινικές.

Πολύ σημαντικά διοικητικά-οργανωτικά μέτρα αποτελούν, **η ανάπτυξη και εκπόνηση προγράμματος εκπαίδευσης και ενημέρωσης σε ζητήματα χρήσης των ΠΣ για το προσωπικό του ΓΝ** και η εκπαίδευση του προσωπικού του Τμήματος Πληροφορικής και Οργάνωσης σε θέματα ασφαλείας.

Το ΓΝ οφείλει να συμμορφώνεται με τη νομοθεσία περί προστασίας προσωπικών δεδομένων (Νόμος 2472/97).

Τα προσωπικά δεδομένα που επεξεργάζονται τα ΠΣ του Νοσοκομείου, όπως τα δεδομένα που αφορούν ασθενείς, νοσηλευόμενους και το προσωπικό του ΓΝ, να τυγχάνουν επεξεργασίας σύμφωνα με το Ν. 2472/97 και τις οδηγίες που έχει εκδώσει η Αρχή Προστασίας Προσωπικών Δεδομένων Υπεύθυνος Ασφάλειας ΠΣ είναι υπεύθυνος για το χαρακτηρισμό κάθε ομάδας δεδομένων, ως «δεδομένα προσωπικού χαρακτήρα», «ευαίσθητα προσωπικά δεδομένα» ή «δεδομένα μη-προσωπικού χαρακτήρα», σύμφωνα με τα οριζόμενα στο Ν.2472/97.

Τα προτεινόμενα Μέτρα Προστασίας εντάσσονται στις ακόλουθες γενικές κατηγορίες και αναλυτικά φαίνονται στο **Παράρτημα Η:**

Πίνακας 19: Μέτρα Προστασίας

Αρ.Μέτρου	Πολιτική Ασφαλείας και Κώδικας Δεοντολογίας
4.2	Συμμόρφωση με Νομοθετικό και Κανονιστικό Πλαίσιο
4.13	Οργανωτική Υποδομή
4.11	Προσωπικό
A5	Εκπαίδευση στην Ασφάλεια Πληροφοριακών Συστημάτων
	Εποπτεία και Έλεγχος
4.1	Διαχείριση Περιστατικών Παραβίασης της Ασφάλειας Πληροφοριακών Συστημάτων
4.1	Ταυτοποίηση και Αυθεντικοποίηση
4.1	Έλεγχος Προσπέλασης και Χρήσης Πόρων
4.2	Διαχείριση Εμπιστευτικών Δεδομένων
4.14	Ανάδοχοι Εργασιών Ανάπτυξης και Συντήρησης
4.5	Προστασία Λογισμικού
	Διαχείριση Ασφάλειας Δικτύου
	Προστασία από Ιομορφικό Λογισμικό
4.4	Ασφαλής Χρήση Ηλεκτρονικού Ταχυδρομείου και Πλοήγηση στο Διαδίκτυο
4.6	Ασφάλεια Εξοπλισμού
4.9	Φυσική Ασφάλεια Κτηριακών Εγκαταστάσεων
4,2	Προστασία Αρχείων Εγγράφων και Φακέλων
4.9	Προστασία από Κλοπή Εξοπλισμού
4.9	Προστασία από Πυρκαγιά
4.9	Προστασία από Πλημμύρα και Ακραία Καιρικά Φαινόμενα
4.12	Σχέδιο Αντιμετώπισης Έκτακτων Αναγκών
4.7	Προστασία Επικοινωνιών
	Διαχείριση κρυπτογραφικών κλειδών

3.15 Επίλογος

3.15.1 Γενικά

Η παρούσα μελέτη ανάλυσης κινδύνων στο ΠΣ ΓΝ διερεύνησε το βαθμό επικινδυνότητας των κρίσιμων περιουσιακών στοιχείων του ΠΣ του ΓΝ και ανέδειξε μέτρα ασφαλείας για την αντιμετώπιση τους στα πλαίσια της διαχείρισης της επικινδυνότητας.

Σκοπός της εργασίας ήταν η ανάλυση και αποτίμηση συγκεκριμένων απειλών του ΠΣ του ΓΝ ώστε να υπολογιστεί **με ποσοτικούς όρους ο βαθμός επικινδυνότητας για κάθε συνδυασμό απειλή-αγαθό.** Μετά την υλοποίηση του αρχικού σταδίου απαιτείται ο καθορισμός ενεργειών έτσι ώστε να επιτευχθεί το επίπεδο ωριμότητας που έχει τεθεί ως στόχος και να προστατευτούν τα ΠΣ του ΓΝ στον επιθυμητό βαθμό ασφαλείας τους.

Τα αποτελέσματα αυτά παρήγαγαν τις διαδικασίες ασφαλείας οι οποίες στο πλαίσιο μιας αποτελεσματικής στρατηγικής συμπεριλαμβάνονται στη δημιουργία του **σχεδίου ασφαλείας**. Τα αντίμετρα ασφαλείας αυτά που παρήχθησαν από την διαχείριση επικινδυνότητας μαζί με την πολιτική ασφαλείας του ΓΝ δημιουργούν το σχέδιο ασφαλείας το οποίο πρέπει να εφαρμοστεί σωστά ώστε να επιτύχει το στόχο του.

3.15.2 Προτάσεις Βελτίωσης.

3.15.2.1 Συλλογή Δεδομένων για χρήση στο εργαλείο Pilar.

Η μελέτη ανέδειξε σημαντικά προβλήματα και ελλείψεις ασφαλείας προς αντιμετώπιση και σημεία προσοχής. Τα περισσότερα μπορούν να επιλυθούν μέσα από το ίδιο το ΓΝ και έχουν μικρότερο κόστος υλοποίησης. Η ανάλυση κινδύνων όμως είναι δυναμική διαδικασία και η υλοποίηση των μέτρων ασφαλείας γίνεται σταδιακά.

Η διεξαγωγή της ανάλυσης επικινδυνότητας πρέπει να λάβει υπόψη της **το ζήτημα της υποκειμενικότητας κατά τη συλλογή των δεδομένων για το ΠΣ του ΓΝ** επειδή στηρίχθηκε στις απόψεις του προσωπικού του ΓΝ. Επομένως, η ακρίβεια των αποτελεσμάτων επηρεάζεται είναι συνάρτηση της αντικειμενικότητας των απαντήσεων του προσωπικού.

- Είναι χρήσιμο να γίνεται καλύτερη ενημέρωση των προβλημάτων που σχετίζονται με την ασφάλεια του ΠΣ του ΓΝ όπως:
- Συνεχή περιστατικά που σχετίζονται με την ασφάλεια.
- Έλλειψη πρόβλεψης για αξιολόγηση των αναγκών του Νοσοκομείου που σχετίζονται με την εκπλήρωση της αποστολής και των εργασιών του ΓΝ.
- Ανανέωση των προϊόντων και των Υπηρεσιών που απαιτούνται.
- Τεχνολογικές αλλαγές
- Ανάπτυξη νέων συστημάτων.

Θα πρέπει να ληφθούν υπόψη σχόλια από μελέτες ασφαλείας για τα ΠΣ του ΓΝ οργανογράμματα, απαιτήσεις, τεχνικές προδιαγραφές, πληροφορίες που να υποδεικνύουν τις κρίσιμες περιοχές αποτελέσματα από προηγούμενες αναλύσεις επικινδυνότητας.

Η μελέτη θα πρέπει να λαμβάνει υπόψη το κοινωνικό και οργανωτικό πλαίσιο λειτουργίας του Π.Σ. **Η μεθοδολογία δίνει τη δυνατότητα επιλογής απαιτήσεων από το ISO27001 και προσαρμογής του για εφαρμογή στο συγκεκριμένο περιβάλλον του ΓΝ.** Λόγω του ότι η ανάλυση και διαχείριση κινδύνων είναι μια δυναμική διαδικασία θα πρέπει να υπάρχει συνεχώς επικαιροποίηση των ευπαθειών από την βάση του NIST καθώς επίσης και από τα μέτρα που έχουν εφαρμοστότατα και από άλλες καλές πρακτικές όπως είναι η βάση δεδομένων του NIST IT Grundschutz της BSI.

3.15.2.2 Καθορισμός επιπέδων ωριμότητας(Maturity Levels).

3.15.2.3 Επιπλέον μέτρα ασφαλείας

Εκτιμάται ότι η χρήση του Διαδικτύου, όπως και του ηλεκτρονικού ταχυδρομείου από το προσωπικό του Νοσοκομείου, σε σύντομο χρονικό διάστημα θα αποτελεί συνήθη πρακτική για σημαντικό αριθμό υπαλλήλων. Κατά συνέπεια, θα πρέπει να αποδοθεί η ανάλογη σημασία στα μέτρα προστασίας κατά των κινδύνων και απειλών που απορρέουν από την πλοήγηση στο Διαδίκτυο και τη χρήση ηλεκτρονικού ταχυδρομείου, όπως είναι η εξάπλωση προγραμμάτων ιών, η δυνατότητα παρείσφρησης τρίτων.

Είναι χρήσιμα επιπλέον μέτρα ασφαλείας στην εγκατάσταση του λογισμικού με δικαιώματα πρόσβασης με συγκεκριμένα δικαιώματα στους χρήστες του Pilar με λογαριασμούς χρήστη λόγω ευαίσθητων προσωπικών δεδομένων.

Επίσης, δύναται το Pilar να χρησιμοποιηθεί για να πραγματοποιηθεί το Σχέδιο Επιχειρησιακής Συνέχειας.

Ακόμα, πρέπει το σχέδιο ασφαλείας να συμπληρωθεί με το σχέδιο Εκτακτης Ανάγκης.

Να δημιουργηθεί ένα σσφαλές περιβάλλον εγκατάστασης λογισμικού EAR/Pilar.

ΠΑΡΑΡΤΗΜΑ Α Συλλογή περιουσιακών στοιχείων ΠΣ-ΓΝ

The following sections provide forms for collecting the data in a risk analysis and management project.

For each type of asset:

- [D] data / information
- [S] services
- [SW] software
- [HW] hardware
- [COM] communication networks
- [SI] media
- [AUX] auxiliary equipment
- [L] installations
- [P] personnel

[D] Data / information

[D] Data / information	
code:	**name:**
description:	
proprietary:	
responsible:	
type (tick on all those that apply):	
( ) [vr] vital records	
( ) [com] data of commercial interest	
( ) [adm] data interesting for the public administration	
( ) [int] internal management data	
( ) [source] source code	
( ) [exe] executable code	
( ) [conf] configuration data	
( ) [log] activity *log*	
( ) [test] test data	
( ) [per] personal data	
( ) [A] high level	
( ) [M] medium level	
( ) [B] basic level	
( ) [label] classified data	
( ) [S] TOP SECRET	
( ) [R] SECRET	
( ) [C] CONFIDENTIEL	
( ) [DL] RESTREINT	
( ) [SC] UNCLASSIFIED	

Valuation of the data/information, typically in the following security dimensions:

[I] integrity

[C] confidentiality

[A_D] authenticity of who accesses the data

[T_D] accountability of who accesses the data, when, and what they do

Valuation		
dimension	*value*	*reason*
[I]		
[C]		
[A_D]		
[T_D]		

Dependencies on assets below (children)	
asset:	**degree:**
why?:	

asset:	**degree:**
why?:	

asset:	**degree:**
why?:	

[S] Services

[S] Services	
code:	name:
description:	
responsible:	
type (tick on all those that apply): ( ) [anon] anonymous (no user identification) ( ) [pub] general public (no contract) ( ) [ext] for external users (subject to contract) ( ) [int] internal (internal users, and means) ( ) [cont] provided by a third party (not owned means) ( ) [www] world wide web ( ) [telnet] remote terminal ( ) [email] electronic mail ( ) [ftp] file transfer ( ) [edi] electronic data interchange ( ) [dir] directory service ( ) [idm] identity management ( ) [ipm] privilege management ( ) [pki] PKI – public key infrastructure	

Valuation of the services offered by the organisation to others, typically in the following dimensions:

[D] availability

[A_S] authenticity of who accesses the service

[T_S] accountability of who accesses the service, when and what they do

Valuation		
dimension	*value*	*reason*
[D]		
[A_S]		
[T_S]		

Dependencies on assets below (children)	
asset:	degree:
why?:	
asset:	degree:
why?:	
asset:	degree:
why?:	

[SW] Software

[SW] Software	
code:	**name:**
description:	
responsible:	

type (tick on all those that apply):

- ( ) [prp] in-house development *(in house)*
- ( ) [sub] sub-contracted development
- ( ) [std] standard *(off the shelf)*
  - ( ) [browser] web browser
  - ( ) [www] presentation server
  - ( ) [email_client] email client
  - ( ) [app] application server
  - ( ) [file] file server
  - ( ) [dbms] database management system
  - ( ) [tm] transactional monitor
  - ( ) [office] office computing
  - ( ) [av] anti virus
  - ( ) [backup] backup system
  - ( ) [os] operating system

[HW] Hardware	
code:	**name:**
description:	
responsible:	
location:	
number:	

type (tick on all those that apply):

- ( ) [host] large equipment
- ( ) [mid] midsize equipment
- ( ) [pc] personal computing
- ( ) [mobile] mobile computing
- ( ) [pda] PDA
- ( ) [easy] easy to replace
- ( ) [data] that stores data
- ( ) [peripheral] peripheral
  - ( ) [print] printer
  - ( ) [scan] scanner
  - ( ) [crypto] cryptographic device
- ( ) [network] network device
  - ( ) [modem] model
  - ( ) [hub] hub
  - ( ) [switch] switch
  - ( ) [router] router
  - ( ) [bridge] bridge
  - ( ) [firewall] firewall
- ( ) [pabx] branch exchange

[COM] Communication networks

[COM] Communication networks	
code:	**name:**
description:	
responsible:	
location:	
number:	

type (tick on all those that apply):

- ( ) [PSTN] telephone network
- ( ) [ISDN] ISDN (digital network)
- ( ) [X25] X25 (data network)
- ( ) [ADSL] ADSL
- ( ) [pp] point to point
- ( ) [radio] wireless network
- ( ) [sat] satellite
- ( ) [LAN] local area network
- ( ) [MAN] metropolitan area network
- ( ) [Internet] Internet
- ( ) [vpn] virtual private network

[L] Installations

[L] Installations	
code:	**name:**
description:	
responsible:	
location:	
number:	
type (tick on all those that apply): ( ) [site] site ( ) [building] building ( ) [local] premises ( ) [mobile] mobile platform ( ) [car] land vehicle: car, truck, etc. ( ) [plane] aircraft, airplane, etc. ( ) [ship] sea transport: ship, boat, etc. ( ) [shelter] shelter ( ) [channel] channel	

[P] Personnel

[P] Personnel	
code:	**name:**
description:	
number:	
type (tick on all those that apply): ( ) [ue] external users ( ) [ui] internal users ( ) [op] operators ( ) [adm] system administrators ( ) [com] communications administrators ( ) [dba] database administrators ( ) [des] developers ( ) [sub] sub-contractors ( ) [prov] providers	

Value model

project: [nos1] nos1

Project data

nos1	nos1
library	[std] INFOSEC library (8.11.2013)

Dimensions

[A] Availability

[I] Integrity

[C] Confidentiality

[Auth] Authenticity of users and information

[Acc] Accountability of service and data

[V] Value

Security domains

[base] Base

Assets

Layer - [B] Essential assets

[datalabpatients] datapatients
[dataemployees] dataemployees
[financial] finlogisticssubcontractor

Layer - [IS] Internal services

[datapdpsn] datadpsn
[S_blooddata] s_blooddata
[s_eprotocol] s_eprotocol

Layer - [E] Equipment

[SW] Applications
[appdpsn] appdpsnsolarisml370
[ossw] os
[ospcwindows] ospcwindows
[oswindows] oswindows200server
[ossolaris] solaris
[appsfinancialwindowspc] logisticsexternalpatients
[appslocal] bloodfinanceeprotocolotsquestwiner server
[specialapps] firewallastro
[HW] Hardware
[lineprinter] lineprinter
[serverprot] questwinerserver
[serverpatients] compaqproliantml370
[serverblood] compaqproliantml370g3
[personalcomputer] pcwindows
[COM] Communications

[LAN] Local Area Network
[firewall] firewall

[AUX] Other elements

Layer - [SS] Subcontracted services

Layer - [L] Facilities

[offices] workingroomisthodosias
[dc] datacenterpliroforikhsorganwsis
[secretary] secretary
[aimodosia] workingroomaimodosia
[hospitaldepartments] hospitaldepartments

Layer - [P] Personnel

Summary of valuation

[B] Essential assets

asset	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[datalabpatients] datapatients	215K(1)	100K(2)	215K(3)	n.a.(4)	n.a.(5)	100K(6)
[dataemployees] dataemployees	1M(7)	215K(8)	215K(9)	n.a.(10)	n.a.(11)	215K(12)
[financial] finlogisticssubcontractor	215K(13)	1M(14)	215K(15)	n.a.(16)	n.a.(17)	100K(18)

(1) [5.pi1] is likely to cause significant distress to an individual
[7.lro] is likely to lead to a major breach of a legal or regulatory obligation
[7.da] Is likely to cause major disruption to activities within an organisation and with major impact on other organizations
[4.rto] 4 hours < RTO < 1 day

(2) [6.pi1] is likely to cause significant distress to a group of individuals
[5.pi1] is likely to cause significant distress to an individual

(3) [6.pi2] is likely to cause a significant breach of a legal regulatory requirement for personal information
[7.lg] Is likely to result in widespread adverse publicity

(4) [pi] Personal Information:
[6.pi2] is likely to cause a significant breach of a legal regulatory requirement for personal information

(5) [7.lro] is likely to lead to a major breach of a legal or regulatory obligation
(6) [6.pi2] is likely to cause a significant breach of a legal regulatory requirement for personal information
[5.lro] is likely to lead to a breach of a legal or regulatory obligation
(7) [5.pi1] is likely to cause significant distress to an individual
[9.lro] is likely to lead to an exceptionally serious breach of a legal or regulatory obligation
[5.lro] is likely to lead to a breach of a legal or regulatory obligation
[5.da] Is likely to cause disruption to activities within an organization and with some impact on other organizations
(8) [7.lro] is likely to lead to a major breach of a legal or regulatory obligation
[5.da] Is likely to cause disruption to activities within an organization and with some impact on other organizations
(9) [6.pi2] is likely to cause a significant breach of a legal regulatory requirement for personal information
[7.lro] is likely to lead to a major breach of a legal or regulatory obligation
(10) [5.pi1] is likely to cause significant distress to an individual
(11) [5.pi1] is likely to cause significant distress to an individual
(12) [6.pi2] is likely to cause a significant breach of a legal regulatory requirement for personal information
[7.lro] is likely to lead to a major breach of a legal or regulatory obligation
(13) [7.lro] is likely to lead to a major breach of a legal or regulatory obligation
(14) [6.pi2] is likely to cause a significant breach of a legal regulatory requirement for personal information
[9.lro] is likely to lead to an exceptionally serious breach of a legal or regulatory obligation
[5.da] is likely to cause disruption to activities within an organization and with some impact on other organizations
(15) [6.pi2] is likely to cause a significant breach of a legal regulatory requirement for personal information
[7.lro] is likely to lead to a major breach of a legal or regulatory obligation
(16) [lro] Legal and Regulatory Obligations:
(17) [7.lro] is likely to lead to a major breach of a legal or regulatory obligation
(18) [6.pi2] is likely to cause a significant breach of a legal regulatory requirement for personal information
[lro] Legal and Regulatory Obligations:

Assets

[datalabpatients] datapatients

[essential] Essential assets

[essential.info] information

[D.per] personal data

[D.per.A] level: high

[availability] Availability

[availability.easy] easy to replace

Security domain

[base] Base

Data

Below (assets on which this one depends on)

[S_blooddata] s_blooddata

Value

dimension	***value***	***accumulated values***
[A] Availability	215K(1)	215K
[I] Integrity	100K(2)	100K
[C] Confidentiality	215K(3)	215K
[Auth] Authenticity of users and information	n.a.(4)	n.a.
[Acc] Accountability of service and data	n.a.(5)	n.a.
[V] Value	100K(6)	100K

(1) [5.pi1] is likely to cause significant distress to an individual
[7.lro] is likely to lead to a major breach of a legal or regulatory obligation
[7.da] Is likely to cause major disruption to activities within an organisation and with major impact on other organizations
[4.rto] 4 hours < RTO < 1 day

(2) [6.pi1] is likely to cause significant distress to a group of individuals
[5.pi1] is likely to cause significant distress to an individual

(3) [6.pi2] is likely to cause a significant breach of a legal regulatory requirement for personal information
[7.lg] Is likely to result in widespread adverse publicity

(4) [pi] Personal Information:
[6.pi2] is likely to cause a significant breach of a legal regulatory requirement for personal information

(5) [7.lro] is likely to lead to a major breach of a legal or regulatory obligation

(6) [6.pi2] is likely to cause a significant breach of a legal regulatory requirement for personal information
[5.lro] is likely to lead to a breach of a legal or regulatory obligation

[dataemployees] dataemployees

[essential] Essential assets

[essential.info] information

[D.biz] business data

Security domain

[base] Base

Below (assets on which this one depends on)

[datapdpsn] datadpsn

Value

dimension	value	accumulated values
[A] Availability	1M(1)	1M
[I] Integrity	215K(2)	215K

[C] Confidentiality	215K(3)	215K
[Auth] Authenticity of users and information	n.a.(4)	n.a.
[Acc] Accountability of service and data	n.a.(5)	n.a.
[V] Value	215K(6)	215K

(1) [5.pi1] is likely to cause significant distress to an individual
[9.lro] is likely to lead to an exceptionally serious breach of a legal or regulatory obligation
[5.lro] is likely to lead to a breach of a legal or regulatory obligation
[5.da] Is likely to cause disruption to activities wi
(2) thin an organisation and with some impact on other organizations
(2) [7.lro] is likely to lead to a major breach of a legal or regulatory obligation
[5.da] Is likely to cause disruption to activities within an organization and with some impact on other organizations
(3) [6.pi2] is likely to cause a significant breach of a legal regulatory requirement for personal information
[7.lro] is likely to lead to a major breach of a legal or regulatory obligation
(4) [5.pi1] is likely to cause significant distress to an individual
(5) [5.pi1] is likely to cause significant distress to an individual
(6) [6.pi2] is likely to cause a significant breach of a legal regulatory requirement for personal information
[7.lro] is likely to lead to a major breach of a legal or regulatory obligation

[financial] finlogisticssubcontractor

- [essential] Essential assets
- [essential.info] information
- [D.vr] vital records (organizational records)

Security domain

- [base] Base Data Below (assets on which this one depends on)
- [s_eprotocol] s_eprotocol

Value

dimension	*value*	*accumulated values*
[A] Availability	215K(1)	215K
[I] Integrity	1M(2)	1M
[C] Confidentiality	215K(3)	215K
[Auth] Authenticity of users and information	n.a.(4)	n.a.
[Acc] Accountability of service and data	n.a.(5)	n.a.
[V] Value	100K(6)	100K

(1) [7.lro] is likely to lead to a major breach of a legal or regulatory obligation
(2) [6.pi2] is likely to cause a significant breach of a legal regulatory requirement for personal information
[9.lro] is likely to lead to an exceptionally serious breach of a legal or regulatory obligation
[5.da] Is likely to cause disruption to activities within an organization and with some impact on other organizations
(3) [6.pi2] is likely to cause a significant breach of a legal regulatory requirement for personal information
[7.lro] is likely to lead to a major breach of a legal or regulatory obligation
(4) [lro] Legal and Regulatory Obligations:
(5) [7.lro] is likely to lead to a major breach of a legal or regulatory obligation
(6) [6.pi2] is likely to cause a significant breach of a legal regulatory requirement for personal information
[lro] Legal and Regulatory Obligations:

[datapdpsn] datadpsn

- [arch] System architecture
- [arch.sap] service access point

Security domain

[base] Base

Above (assets that depend on this one)

- [dataemployees] dataemployees

Below (assets on which this one depends on)

- [ospcwindows] ospcwindows
- [ossolaris] solaris
- [appsfinancialwindowspc] logisticsexternalpatients
- [serverpatients] compaqproliantml370
- [personalcomputer] pcwindows
- [COM.LAN] Local Area Network

Value

dimension	*value*	*accumulated values*
[A] Availability		1M
[I] Integrity		215K
[C] Confidentiality		215K
[V] Value		215K

[S_blooddata] s_blooddata

- [D] Data / Information
- [D.files] data files

Security domain

[base] Base

Above (assets that depend on this one)

- [datalabpatients] datapatients

Below (assets on which this one depends on)

- [ossw] os
- [appslocal] bloodfinanceeprotocolotsquestwiner server
- [serverblood] compaqproliantml370g3

Value

dimension	*value*	*accumulated values*
[A] Availability		215K
[I] Integrity		100K
[C] Confidentiality		215K
[V] Value		100K

[s_eprotocol] s_eprotocol

- [D] Data / Information
- [D.files] data files

Security domain

[base] Base

Above (assets that depend on this one)

- [financial] finlogisticssubcontractor

Below (assets on which this one depends on)

- [oswindows] oswindows200server
- [appslocal] bloodfinanceeprotocolotsquestwiner server
- [serverprot] questwinerserver

Value

dimension	*value*	*accumulated values*
[A] Availability		215K
[I] Integrity		1M
[C] Confidentiality		215K
[V] Value		100K

[appdpsn] appdpsnsolarisml370

- [essential] Essential assets
- [essential.info] information
- [D] Data / Information
- [D.files] data files

Security domain

[base] Base

Above (assets that depend on this one)

- [serverpatients] compaqproliantml370

Value

dimension	*value*	*accumulated values*
[A] Availability		1M
[I] Integrity		215K
[C] Confidentiality		215K
[V] Value		/

[ossw] os

- [SW] Software
- [SW.std] standard (off the shelf)
- [SW.std.email_client] email client
- [SW.std.email_server] email server
- [SW.std.directory] directory server
- [SW.std.file] file server
- [SW.std.dbms] DBMS - data base management system
- [SW.std.os] operating system
- [SW.sec] security tools
- [SW.sec.av] anti virus

Security domain

[base] Base

Data

Above (assets that depend on this one)

- [S_blooddata] s_blooddata

Value

dimension	*value*	*accumulated values*
[A] Availability		215K
[I] Integrity		100K
[C] Confidentiality		215K
[V] Value		100K

[ospcwindows] ospcwindows

- [SW] Software
- [SW.std] standard (off the shelf)
- [SW.std.os] operating system

Security domain

[base] Base

Data

Above (assets that depend on this one)

- [datapdpsn] datadpsn

Value

dimension	*value*	*accumulated values*
[A] Availability		1M
[I] Integrity		215K
[C] Confidentiality		215K
[V] Value		215K

[oswindows] oswindows200server

- [SW] Software
- [SW.std] standard (off the shelf)
- [SW.std.os] operating system
- [SW.std.os.windows] windows

Security domain

[base] Base

Data

Above (assets that depend on this one)

- [s_eprotocol] s_eprotocol

Value

dimension	*value*	*accumulated values*
[A] Availability		215K
[I] Integrity		1M
[C] Confidentiality		215K
[V] Value		100K

[ossolaris] solaris

- [SW] Software
- [SW.std] standard (off the shelf)
- [SW.std.os] operating system
- [SW.std.os.solaris] solaris

Security domain

[base] Base

Above (assets that depend on this one)

- [datapdpsn] datadpsn

Value

dimension	*value*	*accumulated values*
[A] Availability		1M
[I] Integrity		215K
[C] Confidentiality		215K
[V] Value		215K

[appsfinancialwindowspc] logisticsexternalpatients

- [SW] Software
- [SW.prp] in-house development

Security domain

[base] Base

Data

Above (assets that depend on this one)

- [datapdpsn] datadpsn

Value

dimension	*value*	*accumulated values*
[A] Availability		1M
[I] Integrity		215K
[C] Confidentiality		215K
[V] Value		215K

[appslocal] bloodfinanceeprotocolotsquestwiner server

Security domain

[base] Base

Data

Above (assets that depend on this one)

- [S_blooddata] s_blooddata
- [s_eprotocol] s_eprotocol
- [serverprot] questwinerserver
- [serverblood] compaqproliantml370g3

Value

dimension	*value*	*accumulated values*
[A] Availability		430K
[I] Integrity		1.1M
[C] Confidentiality		430K
[V] Value		200K

[specialapps] firewallastro

- [SW] Software
- [SW.sub] contracted development

Security domain

[base] Base

Data

Value

dimension	*value*	*accumulated values*

[lineprinter] lineprinter

- [HW] Hardware
- [HW.peripheral] peripheral equipment
- [HW.peripheral.print] printing equipment

Security domain

[base] Base

Data

Below (assets on which this one depends on)

- [hospitaldepartments] hospitaldepartments

Value

dimension	*value*	*accumulated values*

[serverprot] questwinerserver

- [SW] Software
- [SW.std] standard (off the shelf)
- [SW.std.ts] terminal server
- [HW] Hardware
- [HW.host] hosts

Security domain

[base] Base

Data

Above (assets that depend on this one)

- [s_eprotocol] s_eprotocol

Below (assets on which this one depends on)

- [appslocal] bloodfinanceeprotocolotsquestwiner server
- [secretary] secretary

Value

dimension	*value*	*accumulated values*
[A] Availability		215K
[I] Integrity		1M
[C] Confidentiality		215K
[V] Value		100K

[serverpatients] compaqproliantml370

- [D] Data / Information
- [D.files] data files
- [D.log] activity log
- [HW] Hardware
- [HW.host] hosts

Security domain

[base] Base

Data

1	mid-size equipment with local storage
	files,communications
property	Systemadministator
	1+maintenance contract for hw and sw

Above (assets that depend on this one)

- [datapdpsn] datadpsn

Below (assets on which this one depends on)

- [appdpsn] appdpsnsolarisml370
- [dc] datacenterpliroforikhsorganwsis

Value

dimension	*value*	*accumulated values*
[A] Availability		1M
[I] Integrity		215K
[C] Confidentiality		215K
[V] Value		215K

[serverblood] compaqproliantml370g3

- [HW] Hardware
- [HW.host] hosts

Security domain

[base] Base

Data

Above (assets that depend on this one)

- [S_blooddata] s_blooddata

Below (assets on which this one depends on)

- [appslocal] bloodfinanceeprotocolotsquestwiner server
- [aimodosia] workingroomaimodosia

Value

dimension	*value*	*accumulated values*
[A] Availability		215K
[I] Integrity		100K
[C] Confidentiality		215K
[V] Value		100K

[personalcomputer] pcwindows

Security domain

[base] Base

Data

Above (assets that depend on this one)

- [datapdpsn] datadpsn

Below (assets on which this one depends on)

- [offices] workingroomisthodosias
- [aimodosia] workingroomaimodosia

Value

dimension	*value*	*accumulated values*
[A] Availability		1M
[I] Integrity		215K
[C] Confidentiality		215K
[V] Value		215K

[COM.LAN] Local Area Network

- [COM] Communication networks
- [COM.LAN] local area network

Security domain

[base] Base

Above (assets that depend on this one)

- [datapdpsn] datadpsn

Below (assets on which this one depends on)

- [hospitaldepartments] hospitaldepartments

Value

dimension	*value*	*accumulated values*
[A] Availability		1M
[I] Integrity		215K
[C] Confidentiality		215K
[V] Value		215K

[COM.firewall] firewall

- [arch] System architecture
- [arch.ip] logical interconnection point
- [D] Data / Information
- [D.conf] configuration data

Security domain

[base] Base

Data

	remotemanaged

Below (assets on which this one depends on)

- [dc] datacenterpliroforikhsorganwsis

Value

dimension	*value*	*accumulated values*

[offices] workingroomisthodosias

- [L] Installations
- [L.local] room

Security domain

[base] Base

Above (assets that depend on this one)

- [personalcomputer] pcwindows

Value

dimension	*value*	*accumulated values*
[A] Availability		1M
[I] Integrity		215K
[C] Confidentiality		215K
[V] Value		215K

[dc] datacenterpliroforikhsorganwsis

- [L] Installations
- [L.local] room

Security domain

[base] Base

Above (assets that depend on this one)

- [serverpatients] compaqproliantml370
- [COM.firewall] firewall

Value

dimension	*value*	*accumulated values*
[A] Availability		1M
[I] Integrity		215K
[C] Confidentiality		215K
[V] Value		215K

[secretary] secretary

- [L] Installations
- [L.local] room

Security domain

[base] Base

Above (assets that depend on this one)

- [serverprot] questwinerserver

Value

dimension	*value*	*accumulated values*
[A] Availability		215K
[I] Integrity		1M
[C] Confidentiality		215K
[V] Value		100K

[aimodosia] workingroomaimodosia

- [L] Installations
- [L.local] room

Security domain

[base] Base

Above (assets that depend on this one)

- [serverblood] compaqproliantml370g3
- [personalcomputer] pcwindows

Value

dimension	*value*	*accumulated values*
[A] Availability		1.2M
[I] Integrity		315K
[C] Confidentiality		430K
[V] Value		315K

[hospitaldepartments] hospitaldepartments

- [L] Installations
- [L.local] room

Security domain

[base] Base

Above (assets that depend on this one)

- [lineprinter] lineprinter
- [COM.LAN] Local Area Network

Value

dimension	*value*	*accumulated values*
[A] Availability		1M
[I] Integrity		215K
[C] Confidentiality		215K
[V] Value		215K

A detailed scale of 10 values has been chosen, with zero being a minimal value (for the purposes of risk). If a risk analysis is a made with little detail, a simplified table of five levels could be used.

Both scales - detailed and simplified - are correlated as shown below:

(1) [5.pi1] is likely to cause significant distress to an individual
[7.lro] is likely to lead to a major breach of a legal or regulatory obligation
[7.da] Is likely to cause major disruption to activities within an organisation and with major impact on other organisations
[4.rto] 4 hours < RTO < 1 day

(2) [5.pi1] is likely to cause significant distress to an individual

(3) [6.pi2] is likely to cause a significant breach of a legal regulatory requirement for personal information

(4) [pi] Personal Information:
[6.pi2] is likely to cause a significant breach of a legal regulatory requirement for personal information

(5) [7.lro] is likely to lead to a major breach of a legal or regulatory obligation

(6) [5.pi1] is likely to cause significant distress to an individual
[9.lro] is likely to lead to an exceptionally serious breach of a legal or regulatory obligation

(7) [7.lro] is likely to lead to a major breach of a legal or regulatory obligation

(8) [7.lro] is likely to lead to a major breach of a legal or regulatory obligation

(9) [5.pi1] is likely to cause significant distress to an individual

(10) [5.pi1] is likely to cause significant distress to an individual

(11) [7.lro] is likely to lead to a major breach of a legal or regulatory obligation

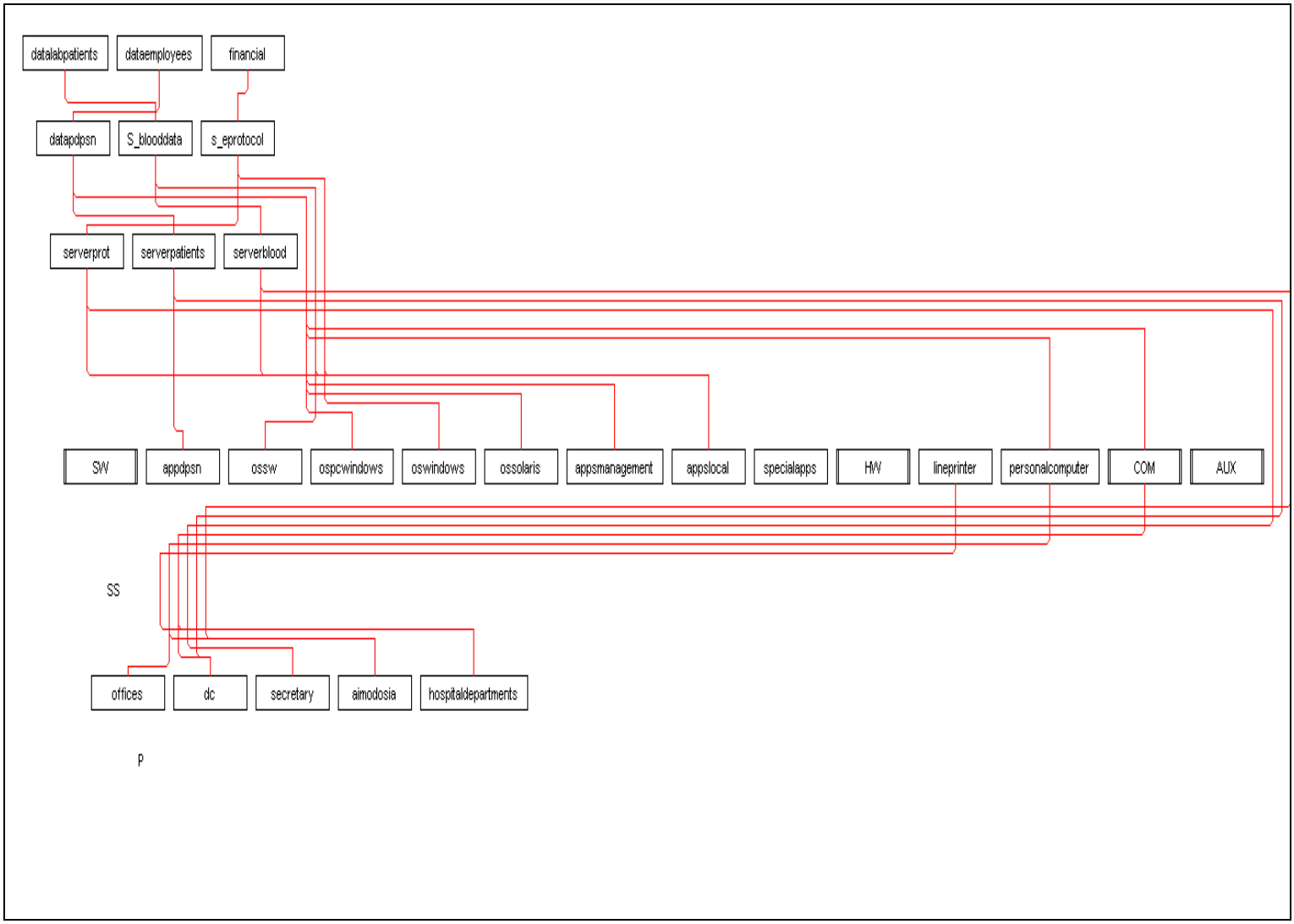
(12) [6.pi2] is likely to cause a significant breach of a legal regulatory requirement for personal information
[9.lro] is likely to lead to an exceptionally serious breach of a legal or regulatory obligation

(13) [7.lro] is likely to lead to a major breach of a legal or regulatory obligation

(14) [lro] Legal and Regulatory Obligations:

(15) [7.lro] is likely to lead to a major breach of a legal or regulatory obligation

Παράρτημα Γ: Εξαρτήσειςπεριουσιακών στοιχείων.



Παράρτημα Δ: Αποτίμηση Απειλών

project: [nos1] nos1
Project data

nos1	nos1
library	[std] INFOSEC library (8.11.2013)

License

Dimensions

[A] Availability
[I] Integrity
[C] Confidentiality
[Auth] Authenticity of users and information
[Acc] Accountability of service and data
[V] Value

Security domains

[base] Base

threats / asset

[datalabpatients] datapatients

threat	***level***	[A]	[I]	[C]	[V]
[A.5.1] By insiders	H	H	H	H	H
[A.5.3] By outsiders	H	H	H	VH	H

[dataemployees] dataemployees

threat	***level***	[A]	[I]	[C]	[V]
[A.5.1] By insiders	M	H	H	H	H
[A.5.3] By outsiders	L	H	H	H	L

[financial] finlogisticssubcontractor

threat	***level***	[A]	[I]	[C]	[V]
[A.5.1] By insiders	M	M	H	M	M
[A.5.3] By outsiders	H	H	H	H	L

[datapdpsn] datadpsn

threat	***level***	[A]	[I]	[C]	[V]
[E.1] User errors	H	-	-	-	M
[E.2] System / Security administrator errors	VH	-	-	-	L
[E.14] Information leaks (> E.19)	0	-	-	-	-
[E.15] Accidental alteration of the	0	-	-	-	-

information					
[E.18] Destruction of information	0	M	-	-	-
[A.5] Masquerading of identity	H	H	H	H	H
[A.6] Abuse of access privileges	L	L	L	L	L
[A.11] Unauthorised access	0	-	-	-	-
[A.15] Deliberate alteration of information	0	-	-	-	-
[A.18] Destruction of information	0	-	-	-	-
[A.19] Disclosure of information	0	-	-	-	-

[S_blooddata] s_blooddata

threat	***level***	[A]	[I]	[C]	[V]
[E.1] User errors	H	M	M	M	M
[E.2] System / Security administrator errors	M	M	M	M	-
[E.15] Accidental alteration of the information	M	-	L	-	-
[E.18] Destruction of information	M	L	-	-	-
[E.19] Information leaks		-	-	M	-
[A.5] Masqueradin g of identity		H	H	VH	H
[A.6] Abuse of access privileges		L	M	L	L
[A.11] Unauthorised access		-	M	H	-
[A.15] Deliberate alteration of information		-	T	-	-

[A.18] Destruction of information	H	H	-	-	-
[A.19] Disclosure of information	H	-	-	T	-

[s_eprotocol] s_eprotocol

threat	***level***	[A]	[I]	[C]	[V]
[E.1] User errors		M	M	M	H
[E.2] System / Security administrator errors	VH	M	M	M	L
[E.15] Accidental alteration of the information		-	L	-	-
[E.18] Destruction of information		L	-	-	-
[E.19] Information leaks		-	-	M	-
[A.5] Masqueradin g of identity		H	VH	H	H
[A.6] Abuse of access privileges		L	L	L	L
[A.11] Unauthorised access		-	M	H	-
[A.15] Deliberate alteration of information		-	T	-	-
[A.18] Destruction of information		H	-	-	-
[A.19] Disclosure of information		-	-	T	-

[appdpsn] appdpsn

threat	***level***	[A]	[I]	[C]	[V]
[E.1] User errors	H	H	H	H	H
[E.2] System / Security administrator errors	VH	M	M	M	M
[E.15] Accidental alteration of the information	M	-	L	-	M
[E.18] Destruction of information	M	L	-	-	M
[E.19] Information leaks	M	-	-	M	M
[A.5] Masqueradin g of identity	H	-	M	H	M
[A.6] Abuse of access privileges	H	L	M	H	M
[A.11] Unauthorised access	VH	-	M	H	-
[A.15] Deliberate alteration of information	H	-	T	-	-
[A.18] Destruction of information	H	H	-	-	-
[A.19] Disclosure of information	H	-	-	T	-

[ossw] os

threat	***level***	[A]	[I]	[C]	[V]
[I.5] Hardware or software failure	M	H	-	-	M
[E.1] User errors	M	L	M	M	M
[E.2] System / Security administrator errors	M	M	M	M	M
[E.8] Malware diffusion	M	M	M	M	M

[E.15] Accidental alteration of the information	M	-	L	-	M
[E.18] Destruction of information	M	H	-	-	M
[E.19] Information leaks	M	-	-	M	M
[E.20] Software vulnerabilities	M	L	M	M	M
[E.21] Defects in software maintenance / updating	H	L	L	-	M
[A.5] Masquerading of identity	M	-	H	H	M
[A.6] Abuse of access privileges	M	L	M	M	M
[A.7] Misuse	M	L	M	M	M
[A.8] Malware diffusion	M	T	T	T	M
[A.11] Unauthorised access	M	-	M	H	M
[A.15] Deliberate alteration of information	M	-	H	-	M
[A.18] Destruction of information	M	H	-	-	M
[A.19] Disclosure of information	M	-	-	H	M
[A.22] Software manipulation	M	H	T	T	M

[ospcwindows] ospcwindows

threat	***level***	[A]	[I]	[C]	[V]
[I.5] Hardware or software failure	M	H	-	-	M
[E.1] User errors	M	L	M	M	M
[E.2] System / Security administrator errors	M	M	M	M	M

[E.8] Malware diffusion	M	M	M	M	M
[E.15] Accidental alteration of the information	M	-	L	-	M
[E.18] Destruction of information	M	H	-	-	M
[E.19] Information leaks	M	-	-	M	-
[E.20] Software vulnerabilities	M	L	M	M	-
[E.21] Defects in software maintenance / updating	H	L	L	-	-
[A.5] Masquerading of identity	M	-	H	H	-
[A.6] Abuse of access privileges	M	L	M	M	-
[A.7] Misuse	M	L	M	M	-
[A.8] Malware diffusion	M	M	M	-	M
[A.11] Unauthorised access	M	-	M	H	-
[A.15] Deliberate alteration of information	M	-	H	-	-
[A.18] Destruction of information	M	H	-	-	-
[A.19] Disclosure of information	M	-	-	H	-
[A.22] Software manipulation	M	H	T	T	-

[oswindows] oswindows200server

threat	***level***	[A]	[I]	[C]	[V]
[I.5] Hardware or software failure	M	H	-	-	-
[E.1] User errors	M	L	M	M	M
[E.2] System / Security administrator errors	M	M	M	M	-
[E.8] Malware diffusion	M	M	M	M	M
[E.15] Accidental alteration of the information	M	-	L	-	-
[E.18] Destruction of information	M	H	-	-	M
[E.19] Information leaks	M	-	-	M	-
[E.20] Software vulnerabilities	M	L	M	M	-
[E.21] Defects in software maintenance / updating	H	L	L	-	-
[A.5] Masquerading of identity	M	-	H	H	-
[A.6] Abuse of access privileges	M	L	M	M	-
[A.7] Misuse	M	L	M	M	-
[A.8] Malware diffusion	M	T	T	T	-
[A.11] Unauthorised access	M	-	M	H	-
[A.15] Deliberate alteration of information	M	-	H	-	-
[A.18] Destruction of information	M	H	-	-	-
[A.19] Disclosure of	M	-	-	H	-

information					
[A.22] Software manipulation	M	H	T	T	-

[ossolaris] solaris

threat	***level***	[A]	[I]	[C]	[V]
[I.5] Hardware or software failure	M	H	-	-	-
[E.1] User errors	M	L	M	M	M
[E.2] System / Security administrator errors	M	M	M	M	-
[E.8] Malware diffusion	M	M	M	M	-
[E.15] Accidental alteration of the information	M	-	L	-	-
[E.18] Destruction of information	M	H	-	-	-
[E.19] Information leaks	M	-	-	M	-
[E.20] Software vulnerabilities	M	L	M	M	-
[E.21] Defects in software maintenance / updating	H	L	L	-	-
[A.5] Masquerading of identity	M	-	H	H	-
[A.6] Abuse of access privileges	M	L	M	M	-
[A.7] Misuse	M	L	M	M	-
[A.8] Malware diffusion	M	T	T	T	-
[A.11] Unauthorised access	M	-	M	H	-
[A.15] Deliberate alteration of information	M	-	H	-	-
[A.18] Destruction of	M	H	-	-	-

information					
[A.19] Disclosure of information	M	-	-	H	-
[A.22] Software manipulation	M	H	T	T	-

[appsmanagement] logisticsexternalpatients

threat	***level***	[A]	[I]	[C]	[V]
[I.5] Hardware or software failure	M	H	-	-	-
[E.1] User errors	M	L	M	M	-
[E.2] System / Security administrator errors	M	M	M	M	-
[E.8] Malware diffusion	M	M	M	M	-
[E.15] Accidental alteration of the information	M	-	L	-	-
[E.18] Destruction of information	M	H	-	-	-
[E.19] Information leaks	M	-	-	M	-
[E.20] Software vulnerabilities	M	L	M	M	-
[E.21] Defects in software maintenance / updating	H	L	L	-	-
[A.5] Masquerading of identity	M	-	H	H	-
[A.6] Abuse of access privileges	M	L	M	M	-
[A.7] Misuse	M	L	M	M	-
[A.8] Malware diffusion	M	T	T	T	-
[A.11] Unauthorised access	M	-	M	H	-
[A.15] Deliberate	M	-	H	-	-

alteration of information					
[A.18] Destruction of information	M	H	-	-	-
[A.19] Disclosure of information	M	-	-	H	-
[A.22] Software manipulation	M	H	T	T	-

[appslocal] bloodfinanceeprotocol

[specialapps] firewallastro

[lineprinter] lineprinter

threat	***level***	[A]	[I]	[C]	[V]
[I.5.2] Hardware	L	M	M	M	L

[serverprot] questwinerserver

threat	***level***	[A]	[I]	[C]	[V]
[N.1] Fire	VL	L	L	L	L
[N.2] Water	VL	L	L	L	L
[N.*] Other natural disasters	L	T	-	-	-
[I.6] Power interruption	M	T	-	-	-
[E.1] User errors	M	L	M	M	-
[E.2] System / Security administrator errors	M	M	M	M	-
[E.8] Malware diffusion	M	M	M	M	-
[E.15] Accidental alteration of the information	M	-	L	-	-
[E.20] Software vulnerabilities	VL	L	L	L	L
[E.21]	VL	L	L	L	L

Defects in software maintenance / updating					
[E.23] Defects in hardware maintenance / updating	M	M	-	-	-
[E.24] System failure due to exhaustion of resources	H	H	-	-	-
[E.25] Equipment loss	L	T	-	T	-
[A.5] Masqueradin g of identity	M	-	H	H	-
[A.6] Abuse of access privileges	M	M	M	H	-
[A.7] Misuse	M	L	L	M	-
[A.8] Malware diffusion	M	T	T	T	-
[A.11] Unauthorised access	M	M	M	H	-
[A.15] Deliberate alteration of information	M	-	H	-	-
[A.18] Destruction of information	M	H	-	-	-
[A.19] Disclosure of information	M	-	-	H	-
[A.22] Software manipulation	M	H	T	T	-
[A.23] Hardware manipulation	M	H	-	H	-
[A.24] Denial of service	M	T	-	-	-
[A.25] Theft	M	M	M	M	M

[serverpatients] compaqproliantml370

threat	***level***	[A]	[I]	[C]	[V]
[N.1] Fire	VL	L	L	L	L
[N.2] Water	VL	L	L	L	L
[I.6] Power interruption	M	T	-	-	-
[E.1] User errors	H	M	M	M	-
[E.2] System / Security administrator errors	M	M	M	M	-
[E.3] Monitoring errors (log)	M	-	L	-	-
[E.15] Accidental alteration of the information	M	-	L	-	-
[E.18] Destruction of information	M	L	-	-	-
[E.19] Information leaks	M	-	-	M	-
[E.23] Defects in hardware maintenance / updating	VL	L	L	L	L
[E.24] System failure due to exhaustion of resources	H	H	-	-	-
[E.25] Equipment loss	L	T	-	T	-
[A.3] Manipulation of activity records (log)	VL	L	L	L	VH
[A.5] Masqueradin g of identity	H	-	M	H	-
[A.6] Abuse of access privileges	M	M	M	H	-
[A.7] Misuse	M	L	L	M	-
[A.11] Unauthorised access	M	M	M	H	-
[A.13] Repudiation (denial of actions)	H	-	T	-	-
[A.15] Deliberate	H	-	T	-	-

alteration of information					
[A.18] Destruction of information	H	H	-	-	-
[A.19] Disclosure of information	H	-	-	T	-
[A.23] Hardware manipulation	VL	L	L	L	H
[A.24] Denial of service	M	T	-	-	-
[A.25] Theft	M	M	M	M	M
[A.26] Destructive attack	L	L	L	L	L

[serverblood] compaqproliantml370g3

threat	***level***	[A]	[I]	[C]	[V]
[N.1] Fire	VL	L	L	L	L
[N.2] Water	VL	L	L	L	L
[N.*] Other natural disasters	L	T	-	-	-
[I.4] Electromagnetic pollution	M	M	-	-	-
[I.5] Hardware or software failure	VL	L	L	L	-
[I.6] Power interruption	M	T	-	-	-
[I.11] Electromagnetic emanations	M	-	-	L	-
[E.2] System / Security administrator errors	M	M	M	M	-
[E.23] Defects in hardware maintenance / updating	M	M	-	-	-
[E.24] System failure due to exhaustion of resources	H	H	-	-	-
[E.25] Equipment loss	L	T	-	T	-
[A.6] Abuse of access privileges	M	M	M	H	-
[A.7] Misuse	M	L	L	M	-

[A.11] Unauthorised access	M	M	M	H	-
[A.23] Hardware manipulation	L	L	L	L	L
[A.24] Denial of service	M	T	-	-	-
[A.25] Theft	VL	L	L	L	L
[A.26] Destructive attack	VL	L	L	L	L

[personalcomputer] pcwindows

threat	***level***	[A]	[I]	[C]	[V]
[N.1] Fire	VL	L	L	L	L
[N.2] Water	VL	L	L	L	L
[I.4] Electromagnetic pollution	0	-	-	-	-
[I.5] Hardware or software failure	0	-	-	-	-
[I.6] Power interruption	0	-	-	-	-
[I.11] Electromagnetic emanations	0	-	-	-	-
[E.2] System / Security administrator errors	0	-	-	-	-
[E.23] Defects in hardware maintenance / updating	VL	L	L	L	L
[E.24] System failure due to exhaustion of resources	M	M	M	M	M
[E.25] Equipment loss	0	-	-	-	-
[A.6] Abuse of access privileges	0	-	-	-	-
[A.7] Misuse	0	-	-	-	-
[A.11] Unauthorised access	0	-	-	-	-
[A.23] Hardware manipulation	M	M	M	M	M
[A.24] Denial of service	0	-	-	-	-
[A.25] Theft	0	-	-	-	-

[A.26] Destructive attack	VL	L	L	L	L

[COM.LAN] Local Area Network

threat	***level***	[A]	[I]	[C]	[V]
[I.8] Communications services failure	L	L	-	-	L
[E.2] System / Security administrator errors	M	M	M	M	M
[E.9] [Re-]routing errors	VL	L	L	L	L
[E.10] Sequence errors	VL	L	L	L	L
[E.15] Accidental alteration of the information	L	M	L	M	M
[E.19] Information leaks	L	L	L	L	L
[E.24] System failure due to exhaustion of resources	L	L	L	L	L
[A.5] Masqueradin g of identity	L	L	L	L	H
[A.6] Abuse of access privileges	M	M	M	H	M
[A.7] Misuse	M	M	M	M	M
[A.9] [Re-]routing of messages	M	M	M	M	M
[A.10] Sequence alteration	M	M	M	M	M
[A.11] Unauthorised access	M	M	M	H	M
[A.12] Traffic analysis	M	M	M	L	M
[A.14] Eavesdroppin g	M	M	M	L	M
[A.15] Deliberate alteration of information	M	M	M	M	M
[A.18]	M	H	M	M	M

Destruction of information					
[A.19] Disclosure of information	M	M	M	H	M
[A.24] Denial of service	H	H	M	M	M

[COM.firewall] firewall

[offices] workingroomisthodosias

threat	***level***	[A]	[I]	[C]	[V]
[N.1] Fire	VL	L	L	L	L
[N.2] Water	VL	L	L	L	-
[N.*] Other natural disasters	VL	L	L	L	L
[A.7] Misuse	M	M	M	H	-
[A.11] Unauthorised access	H	-	M	H	-
[A.26] Destructive attack	L	L	L	L	L
[A.27] Enemy over-run	L	T	-	H	L

[dc] datacenterπληροφορικήςοργάνωσης

threat	***level***	[A]	[I]	[C]	[V]
[N.1] Fire	VL	L	L	L	L
[N.2] Water	VL	L	L	L	L
[N.*] Other natural disasters	VL	L	L	L	L
[I.11] Electromagnetic emanations	L	-	-	L	-
[A.11] Unauthorised access	H	-	M	H	-
[A.26] Destructive attack	L	L	L	L	L
[A.27] Enemy over-run	L	T	-	H	L

[secretary] secretary

threat	***level***	[A]	[I]	[C]	[V]
[N.1] Fire	VL	T	-	-	-
[N.2] Water	VL	T	-	-	-
[N.*] Other natural disasters	VL	L	L	L	L
[I.3] Environment	0	-	-	-	-

al pollution					
[I.4] Electromagnetic pollution	L	M	-	-	-
[A.11] Unauthorised access	H	-	M	H	-
[A.26] Destructive attack	L	L	L	L	L
[A.27] Enemy over-run	VL	T	-	H	-

[aimodosia] workingroomaimodosia

threat	***level***	[A]	[I]	[C]	[V]
[N.1] Fire	VL	T	-	-	-
[N.2] Water	VL	T	-	-	-
[N.*] Other natural disasters	VL	L	L	L	L
[I.3] Environmental pollution	M	M	-	-	-
[I.11] Electromagnetic emanations	L	-	-	L	-
[A.11] Unauthorised access	H	-	M	H	-
[A.26] Destructive attack	L	L	L	L	L
[A.27] Enemy over-run	M	T	-	H	-

[hospitaldepartments] hospitaldepartments

threat	***level***	[A]	[I]	[C]	[V]
[N.1] Fire	VL	T	-	-	-
[N.2] Water	VL	L	L	L	L
[N.*] Other natural disasters	VL	L	L	L	L
[I.11] Electromagnetic emanations	L	-	-	L	-
[A.7] Misuse	M	M	M	H	-
[A.11] Unauthorised access	H	-	M	H	-
[A.26] Destructive attack	VL	L	L	L	L
[A.27] Enemy over-run	VL	T	-	H	-

- **assets / threat**

[N.1] Fire

asset	***level***	[A]	[I]	[C]	[V]
[serverprot] questwinerserver	VL	L	L	L	L
[serverpatients] compaqprolia ntml370	VL	L	L	L	L
[serverblood] compaqprolia ntml370g3	VL	L	L	L	L
[personalcomputer] pcwindows	VL	L	L	L	L
[offices] workingroom isthodosias	VL	L	L	L	L
[dc] datacenterpliroforikhsorganwsis	VL	L	L	L	L
[secretary] secretary	VL	T	-	-	-
[aimodosia] workingroom aimodosia	VL	T	-	-	-
[hospitaldepartments] hospitaldepartments	VL	T	-	-	-

[N.2] Water

asset	***level***	[A]	[I]	[C]	[V]
[serverprot] questwinerserver	VL	L	L	L	L
[serverpatients] compaqprolia ntml370	VL	L	L	L	L
[serverblood] compaqprolia ntml370g3	VL	L	L	L	L
[personalcomputer] pcwindows	VL	L	L	L	L
[offices] workingroom isthodosias	VL	L	L	L	-
[dc] datacenterpliroforikhsorganwsis	VL	L	L	L	L
[secretary] secretary	VL	T	-	-	-
[aimodosia]	VL	T	-	-	-

workingroom aimodosia					
[hospitaldepartments] hospitaldepartments	VL	L	L	L	L

[N.*] Other natural disasters

asset	***level***	[A]	[I]	[C]	[V]
[serverprot] questwinerserver	L	T	-	-	-
[serverblood] compaqproliantml370g3	L	T	-	-	-
[offices] workingroom isthodosias	VL	L	L	L	L
[dc] datacenterpliroforikhsorganwsis	VL	L	L	L	L
[secretary] secretary	VL	L	L	L	L
[aimodosia] workingroom aimodosia	VL	L	L	L	L
[hospitaldepartments] hospitaldepartments	VL	L	L	L	L

[I.3] Environmental pollution

asset	***level***	[A]	[I]	[C]	[V]
[secretary] secretary	0	-	-	-	-
[aimodosia] workingroom aimodosia	M	M	-	-	-

[I.4] Electromagnetic pollution

asset	***level***	[A]	[I]	[C]	[V]
[serverblood] compaqproliantml370g3	M	M	-	-	-
[personalcomputer] pcwindows	0	-	-	-	-
[secretary] secretary	L	M	-	-	-

[I.5] Hardware or software failure

asset	***level***	[A]	[I]	[C]	[V]
[ossw] os	M	H	-	-	M
[ospcwindows] ospcwindows	M	H	-	-	M

[oswindows] oswindows200server	M	H	-	-	-
[ossolaris] solaris	M	H	-	-	-
[appsmanagement] logisticsexternalpatients	M	H	-	-	-
[serverblood] compaqprolia ntml370g3	VL	L	L	L	-
[personalcomputer] pcwindows	0	-	-	-	-

[I.5.2] Hardware

asset	***level***	[A]	[I]	[C]	[V]
[lineprinter] lineprinter	L	M	M	M	L

[I.6] Power interruption

asset	***level***	[A]	[I]	[C]	[V]
[serverprot] questwinerserver	M	T	-	-	-
[serverpatients] compaqprolia ntml370	M	T	-	-	-
[serverblood] compaqprolia ntml370g3	M	T	-	-	-
[personalcomputer] pcwindows	0	-	-	-	-

[I.8] Communications services failure

asset	***level***	[A]	[I]	[C]	[V]
[COM.LAN] Local Area Network	L	L	-	-	L

[I.11] Electromagnetic emanations

asset	***level***	[A]	[I]	[C]	[V]
[serverblood] compaqprolia ntml370g3	M	-	-	L	-
[personalcomputer] pcwindows	0	-	-	-	-
[dc] datacenterpliroforikhsorganwsis	L	-	-	L	-
[aimodosia] workingroom	L	-	-	L	-

aimodosia					
[hospitaldepartments] hospitaldepartments	L	-	-	L	-

[E.1] User errors

asset	***level***	[A]	[I]	[C]	[V]
[datapdpsn] datadpsn	H	-	-	-	M
[S_blooddata] s_blooddata	H	M	M	M	M
[s_eprotocol] s_eprotocol		M	M	M	H
[appdpsn] appdpsn	H	H	H	H	H
[ossw] os	M	L	M	M	M
[ospcwindows] ospcwindows	M	L	M	M	M
[oswindows] oswindows2000server	M	L	M	M	M
[ossolaris] solaris	M	L	M	M	M
[appsmanagement] logisticsexternalpatients	M	L	M	M	-
[serverprot] questwinerserver	M	L	M	M	-
[serverpatients] compaqprolianthtml370	H	M	M	M	-

[E.2] System / Security administrator errors

asset	***level***	[A]	[I]	[C]	[V]
[datapdpsn] datadpsn	VH	-	-	-	L
[S_blooddata] s_blooddata	M	M	M	M	-
[s_eprotocol] s_eprotocol	VH	M	M	M	L
[appdpsn] appdpsn	VH	M	M	M	M
[ossw] os	M	M	M	M	M
[ospcwindows] ospcwindows	M	M	M	M	M
[oswindows] oswindows2000server	M	M	M	M	-
[ossolaris] solaris	M	M	M	M	-
[appsmanagement] logisticsexternalpatients	M	M	M	M	-

[serverprot] questwinerserver	M	M	M	M	-
[serverpatients] compaqprolia ntml370	M	M	M	M	-
[serverblood] compaqprolia ntml370g3	M	M	M	M	-
[personalcomputer] pcwindows	0	-	-	-	-
[COM.LAN] Local Area Network	M	M	M	M	M

[E.3] Monitoring errors (log)

asset	***level***	[A]	[I]	[C]	[V]
[serverpatients] compaqprolia ntml370	M	-	L	-	-

[E.8] Malware diffusion

asset	***level***	[A]	[I]	[C]	[V]
[ossw] os	M	M	M	M	M
[ospcwindows] ospcwindows	M	M	M	M	M
[oswindows] oswindows200server	M	M	M	M	M
[ossolaris] solaris	M	M	M	M	-
[appsmanagement] logisticsexternalpatients	M	M	M	M	-
[serverprot] questwinerserver	M	M	M	M	-

[E.9] [Re-]routing errors

asset	***level***	[A]	[I]	[C]	[V]
[COM.LAN] Local Area Network	VL	L	L	L	L

[E.10] Sequence errors

asset	***level***	[A]	[I]	[C]	[V]
[COM.LAN] Local Area Network	VL	L	L	L	L

[E.14] Information leaks (> E.19)

asset	*level*	[A]	[I]	[C]	[V]
[datapdpsn] datadpsn	0	-	-	-	-

[E.15] Accidental alteration of the information

asset	*level*	[A]	[I]	[C]	[V]
[datapdpsn] datadpsn	0	-	-	-	-
[S_blooddata] s_blooddata	M	-	L	-	-
[s_eprotocol] s_eprotocol		-	L	-	-
[appdpsn] appdpsn	M	-	L	-	M
[ossw] os	M	-	L	-	M
[ospcwindows] ospcwindows	M	-	L	-	M
[oswindows] oswindows2000server	M	-	L	-	-
[ossolaris] solaris	M	-	L	-	-
[appsmanagement] logisticsexternalpatients	M	-	L	-	-
[serverprot] questwinerserver	M	-	L	-	-
[serverpatients] compaqprolianthtml370	M	-	L	-	-
[COM.LAN] Local Area Network	L	M	L	M	M

[E.18] Destruction of information

asset	*level*	[A]	[I]	[C]	[V]
[datapdpsn] datadpsn	0	M	-	-	-
[S_blooddata] s_blooddata	M	L	-	-	-
[s_eprotocol] s_eprotocol		L	-	-	-
[appdpsn] appdpsn	M	L	-	-	M
[ossw] os	M	H	-	-	M
[ospcwindows] ospcwindows	M	H	-	-	M
[oswindows] oswindows2000server	M	H	-	-	M

[ossolaris] solaris	M	H	-	-	-
[appsmanagement] logisticsexternalpatients	M	H	-	-	-
[serverpatients] compaqprolianttml370	M	L	-	-	-

[E.19] Information leaks

asset	***level***	[A]	[I]	[C]	[V]
[S_blooddata] s_blooddata		-	-	M	-
[s_eprotocol] s_eprotocol		-	-	M	-
[appdpsn] appdpsn	M	-	-	M	M
[ossw] os	M	-	-	M	M
[ospcwindows] ospcwindows	M	-	-	M	-
[oswindows] oswindows2000server	M	-	-	M	-
[ossolaris] solaris	M	-	-	M	-
[appsmanagement] logisticsexternalpatients	M	-	-	M	-
[serverpatients] compaqprolianttml370	M	-	-	M	-
[COM.LAN] Local Area Network	L	L	L	L	L

[E.20] Software vulnerabilities

asset	***level***	[A]	[I]	[C]	[V]
[ossw] os	M	L	M	M	M
[ospcwindows] ospcwindows	M	L	M	M	-
[oswindows] oswindows2000server	M	L	M	M	-
[ossolaris] solaris	M	L	M	M	-
[appsmanagement] logisticsexternalpatients	M	L	M	M	-
[serverprot] questwinerserver	VL	L	L	L	L

[E.21] Defects in software maintenance / updating

asset	***level***	[A]	[I]	[C]	[V]
[ossw] os	H	L	L	-	M
[ospcwindows] ospcwindows	H	L	L	-	-
[oswindows] oswindows2000server	H	L	L	-	-
[ossolaris] solaris	H	L	L	-	-
[appsmanagement] logisticsexternalpatients	H	L	L	-	-
[serverprot] questwinerserver	VL	L	L	L	L

[E.23] Defects in hardware maintenance / updating

asset	***level***	[A]	[I]	[C]	[V]
[serverprot] questwinerserver	M	M	-	-	-
[serverpatients] compaqproliantml370	VL	L	L	L	L
[serverblood] compaqproliantml370g3	M	M	-	-	-
[personalcomputer] pcwindows	VL	L	L	L	L

[E.24] System failure due to exhaustion of resources

asset	***level***	[A]	[I]	[C]	[V]
[serverprot] questwinerserver	H	H	-	-	-
[serverpatients] compaqproliantml370	H	H	-	-	-
[serverblood] compaqproliantml370g3	H	H	-	-	-
[personalcomputer] pcwindows	M	M	M	M	M
[COM.LAN] Local Area Network	L	L	L	L	L

[E.25] Equipment loss

asset	*level*	[A]	[I]	[C]	[V]
[serverprot] questwinerserver	L	T	-	T	-
[serverpatients] compaqprolia ntml370	L	T	-	T	-
[serverblood] compaqprolia ntml370g3	L	T	-	T	-
[personalcomputer] pcwindows	0	-	-	-	-

[A.3] Manipulation of activity records (log)

asset	*level*	[A]	[I]	[C]	[V]
[serverpatients] compaqprolia ntml370	VL	L	L	L	VH

[A.5] Masquerading of identity

asset	*level*	[A]	[I]	[C]	[V]
[datapdpsn] datadpsn	H	H	H	H	H
[S_blooddata] s_blooddata		H	H	VH	H
[s_eprotocol] s_eprotocol		H	VH	H	H
[appdpsn] appdpsn	H	-	M	H	M
[ossw] os	M	-	H	H	M
[ospcwindows] ospcwindows	M	-	H	H	-
[oswindows] oswindows200server	M	-	H	H	-
[ossolaris] solaris	M	-	H	H	-
[appsmanagement] logisticsexternalpatients	M	-	H	H	-
[serverprot] questwinerserver	M	-	H	H	-
[serverpatients] compaqprolia ntml370	H	-	M	H	-
[COM.LAN] Local Area Network	L	L	L	L	H

[A.5.1] By insiders

asset	*level*	[A]	[I]	[C]	[V]
[datalabpatients] datapatients	H	H	H	H	H
[dataemployees] dataemployees	M	H	H	H	H
[financial] finlogisticssubcontractor	M	M	H	M	M

[A.5.3] By outsiders

asset	*level*	[A]	[I]	[C]	[V]
[datalabpatients] datapatients	H	H	H	VH	H
[dataemployees] dataemployees	L	H	H	H	L
[financial] finlogisticssubcontractor	H	H	H	H	L

[A.6] Abuse of access privileges

asset	*level*	[A]	[I]	[C]	[V]
[datapdpsn] datadpsn	L	L	L	L	L
[S_blooddata] s_blooddata		L	M	L	L
[s_eprotocol] s_eprotocol		L	L	L	L
[appdpsn] appdpsn	H	L	M	H	M
[ossw] os	M	L	M	M	M
[ospcwindows] ospcwindows	M	L	M	M	-
[oswindows] oswindows2000server	M	L	M	M	-
[ossolaris] solaris	M	L	M	M	-
[appsmanagement] logisticsexternalpatients	M	L	M	M	-
[serverprot] questwinerserver	M	M	M	H	-
[serverpatients] compaqproliantml370	M	M	M	H	-
[serverblood] compaqproliantml370g3	M	M	M	H	-
[personalcomputer] pcwindows	0	-	-	-	-
[COM.LAN]	M	M	M	H	M

Local Area Network					

[A.7] Misuse

asset	***level***	[A]	[I]	[C]	[V]
[ossw] os	M	L	M	M	M
[ospcwindows] ospcwindows	M	L	M	M	-
[oswindows] oswindows200server	M	L	M	M	-
[ossolaris] solaris	M	L	M	M	-
[appsmanagement] logisticsexternalpatients	M	L	M	M	-
[serverprot] questwinerserver	M	L	L	M	-
[serverpatients] compaqproliantml370	M	L	L	M	-
[serverblood] compaqproliantml370g3	M	L	L	M	-
[personalcomputer] pcwindows	0	-	-	-	-
[COM.LAN] Local Area Network	M	M	M	M	M
[offices] workingroomisthodosias	M	M	M	H	-
[hospitaldepartments] hospitaldepartments	M	M	M	H	-

[A.8] Malware diffusion

asset	***level***	[A]	[I]	[C]	[V]
[ossw] os	M	T	T	T	M
[ospcwindows] ospcwindows	M	M	M	-	M
[oswindows] oswindows200server	M	T	T	T	-
[ossolaris] solaris	M	T	T	T	-
[appsmanagement] logisticsexternalpatients	M	T	T	T	-
[serverprot] questwinerserver	M	T	T	T	-

[A.9] [Re-]routing of messages

asset	*level*	[A]	[I]	[C]	[V]
[COM.LAN] Local Area Network	M	M	M	M	M

[A.10] Sequence alteration

asset	*level*	[A]	[I]	[C]	[V]
[COM.LAN] Local Area Network	M	M	M	M	M

[A.11] Unauthorised access

asset	*level*	[A]	[I]	[C]	[V]
[datapdpsn] datadpsn	0	-	-	-	-
[S_blooddata] s_blooddata		-	M	H	-
[s_eprotocol] s_eprotocol		-	M	H	-
[appdpsn] appdpsn	VH	-	M	H	-
[ossw] os	M	-	M	H	M
[ospcwindows] ospcwindows	M	-	M	H	-
[oswindows] oswindows2000server	M	-	M	H	-
[ossolaris] solaris	M	-	M	H	-
[appsmanagement] logisticsexternalpatients	M	-	M	H	-
[serverprot] questwinerserver	M	M	M	H	-
[serverpatients] compaqprolia ntml370	M	M	M	H	-
[serverblood] compaqprolia ntml370g3	M	M	M	H	-
[personalcomputer] pcwindows	0	-	-	-	-
[COM.LAN] Local Area Network	M	M	M	H	M
[offices] workingroom isthodosias	H	-	M	H	-
[dc] datacenterpliroforikhsorganwsis	H	-	M	H	-
[secretary] secretary	H	-	M	H	-
[aimodosia] workingroom	H	-	M	H	-

aimodosia					
[hospitaldepartments] hospitaldepartments	H	-	M	H	-

[A.12] Traffic analysis

asset	***level***	[A]	[I]	[C]	[V]
[COM.LAN] Local Area Network	M	M	M	L	M

[A.13] Repudiation (denial of actions)

asset	***level***	[A]	[I]	[C]	[V]
[serverpatients] compaqprolia ntml370	H	-	T	-	-

[A.14] Eavesdropping

asset	***level***	[A]	[I]	[C]	[V]
[COM.LAN] Local Area Network	M	M	M	L	M

[A.15] Deliberate alteration of information

asset	***level***	[A]	[I]	[C]	[V]
[datapdpsn] datadpsn	0	-	-	-	-
[S_blooddata] s_blooddata		-	T	-	-
[s_eprotocol] s_eprotocol		-	T	-	-
[appdpsn] appdpsn	H	-	T	-	-
[ossw] os	M	-	H	-	M
[ospcwindows] ospcwindows	M	-	H	-	-
[oswindows] oswindows200server	M	-	H	-	-
[ossolaris] solaris	M	-	H	-	-
[appsmanagement] logisticsexternalpatients	M	-	H	-	-
[serverprot] questwinerserver	M	-	H	-	-
[serverpatients] compaqprolia ntml370	H	-	T	-	-
[COM.LAN] Local Area Network	M	M	M	M	M

[A.18] Destruction of information

asset	***level***	[A]	[I]	[C]	[V]
[datapdpsn] datadpsn	0	-	-	-	-
[S_blooddata] s_blooddata	H	H	-	-	-
[s_eprotocol] s_eprotocol		H	-	-	-
[appdpsn] appdpsn	H	H	-	-	-
[ossw] os	M	H	-	-	M
[ospcwindows] ospcwindows	M	H	-	-	-
[oswindows] oswindows2000server	M	H	-	-	-
[ossolaris] solaris	M	H	-	-	-
[appsmanagement] logisticsexternalpatients	M	H	-	-	-
[serverprot] questwinerserver	M	H	-	-	-
[serverpatients] compaqprolia ntml370	H	H	-	-	-
[COM.LAN] Local Area Network	M	H	M	M	M

[A.19] Disclosure of information

asset	***level***	[A]	[I]	[C]	[V]
[datapdpsn] datadpsn	0	-	-	-	-
[S_blooddata] s_blooddata	H	-	-	T	-
[s_eprotocol] s_eprotocol		-	-	T	-
[appdpsn] appdpsn	H	-	-	T	-
[ossw] os	M	-	-	H	M
[ospcwindows] ospcwindows	M	-	-	H	-
[oswindows] oswindows2000server	M	-	-	H	-
[ossolaris] solaris	M	-	-	H	-
[appsmanagement] logisticsexter	M	-	-	H	-

nalpatients					
[serverprot] questwinerserver	M	-	-	H	-
[serverpatients] compaqprolia ntml370	H	-	-	T	-
[COM.LAN] Local Area Network	M	M	M	H	M

[A.22] Software manipulation

asset	***level***	[A]	[I]	[C]	[V]
[ossw] os	M	H	T	T	M
[ospcwindows] ospcwindows	M	H	T	T	-
[oswindows] oswindows200server	M	H	T	T	-
[ossolaris] solaris	M	H	T	T	-
[appsmanagement] logisticsexternalpatients	M	H	T	T	-
[serverprot] questwinerserver	M	H	T	T	-

[A.23] Hardware manipulation

asset	***level***	[A]	[I]	[C]	[V]
[serverprot] questwinerserver	M	H	-	H	-
[serverpatients] compaqprolia ntml370	VL	L	L	L	H
[serverblood] compaqprolia ntml370g3	L	L	L	L	L
[personalcomputer] pcwindows	M	M	M	M	M

[A.24] Denial of service

asset	***level***	[A]	[I]	[C]	[V]
[serverprot] questwinerser	M	T	-	-	-

ver					
[serverpatients] compaqprolia ntml370	M	T	-	-	-
[serverblood] compaqprolia ntml370g3	M	T	-	-	-
[personalcomputer] pcwindows	0	-	-	-	-
[COM.LAN] Local Area Network	H	H	M	M	M

[A.25] Theft

asset	***level***	[A]	[I]	[C]	[V]
[serverprot] questwinerserver	M	M	M	M	M
[serverpatients] compaqprolia ntml370	M	M	M	M	M
[serverblood] compaqprolia ntml370g3	VL	L	L	L	L
[personalcomputer] pcwindows	0	-	-	-	-

[A.26] Destructive attack

asset	***level***	[A]	[I]	[C]	[V]
[serverpatients] compaqprolia ntml370	L	L	L	L	L
[serverblood] compaqprolia ntml370g3	VL	L	L	L	L
[personalcomputer] pcwindows	VL	L	L	L	L
[offices] workingroom isthodosias	L	L	L	L	L
[dc] datacenterpliroforikhsorganwsis	L	L	L	L	L
[secretary] secretary	L	L	L	L	L
[aimodosia] workingroom aimodosia	L	L	L	L	L
[hospitaldepartments] hospitaldepartments	VL	L	L	L	L

[A.27] Enemy over-run

asset	***level***	[A]	[I]	[C]	[V]
[offices] workingroom isthodosias	L	T	-	H	L
[dc] datacenterplir oforikhsorga nwsis	L	T	-	H	L
[secretary] secretary	VL	T	-	H	-
[aimodosia] workingroom aimodosia	M	T	-	H	-
[hospitaldepa rtments] hospitaldepar tments	VL	T	-	H	-

Παράρτημα Ε: Ανακλώμενος Κίνδυνος

Ανακλώμενος Κίνδυνος (Deflected Risk)

Parent	Child	Threat	Risk	Current	Target	Pilar
[dataemployees] dataemployees	[serverpatients] compaqproliantml370	[I.6] Power interruption	1,05E+12	1,37E+10	4,67E+07	3,65E+08
[dataemployees] dataemployees	[appsfinancialwindowspc] logisticsexternalpatients	[I.5] Hardware or software failure	5,25E+11	6,16E+09	2,10E+07	1,46E+08
[dataemployees] dataemployees	[ospcwindows] ospcwindows	[I.5] Hardware or software failure	5,25E+11	6,16E+09	2,10E+07	1,46E+08
[dataemployees] dataemployees	[ossolaris] solaris	[I.5] Hardware or software failure	5,25E+11	6,16E+09	2,10E+07	1,46E+08
[datalabpatients] datapatients	[serverblood] compaqproliantml370g3	[I.6] Power interruption	2,26E+11	2,95E+09	1,00E+07	7,84E+07
[financial] finlogisticssubcontractor	[serverprot] questwinerserver	[I.6] Power interruption	2,26E+11	2,95E+09	1,00E+07	7,84E+07
[datalabpatients] datapatients	[ossw] os	[I.5] Hardware or software failure	1,13E+11	1,32E+09	4,52E+06	3,18E+07
[financial] finlogisticssubcontractor	[oswindows] oswindows200server	[I.5] Hardware or software failure	1,13E+11	1,32E+09	4,52E+06	3,18E+07
[dataemployees] dataemployees	[aimodosia] workingroomaimodosia	[I.3] Environmental pollution	1,05E+11	1,69E+09	5,58E+06	4,50E+07
[datalabpatients] datapatients	[aimodosia] workingroomaimodosia	[I.3] Environmental pollution	2,26E+10	3,64E+08	1,20E+06	9,67E+06
[datalabpatients] datapatients	[serverblood] compaqproliantml370g3	[I.4] Electromagnetic pollution	2,26E+10	3,94E+08	1,27E+06	1,23E+07
[dataemployees] dataemployees	[ospcwindows] ospcwindows	[I.5] Hardware or software failure	2,26E+10	2,65E+08	0.904486	6,45E+06
[datalabpatients] datapatients	[serverblood] compaqproliantml370g3	[N.*] Other natural disasters	2,26E+10	4,00E+08	1,29E+06	1,68E+07
[financial] finlogisticssubcontractor	[serverprot] questwinerserver	[N.*] Other natural disasters	2,26E+10	4,00E+08	1,29E+06	1,67E+07
[datalabpatients] datapatients	[ossw] os	[I.5] Hardware or software failure	1,05E+10	1,23E+08	0.420691	3,05E+06
[dataemployees] dataemployees	[aimodosia] workingroomaimodosia	[N.1] Fire	1,00E+10	1,31E+08	0,00E+00	5,06E+06
[dataemployees] dataemployees	[hospitaldepartments] hospitaldepartments	[N.1] Fire	1,00E+10	1,31E+08	0,00E+00	5,06E+06
[dataemployees] dataemployees	[aimodosia] workingroomaimodosia	[N.2] Water	1,00E+10	1,77E+08	0,00E+00	5,50E+06
[financial] finlogisticssubcontractor	[secretary] secretary	[I.4] Electromagnetic pollution	2,26E+09	2,75E+07	0.093943	0.779401
[datalabpatients] datapatients	[serverblood] compaqproliantml370g3	[I.11] Electromagnetic emanations	2,26E+09	3,62E+07	0.119253	1,49E+06
[datalabpatients] datapatients	[aimodosia] workingroomaimodosia	[N.1] Fire	2,15E+09	2,81E+07	0,00E+00	1,09E+06
[datalabpatients] datapatients	[aimodosia] workingroomaimodosia	[N.2] Water	2,15E+09	3,81E+07	0,00E+00	1,18E+06
[financial] finlogisticssubcontractor	[secretary] secretary	[N.1] Fire	2,15E+09	2,81E+07	0,00E+00	1,09E+06
[financial] finlogisticssubcontractor	[secretary] secretary	[N.2] Water	2,15E+09	3,81E+07	0,00E+00	1,19E+06
[dataemployees] dataemployees	[COM.LAN] Local Area Network	[I.8] Communications services failure	1,00E+09	1,31E+07	0.044881	0.487427
[datalabpatients] datapatients	[aimodosia] workingroomaimodosia	[I.11] Electromagnetic emanations	2,26E+08	2,79E+06	0.009521	0.067073
[dataemployees] dataemployees	[dc] datacenterpliroforikhsorganwsis	[I.11] Electromagnetic emanations	2,26E+08	2,79E+06	0.009521	0.067940
[dataemployees] dataemployees	[aimodosia] workingroomaimodosia	[I.11] Electromagnetic emanations	2,26E+08	2,79E+06	0.009521	0.067073
[dataemployees] dataemployees	[hospitaldepartments] hospitaldepartments	[I.11] Electromagnetic emanations	2,26E+08	2,79E+06	0.009521	0.067940
[dataemployees] dataemployees	[COM.LAN] Local Area Network	[I.8] Communications services failure	2,15E+08	3,45E+06	0.011357	0.098770
[dataemployees] dataemployees	[serverpatients] compaqproliantml370	[N.1] Fire	1,00E+08	1,77E+06	0,00E+00	0.075674
[dataemployees] dataemployees	[offices] workingroomisthodosias	[N.1] Fire	1,00E+08	1,31E+06	0,00E+00	0.051446
[dataemployees] dataemployees	[serverpatients] compaqproliantml370	[N.2] Water	1,00E+08	1,77E+06	0,00E+00	0.075674
[dataemployees] dataemployees	[personalcomputer] pcwindows	[N.1] Fire	1,00E+08	1,24E+06	0,00E+00	0.048982
[dataemployees] dataemployees	[dc] datacenterpliroforikhsorganwsis	[N.2] Water	1,00E+08	1,77E+06	0,00E+00	0.056015
[dataemployees] dataemployees	[offices] workingroomisthodosias	[N.2] Water	1,00E+08	1,77E+06	0,00E+00	0.056015
[dataemployees] dataemployees	[aimodosia] workingroomaimodosia	[N.*] Other natural disasters	1,00E+08	1,79E+06	0,00E+00	0.061995
[dataemployees] dataemployees	[hospitaldepartments] hospitaldepartments	[N.*] Other natural disasters	1,00E+08	1,79E+06	0,00E+00	0.062332
[dataemployees] dataemployees	[personalcomputer] pcwindows	[N.2] Water	1,00E+08	1,24E+06	0,00E+00	0.048982

[dataemployees] dataemployees	[dc] datacenterpliroforikhsorganwsis	[N.*] Other natural disasters	1,00E+08	1,79E+06	0,00E+00	0.062332
[dataemployees] dataemployees	[offices] workingroomisthodosias	[N.*] Other natural disasters	1,00E+08	1,79E+06	0,00E+00	0.062332
[dataemployees] dataemployees	[dc] datacenterpliroforikhsorganwsis	[N.1] Fire	1,00E+08	1,31E+06	0,00E+00	0.051446
[dataemployees] dataemployees	[hospitaldepartments] hospitaldepartments	[N.2] Water	1,00E+08	1,77E+06	0,00E+00	0.056015
[financial] finlogisticssubcontractor	[secretary] secretary	[N.*] Other natural disasters	1,00E+08	1,74E+06	0,00E+00	0.047400
[financial] finlogisticssubcontractor	[serverprot] questwinerserver	[N.1] Fire	1,00E+08	1,74E+06	0,00E+00	0.056540
[financial] finlogisticssubcontractor	[serverprot] questwinerserver	[N.2] Water	1,00E+08	1,74E+06	0,00E+00	0.056540
[datalabpatients] datapatients	[serverblood] compaqproliantml370g3	[N.2] Water	2,15E+07	0.381031	0,00E+00	0.016270
[datalabpatients] datapatients	[aimodosia] workingroomaimodosia	[N.*] Other natural disasters	2,15E+07	0.384547	0,00E+00	0.013329
[datalabpatients] datapatients	[serverblood] compaqproliantml370g3	[I.5] Hardware or software failure	2,15E+07	0.349759	0,00E+00	0.010612
[datalabpatients] datapatients	[serverblood] compaqproliantml370g3	[N.1] Fire	2,15E+07	0.381031	0,00E+00	0.016270
[datalabpatients] datapatients	[aimodosia] workingroomaimodosia	[N.*] Other natural disasters	2,15E+07	0.374887	0,00E+00	0.010191
[datalabpatients] datapatients	[serverblood] compaqproliantml370g3	[N.1] Fire	2,15E+07	0.374887	0,00E+00	0.012156
[datalabpatients] datapatients	[serverblood] compaqproliantml370g3	[N.2] Water	2,15E+07	0.374887	0,00E+00	0.012156
[datalabpatients] datapatients	[serverblood] compaqproliantml370g3	[I.5] Hardware or software failure	2,15E+07	0.345043	0,00E+00	0.013989
[dataemployees] dataemployees	[serverpatients] compaqproliantml370	[N.1] Fire	2,15E+07	0.374887	0,00E+00	0.012156
[dataemployees] dataemployees	[serverpatients] compaqproliantml370	[N.2] Water	2,15E+07	0.374887	0,00E+00	0.012156
[dataemployees] dataemployees	[personalcomputer] pcwindows	[N.2] Water	2,15E+07	0.252282	0,00E+00	0.006653
[dataemployees] dataemployees	[personalcomputer] pcwindows	[N.1] Fire	2,15E+07	0.252282	0,00E+00	0.006653
[dataemployees] dataemployees	[hospitaldepartments] hospitaldepartments	[N.2] Water	2,15E+07	0.380011	0,00E+00	0.009865
[dataemployees] dataemployees	[aimodosia] workingroomaimodosia	[N.*] Other natural disasters	2,15E+07	0.374887	0,00E+00	0.010191
[dataemployees] dataemployees	[hospitaldepartments] hospitaldepartments	[N.*] Other natural disasters	2,15E+07	0.374887	0,00E+00	0.010191
[dataemployees] dataemployees	[dc] datacenterpliroforikhsorganwsis	[N.1] Fire	2,15E+07	0.280146	0,00E+00	0.009467
[dataemployees] dataemployees	[dc] datacenterpliroforikhsorganwsis	[N.*] Other natural disasters	2,15E+07	0.374887	0,00E+00	0.010191
[dataemployees] dataemployees	[dc] datacenterpliroforikhsorganwsis	[N.2] Water	2,15E+07	0.380011	0,00E+00	0.009865
[dataemployees] dataemployees	[offices] workingroomisthodosias	[N.1] Fire	2,15E+07	0.280146	0,00E+00	0.009467
[dataemployees] dataemployees	[offices] workingroomisthodosias	[N.2] Water	2,15E+07	0.380011	0,00E+00	0.009865
[dataemployees] dataemployees	[offices] workingroomisthodosias	[N.*] Other natural disasters	2,15E+07	0.374887	0,00E+00	0.010191
[dataemployees] dataemployees	[aimodosia] workingroomaimodosia	[N.*] Other natural disasters	2,15E+07	0.374887	0,00E+00	0.010191
[dataemployees] dataemployees	[dc] datacenterpliroforikhsorganwsis	[N.1] Fire	2,15E+07	0.280146	0,00E+00	0.009467
[dataemployees] dataemployees	[hospitaldepartments] hospitaldepartments	[N.*] Other natural disasters	2,15E+07	0.374887	0,00E+00	0.010191
[dataemployees] dataemployees	[offices] workingroomisthodosias	[N.2] Water	2,15E+07	0.380011	0,00E+00	0.009865
[dataemployees] dataemployees	[personalcomputer] pcwindows	[N.2] Water	2,15E+07	0.252282	0,00E+00	0.006653
[dataemployees] dataemployees	[hospitaldepartments] hospitaldepartments	[N.2] Water	2,15E+07	0.380011	0,00E+00	0.009865
[dataemployees] dataemployees	[serverpatients] compaqproliantml370	[N.2] Water	2,15E+07	0.374887	0,00E+00	0.012156
[dataemployees] dataemployees	[personalcomputer] pcwindows	[N.1] Fire	2,15E+07	0.252282	0,00E+00	0.006653
[dataemployees] dataemployees	[serverpatients] compaqproliantml370	[N.1] Fire	2,15E+07	0.374887	0,00E+00	0.012156
[dataemployees] dataemployees	[offices] workingroomisthodosias	[N.1] Fire	2,15E+07	0.280146	0,00E+00	0.009467
[dataemployees] dataemployees	[dc] datacenterpliroforikhsorganwsis	[N.*] Other natural disasters	2,15E+07	0.374887	0,00E+00	0.010191
[dataemployees] dataemployees	[dc] datacenterpliroforikhsorganwsis	[N.2] Water	2,15E+07	0.380011	0,00E+00	0.009865
[dataemployees] dataemployees	[offices] workingroomisthodosias	[N.*] Other natural disasters	2,15E+07	0.374887	0,00E+00	0.010191
[dataemployees] dataemployees	[dc] datacenterpliroforikhsorganwsis	[N.*] Other natural disasters	2,15E+07	0.374887	0,00E+00	0.010191
[dataemployees] dataemployees	[personalcomputer] pcwindows	[N.2] Water	2,15E+07	0.252282	0,00E+00	0.006653
[dataemployees] dataemployees	[offices] workingroomisthodosias	[N.*] Other natural disasters	2,15E+07	0.374887	0,00E+00	0.010191

[dataemployees] dataemployees	[dc] datacenterpliroforikhsorganwsis	[N.1] Fire	2,15E+07	0.280146	0,00E+00	0.009467
[dataemployees] dataemployees	[serverpatients] compaqproliantml370	[N.1] Fire	2,15E+07	0.374887	0,00E+00	0.012156
[dataemployees] dataemployees	[offices] workingroomisthodosias	[N.1] Fire	2,15E+07	0.280146	0,00E+00	0.009467
[dataemployees] dataemployees	[serverpatients] compaqproliantml370	[N.2] Water	2,15E+07	0.374887	0,00E+00	0.012156
[dataemployees] dataemployees	[personalcomputer] pcwindows	[N.1] Fire	2,15E+07	0.252282	0,00E+00	0.006653
[dataemployees] dataemployees	[dc] datacenterpliroforikhsorganwsis	[N.2] Water	2,15E+07	0.380011	0,00E+00	0.009865
[dataemployees] dataemployees	[hospitaldepartments] hospitaldepartments	[N.2] Water	2,15E+07	0.380011	0,00E+00	0.009865
[dataemployees] dataemployees	[aimodosia] workingroomaimodosia	[N.*] Other natural disasters	2,15E+07	0.374887	0,00E+00	0.010191
[dataemployees] dataemployees	[hospitaldepartments] hospitaldepartments	[N.*] Other natural disasters	2,15E+07	0.374887	0,00E+00	0.010191
[financial] finlogisticssubcontractor	[serverprot] questwinerserver	[N.1] Fire	2,15E+07	0.381031	0,00E+00	0.016148
[financial] finlogisticssubcontractor	[serverprot] questwinerserver	[N.2] Water	2,15E+07	0.381031	0,00E+00	0.016148
[financial] finlogisticssubcontractor	[secretary] secretary	[N.*] Other natural disasters	2,15E+07	0.384547	0,00E+00	0.013401
[financial] finlogisticssubcontractor	[serverprot] questwinerserver	[N.1] Fire	2,15E+07	0.374887	0,00E+00	0.012156
[financial] finlogisticssubcontractor	[serverprot] questwinerserver	[N.2] Water	2,15E+07	0.374887	0,00E+00	0.012156
[financial] finlogisticssubcontractor	[secretary] secretary	[N.*] Other natural disasters	2,15E+07	0.374887	0,00E+00	0.010191
[datalabpatients] datapatients	[serverblood] compaqproliantml370g3	[I.5] Hardware or software failure	1,00E+07	0.160485	0,00E+00	0.006506
[datalabpatients] datapatients	[serverblood] compaqproliantml370g3	[N.1] Fire	1,00E+07	0.174366	0,00E+00	0.005654
[datalabpatients] datapatients	[serverblood] compaqproliantml370g3	[N.2] Water	1,00E+07	0.174366	0,00E+00	0.005654
[datalabpatients] datapatients	[aimodosia] workingroomaimodosia	[N.*] Other natural disasters	1,00E+07	0.174366	0,00E+00	0.004740
[datalabpatients] datapatients	[serverblood] compaqproliantml370g3	[N.1] Fire	1,00E+07	0.174366	0,00E+00	0.005654
[datalabpatients] datapatients	[serverblood] compaqproliantml370g3	[N.2] Water	1,00E+07	0.174366	0,00E+00	0.005654
[datalabpatients] datapatients	[aimodosia] workingroomaimodosia	[N.*] Other natural disasters	1,00E+07	0.174366	0,00E+00	0.004740
[financial] finlogisticssubcontractor	[serverprot] questwinerserver	[N.2] Water	1,00E+07	0.174366	0,00E+00	0.005654
[financial] finlogisticssubcontractor	[secretary] secretary	[N.*] Other natural disasters	1,00E+07	0.174366	0,00E+00	0.004740
[financial] finlogisticssubcontractor	[serverprot] questwinerserver	[N.1] Fire	1,00E+07	0.174366	0,00E+00	0.005654

ΠΑΡΑΡΤΗΜΑ ΣΤ:Εναπομείναν κίνδυνος

project: [nos1] nos1

	Asset	Threat	Dimension	Risk	Current	Target	PILAR
[s_eprotocol] s_eprotocol	[E.2] System / Security administrator errors	[I]	2,00E+13	2,00E+13	2,12E+11	2,55E+09	4,38E+09
[appdpsn] appdpsnsolarisml370	[E.2] System / Security administrator errors	[A]	2,00E+13	2,00E+13	1,68E+11	7,43E+08	4,65E+09
[appdpsn] appdpsnsolarisml370	[A.11] Unauthorised access	[C]	1,04E+13	1,04E+13	1,32E+11	7,13E+08	2,17E+09
[datapdpsn] datadpsn	[E.2] System / Security administrator errors	[A]	1,00E+13	1,00E+13	7,87E+10	3,70E+08	2,78E+09
[COM.LAN] Local Area Network	[A.24] Denial of service	[A]	6,06E+12	6,06E+12	7,37E+10	2,52E+08	2,72E+09
[serverpatients] compaqproliantml370	[E.24] System failure due to exhaustion of resources	[A]	5,77E+12	5,77E+12	7,18E+10	2,45E+08	1,91E+09
[appdpsn] appdpsnsolarisml370	[E.1] User errors	[A]	5,77E+12	5,77E+12	4,86E+10	2,15E+08	1,35E+09
[financial] finlogisticssubcontractor	[A.5.3] By outsiders	[I]	5,00E+12	5,00E+12	4,82E+10	1,70E+08	1,05E+09
[datapdpsn] datadpsn	[A.5] Masquerading of identity	[A]	5,00E+12	5,00E+12	4,82E+10	1,70E+08	1,05E+09
[appdpsn] appdpsnsolarisml370	[A.18] Destruction of information	[A]	4,85E+12	4,85E+12	4,38E+10	1,87E+08	1,03E+09
[serverpatients] compaqproliantml370	[A.18] Destruction of information	[A]	4,85E+12	4,85E+12	6,46E+10	2,55E+08	1,65E+09
[appdpsn] appdpsnsolarisml370	[E.2] System / Security administrator errors	[I]	4,30E+12	4,30E+12	4,41E+10	4,68E+08	9,35E+08
[s_eprotocol] s_eprotocol	[E.2] System / Security administrator errors	[A]	4,30E+12	4,30E+12	3,61E+10	1,59E+08	1,02E+09
[appdpsn] appdpsnsolarisml370	[E.2] System / Security administrator errors	[C]	4,30E+12	4,30E+12	4,05E+10	2,69E+08	8,70E+08
[s_eprotocol] s_eprotocol	[E.2] System / Security administrator errors	[C]	4,30E+12	4,30E+12	4,05E+10	2,69E+08	8,76E+08
[serverpatients] compaqproliantml370	[A.24] Denial of service	[A]	2,43E+12	2,43E+12	3,00E+10	1,02E+08	1,08E+09
[appdpsn] appdpsnsolarisml370	[E.2] System / Security administrator errors	[V]	2,15E+12	2,15E+12	1,66E+10	7,72E+07	3,94E+08
[datapdpsn] datadpsn	[E.2] System / Security administrator errors	[C]	2,15E+12	2,15E+12	1,52E+10	7,67E+07	4,74E+08
[datapdpsn] datadpsn	[E.2] System / Security administrator errors	[I]	2,15E+12	2,15E+12	1,52E+10	7,67E+07	4,74E+08
[datapdpsn] datadpsn	[E.2] System / Security administrator errors	[V]	2,15E+12	2,15E+12	1,52E+10	7,67E+07	4,75E+08
[appdpsn] appdpsnsolarisml370	[A.11] Unauthorised access	[I]	2,09E+12	2,09E+12	2,48E+10	8,46E+07	4,34E+08
[serverpatients] compaqproliantml370	[A.19] Disclosure of information	[C]	2,09E+12	2,09E+12	2,99E+10	2,20E+08	6,79E+08
[S_blooddata] s_blooddata	[A.19] Disclosure of information	[C]	2,09E+12	2,09E+12	1,96E+10	1,31E+08	4,09E+08
[appdpsn] appdpsnsolarisml370	[A.15] Deliberate alteration of information	[I]	2,09E+12	2,09E+12	2,15E+10	2,27E+08	4,47E+08
[appdpsn] appdpsnsolarisml370	[A.19] Disclosure of information	[C]	2,09E+12	2,09E+12	1,96E+10	1,31E+08	4,17E+08

[serverpatients] compaqproliantml370	[A.15] Deliberate alteration of information	[I]	2,09E+12	2,09E+12	3,16E+10	2,60E+08	7,58E+08
[datalabpatients] datapatients	[A.5.3] By outsiders	[C]	1,94E+12	1,94E+12	1,86E+10	6,58E+07	4,07E+08
[appdpsn] appdpsnsolarisml370	[A.6] Abuse of access privileges	[C]	1,30E+12	1,30E+12	1,23E+10	8,17E+07	2,64E+08
[serverprot] questwinerserver	[E.24] System failure due to exhaustion of resources	[A]	1,24E+12	1,24E+12	1,43E+10	4,89E+07	3,96E+08
[appdpsn] appdpsnsolarisml370	[E.1] User errors	[V]	1,24E+12	1,24E+12	9,57E+09	4,46E+07	2,28E+08
[appdpsn] appdpsnsolarisml370	[E.1] User errors	[C]	1,24E+12	1,24E+12	1,17E+10	7,78E+07	2,51E+08
[serverblood] compaqproliantml370g3	[E.24] System failure due to exhaustion of resources	[A]	1,24E+12	1,24E+12	1,52E+10	5,19E+07	3,93E+08
[appdpsn] appdpsnsolarisml370	[E.1] User errors	[I]	1,24E+12	1,24E+12	1,27E+10	1,35E+08	2,70E+08
[aimodosia] workingroomaimodosia	[A.27] Enemy over-run	[A]	1,22E+12	1,22E+12	1,58E+10	5,40E+07	6,84E+08
[serverprot] questwinerserver	[A.22] Software manipulation	[I]	1,21E+12	1,21E+12	1,61E+10	7,70E+07	4,80E+08
[oswindows] oswindows200server	[A.22] Software manipulation	[I]	1,21E+12	1,21E+12	1,52E+10	7,70E+07	6,31E+08
[serverpatients] compaqproliantml370	[E.1] User errors	[A]	1,15E+12	1,15E+12	1,47E+10	5,92E+07	4,29E+08
[datalabpatients] datapatients	[A.5.3] By outsiders	[A]	1,08E+12	1,08E+12	1,04E+10	3,65E+07	2,26E+08
[datapdpsn] datadpsn	[A.5] Masquerading of identity	[V]	1,08E+12	1,08E+12	1,04E+10	3,65E+07	2,26E+08
[datalabpatients] datapatients	[A.5.1] By insiders	[C]	1,08E+12	1,08E+12	1,04E+10	3,65E+07	2,26E+08
[financial] finlogisticssubcontractor	[A.5.3] By outsiders	[C]	1,08E+12	1,08E+12	1,04E+10	3,65E+07	2,26E+08
[datapdpsn] datadpsn	[A.5] Masquerading of identity	[C]	1,08E+12	1,08E+12	1,04E+10	3,65E+07	2,26E+08
[datalabpatients] datapatients	[A.5.1] By insiders	[A]	1,08E+12	1,08E+12	1,04E+10	3,65E+07	2,26E+08
[datapdpsn] datadpsn	[A.5] Masquerading of identity	[I]	1,08E+12	1,08E+12	1,04E+10	3,65E+07	2,26E+08
[financial] finlogisticssubcontractor	[A.5.3] By outsiders	[A]	1,08E+12	1,08E+12	1,04E+10	3,65E+07	2,26E+08
[S_blooddata] s_blooddata	[A.18] Destruction of information	[A]	1,04E+12	1,04E+12	9,36E+09	4,00E+07	2,15E+08
[aimodosia] workingroomaimodosia	[A.11] Unauthorised access	[C]	1,04E+12	1,04E+12	1,20E+10	4,08E+07	2,02E+08
[serverpatients] compaqproliantml370	[A.5] Masquerading of identity	[C]	1,04E+12	1,04E+12	2,32E+10	1,16E+09	1,83E+08
[appdpsn] appdpsnsolarisml370	[A.5] Masquerading of identity	[C]	1,04E+12	1,04E+12	2,32E+10	1,16E+09	1,83E+08
[oswindows] oswindows200server	[A.8] Malware diffusion	[I]	9,70E+11	9,70E+11	1,05E+10	3,58E+07	1,33E+08
[ossolaris] solaris	[A.8] Malware diffusion	[A]	9,70E+11	9,70E+11	1,05E+10	3,58E+07	1,33E+08
[serverprot] questwinerserver	[A.8] Malware diffusion	[I]	9,70E+11	9,70E+11	1,05E+10	3,57E+07	1,48E+08
[appsfinancialwindowspc] logisticsexternalpatients	[A.8] Malware diffusion	[A]	9,70E+11	9,70E+11	1,05E+10	3,58E+07	1,33E+08
[serverpatients] compaqproliantml370	[A.13] Repudiation (denial of actions)	[I]	9,48E+11	9,48E+11	1,20E+10	4,10E+07	3,21E+08
[ossolaris] solaris	[A.22] Software manipulation	[A]	6,06E+11	6,06E+11	7,80E+09	3,14E+07	3,16E+08
[ospcwindows] ospcwindows	[A.22] Software manipulation	[A]	6,06E+11	6,06E+11	7,80E+09	3,14E+07	3,16E+08
[appsfinancialwindowspc] logisticsexternalpatients	[A.22] Software manipulation	[A]	6,06E+11	6,06E+11	5,76E+09	2,46E+07	1,77E+08
[appsfinancialwindowspc] logisticsexternalpatients	[E.18] Destruction of information	[A]	5,77E+11	5,77E+11	5,49E+09	2,34E+07	1,69E+08
[ossolaris] solaris	[E.18] Destruction of information	[A]	5,77E+11	5,77E+11	7,43E+09	3,00E+07	3,02E+08

[ospcwindows] ospcwindows	[E.18] Destruction of information	[A]	5,77E+11	5,77E+11	7,43E+09	3,00E+07	3,02E+08
[secretary] secretary	[A.11] Unauthorised access	[C]	5,21E+11	5,21E+11	5,98E+09	2,04E+07	1,00E+08
[offices] workingroomisthodosias	[A.11] Unauthorised access	[C]	5,21E+11	5,21E+11	5,98E+09	2,04E+07	1,00E+08
[serverblood] compaqproliantml370g3	[A.24] Denial of service	[A]	5,21E+11	5,21E+11	6,45E+09	2,20E+07	2,30E+08
[serverprot] questwinerserver	[A.24] Denial of service	[A]	5,21E+11	5,21E+11	6,08E+09	2,08E+07	1,99E+08
[hospitaldepartments] hospitaldepartments	[A.11] Unauthorised access	[C]	5,21E+11	5,21E+11	5,98E+09	2,04E+07	1,00E+08
[dc] datacenterpliroforikhsorganwsis	[A.11] Unauthorised access	[C]	5,21E+11	5,21E+11	5,98E+09	2,04E+07	1,00E+08
[datalabpatients] datapatients	[A.5.3] By outsiders	[V]	5,00E+11	5,00E+11	4,82E+09	1,71E+07	1,08E+08
[datalabpatients] datapatients	[A.5.1] By insiders	[V]	5,00E+11	5,00E+11	4,82E+09	1,71E+07	1,08E+08
[dataemployees] dataemployees	[A.5.1] By insiders	[A]	5,00E+11	5,00E+11	4,82E+09	1,70E+07	1,05E+08
[financial] finlogisticssubcontractor	[A.5.1] By insiders	[I]	5,00E+11	5,00E+11	4,82E+09	1,70E+07	1,05E+08
[datalabpatients] datapatients	[A.5.3] By outsiders	[I]	5,00E+11	5,00E+11	4,82E+09	1,71E+07	1,08E+08
[datalabpatients] datapatients	[A.5.1] By insiders	[I]	5,00E+11	5,00E+11	4,82E+09	1,71E+07	1,08E+08
[ospcwindows] ospcwindows	[A.18] Destruction of information	[A]	4,85E+11	4,85E+11	6,24E+09	2,51E+07	2,53E+08
[COM.LAN] Local Area Network	[A.18] Destruction of information	[A]	4,85E+11	4,85E+11	6,70E+09	5,40E+07	1,99E+08
[appsfinancialwindowspc] logisticsexternalpatients	[A.18] Destruction of information	[A]	4,85E+11	4,85E+11	4,65E+09	1,96E+07	1,42E+08
[oswindows] oswindows200server	[A.5] Masquerading of identity	[I]	4,85E+11	4,85E+11	1,08E+10	5,38E+08	8,52E+07
[ossolaris] solaris	[A.18] Destruction of information	[A]	4,85E+11	4,85E+11	6,24E+09	2,51E+07	2,53E+08
[oswindows] oswindows200server	[A.15] Deliberate alteration of information	[I]	4,85E+11	4,85E+11	5,93E+09	2,45E+07	2,52E+08
[serverprot] questwinerserver	[A.5] Masquerading of identity	[I]	4,85E+11	4,85E+11	1,08E+10	5,38E+08	8,52E+07
[serverprot] questwinerserver	[A.15] Deliberate alteration of information	[I]	4,85E+11	4,85E+11	6,32E+09	2,54E+07	1,92E+08
[secretary] secretary	[A.11] Unauthorised access	[I]	4,85E+11	4,85E+11	5,56E+09	1,90E+07	9,38E+07
[COM.LAN] Local Area Network	[A.24] Denial of service	[I]	2,61E+11	2,61E+11	4,18E+09	1,38E+07	1,13E+08
[appdpsn] appdpsnsolarisml370	[A.6] Abuse of access privileges	[V]	2,61E+11	2,61E+11	2,01E+09	9,37E+06	4,83E+07
[COM.LAN] Local Area Network	[A.24] Denial of service	[C]	2,61E+11	2,61E+11	4,18E+09	1,38E+07	1,13E+08
[appdpsn] appdpsnsolarisml370	[A.6] Abuse of access privileges	[I]	2,61E+11	2,61E+11	2,60E+09	2,45E+07	5,72E+07
[COM.LAN] Local Area Network	[A.24] Denial of service	[V]	2,61E+11	2,61E+11	4,18E+09	1,38E+07	1,13E+08
[ossolaris] solaris	[A.22] Software manipulation	[C]	2,61E+11	2,61E+11	3,19E+09	1,32E+07	1,32E+08
[ospcwindows] ospcwindows	[A.22] Software manipulation	[C]	2,61E+11	2,61E+11	3,19E+09	1,32E+07	1,32E+08
[appsfinancialwindowspc] logisticsexternalpatients	[A.22] Software manipulation	[I]	2,61E+11	2,61E+11	2,33E+09	1,03E+07	7,01E+07
[ossolaris] solaris	[A.22] Software manipulation	[I]	2,61E+11	2,61E+11	3,19E+09	1,32E+07	1,35E+08
[oswindows] oswindows200server	[A.22] Software manipulation	[C]	2,61E+11	2,61E+11	3,19E+09	1,32E+07	1,32E+08
[appsfinancialwindowspc] logisticsexternalpatients	[A.22] Software manipulation	[C]	2,61E+11	2,61E+11	2,33E+09	1,03E+07	6,78E+07
[serverprot] questwinerserver	[A.22] Software	[C]	2,61E+11	2,61E+11	3,55E+09	2,08E+07	1,00E+08

	manipulation						
[ossw] os	[A.22] Software manipulation	[C]	2,61E+11	2,61E+11	3,15E+09	1,31E+07	1,30E+08
[ospcwindows] ospcwindows	[A.22] Software manipulation	[I]	2,61E+11	2,61E+11	3,19E+09	1,32E+07	1,35E+08
[serverpatients] compaqproliantml370	[E.1] User errors	[I]	2,48E+11	2,48E+11	3,66E+09	2,73E+07	9,16E+07
[serverpatients] compaqproliantml370	[E.1] User errors	[C]	2,48E+11	2,48E+11	3,55E+09	2,55E+07	8,19E+07
[S_blooddata] s_blooddata	[E.1] User errors	[A]	2,15E+11	2,15E+11	1,80E+09	7,95E+06	4,97E+07
[datapdpsn] datadpsn	[E.1] User errors	[V]	2,15E+11	2,15E+11	1,52E+09	7,69E+06	4,80E+07
[S_blooddata] s_blooddata	[E.1] User errors	[C]	2,15E+11	2,15E+11	2,02E+09	1,31E+07	4,30E+07
[aimodosia] workingroomaimodosia	[A.27] Enemy over-run	[C]	2,15E+11	2,15E+11	2,73E+09	9,29E+06	9,35E+07
[serverpatients] compaqproliantml370	[E.2] System / Security administrator errors	[A]	2,10E+11	2,10E+11	2,67E+09	1,08E+07	7,81E+07
[ossolaris] solaris	[E.2] System / Security administrator errors	[A]	2,10E+11	2,10E+11	2,70E+09	1,09E+07	1,10E+08
[ospcwindows] ospcwindows	[E.2] System / Security administrator errors	[A]	2,10E+11	2,10E+11	2,70E+09	1,09E+07	1,10E+08
[oswindows] oswindows200server	[E.2] System / Security administrator errors	[I]	2,10E+11	2,10E+11	2,57E+09	1,06E+07	1,10E+08
[serverprot] questwinerserver	[E.2] System / Security administrator errors	[I]	2,10E+11	2,10E+11	2,74E+09	1,10E+07	8,38E+07
[appsfinancialwindowspc] logisticsexternalpatients	[E.2] System / Security administrator errors	[A]	2,10E+11	2,10E+11	2,00E+09	8,51E+06	6,16E+07
[COM.LAN] Local Area Network	[E.2] System / Security administrator errors	[A]	2,10E+11	2,10E+11	2,90E+09	2,34E+07	8,65E+07
[oswindows] oswindows200server	[E.20] Software vulnerabilities	[I]	2,10E+11	2,10E+11	3,50E+09	1,15E+07	1,19E+08
[serverprot] questwinerserver	[A.8] Malware diffusion	[A]	2,09E+11	2,09E+11	2,25E+09	7,67E+06	3,18E+07
[oswindows] oswindows200server	[A.8] Malware diffusion	[A]	2,09E+11	2,09E+11	2,25E+09	7,69E+06	2,85E+07
[appsfinancialwindowspc] logisticsexternalpatients	[A.8] Malware diffusion	[C]	2,09E+11	2,09E+11	2,25E+09	7,69E+06	2,85E+07
[ossw] os	[A.8] Malware diffusion	[C]	2,09E+11	2,09E+11	2,25E+09	7,69E+06	2,85E+07
[appsfinancialwindowspc] logisticsexternalpatients	[A.8] Malware diffusion	[I]	2,09E+11	2,09E+11	2,25E+09	7,69E+06	2,85E+07
[ossolaris] solaris	[A.8] Malware diffusion	[I]	2,09E+11	2,09E+11	2,25E+09	7,69E+06	2,85E+07
[serverprot] questwinerserver	[A.8] Malware diffusion	[C]	2,09E+11	2,09E+11	2,25E+09	7,67E+06	3,29E+07
[ossw] os	[A.8] Malware diffusion	[A]	2,09E+11	2,09E+11	2,25E+09	7,69E+06	2,85E+07
[ossolaris] solaris	[A.8] Malware diffusion	[C]	2,09E+11	2,09E+11	2,25E+09	7,69E+06	2,85E+07
[oswindows] oswindows200server	[A.8] Malware diffusion	[C]	2,09E+11	2,09E+11	2,25E+09	7,69E+06	2,85E+07
[appdpsn] appdpsnsolarisml370	[A.5] Masquerading of identity	[V]	2,09E+11	2,09E+11	2,01E+09	7,13E+06	4,50E+07
[appdpsn] appdpsnsolarisml370	[A.5] Masquerading of identity	[I]	2,09E+11	2,09E+11	4,18E+09	1,70E+08	3,73E+07
[serverpatients] compaqproliantml370	[A.5] Masquerading of identity	[I]	2,09E+11	2,09E+11	3,48E+09	8,57E+07	4,16E+07
[aimodosia] workingroomaimodosia	[A.11] Unauthorised access	[I]	1,53E+11	1,53E+11	1,75E+09	5,98E+06	2,97E+07

[offices] workingroomisthodosias	[A.7] Misuse	[C]	1,30E+11	1,30E+11	1,06E+09	4,87E+06	3,43E+07
[serverblood] compaqproliantml370g3	[A.6] Abuse of access privileges	[C]	1,30E+11	1,30E+11	1,71E+09	1,53E+07	5,06E+07
[serverprot] questwinerserver	[A.22] Software manipulation	[A]	1,30E+11	1,30E+11	1,75E+09	6,92E+06	5,47E+07
[COM.LAN] Local Area Network	[A.6] Abuse of access privileges	[C]	1,30E+11	1,30E+11	1,83E+09	1,21E+07	5,22E+07
[oswindows] oswindows200server	[A.22] Software manipulation	[A]	1,30E+11	1,30E+11	1,68E+09	6,76E+06	6,87E+07
[serverpatients] compaqproliantml370	[A.6] Abuse of access privileges	[C]	1,30E+11	1,30E+11	1,94E+09	1,50E+07	4,38E+07
[serverprot] questwinerserver	[A.6] Abuse of access privileges	[C]	1,30E+11	1,30E+11	1,88E+09	1,23E+07	5,74E+07
[hospitaldepartments] hospitaldepartments	[A.7] Misuse	[C]	1,30E+11	1,30E+11	1,06E+09	4,87E+06	3,43E+07
[ossw] os	[A.22] Software manipulation	[A]	1,30E+11	1,30E+11	1,67E+09	6,74E+06	6,76E+07
[oswindows] oswindows200server	[E.18] Destruction of information	[A]	1,24E+11	1,24E+11	1,60E+09	6,44E+06	6,57E+07
[ossw] os	[E.18] Destruction of information	[A]	1,24E+11	1,24E+11	1,59E+09	6,42E+06	6,47E+07
[appdpsn] appdpsnsolarisml370	[A.6] Abuse of access privileges	[A]	1,21E+11	1,21E+11	1,02E+09	4,49E+06	2,91E+07
[offices] workingroomisthodosias	[A.7] Misuse	[A]	1,21E+11	1,21E+11	1,08E+09	4,69E+06	3,55E+07
[oswindows] oswindows200server	[A.6] Abuse of access privileges	[I]	1,21E+11	1,21E+11	1,53E+09	6,33E+06	7,16E+07
[serverprot] questwinerserver	[A.6] Abuse of access privileges	[I]	1,21E+11	1,21E+11	1,63E+09	6,56E+06	5,44E+07
[hospitaldepartments] hospitaldepartments	[A.7] Misuse	[A]	1,21E+11	1,21E+11	1,08E+09	4,69E+06	3,55E+07
[ossw] os	[A.22] Software manipulation	[I]	1,21E+11	1,21E+11	1,48E+09	6,12E+06	6,23E+07
[oswindows] oswindows200server	[A.7] Misuse	[I]	1,21E+11	1,21E+11	1,48E+09	6,14E+06	6,34E+07
[COM.LAN] Local Area Network	[A.7] Misuse	[A]	1,21E+11	1,21E+11	1,61E+09	1,02E+07	4,99E+07
[serverpatients] compaqproliantml370	[A.6] Abuse of access privileges	[A]	1,21E+11	1,21E+11	1,56E+09	6,26E+06	4,72E+07
[COM.LAN] Local Area Network	[A.6] Abuse of access privileges	[A]	1,21E+11	1,21E+11	1,68E+09	1,20E+07	5,30E+07
[oswindows] oswindows200server	[E.8] Malware diffusion	[I]	1,15E+11	1,15E+11	1,40E+09	5,79E+06	5,69E+07
[ospcwindows] ospcwindows	[E.8] Malware diffusion	[A]	1,15E+11	1,15E+11	1,44E+09	5,83E+06	5,47E+07
[serverprot] questwinerserver	[E.8] Malware diffusion	[I]	1,15E+11	1,15E+11	1,49E+09	6,01E+06	4,30E+07
[appsfinancialwindowspc] logisticsexternalpatients	[E.8] Malware diffusion	[A]	1,15E+11	1,15E+11	1,06E+09	4,45E+06	2,96E+07
[serverprot] questwinerserver	[E.1] User errors	[I]	1,15E+11	1,15E+11	1,51E+09	6,07E+06	4,63E+07
[ossolaris] solaris	[E.8] Malware diffusion	[A]	1,15E+11	1,15E+11	1,44E+09	5,83E+06	5,47E+07
[oswindows] oswindows200server	[E.1] User errors	[I]	1,15E+11	1,15E+11	1,41E+09	5,86E+06	6,10E+07
[serverpatients] compaqproliantml370	[E.25] Equipment loss	[A]	1,15E+11	1,15E+11	1,48E+09	5,96E+06	4,47E+07
[ossolaris] solaris	[E.21] Defects in software maintenance / updating	[A]	1,15E+11	1,15E+11	1,78E+09	5,95E+06	7,09E+07
[ospcwindows] ospcwindows	[E.21] Defects in software maintenance / updating	[A]	1,15E+11	1,15E+11	1,78E+09	5,95E+06	7,09E+07
[ossw] os	[E.21] Defects in software maintenance /	[V]	1,15E+11	1,15E+11	1,78E+09	5,95E+06	7,88E+07

	updating						
[appsfinancialwindowspc] logisticsexternalpatients	[E.21] Defects in software maintenance / updating	[A]	1,15E+11	1,15E+11	1,37E+09	4,69E+06	4,30E+07
[oswindows] oswindows200server	[E.21] Defects in software maintenance / updating	[I]	1,15E+11	1,15E+11	1,78E+09	5,95E+06	7,38E+07
[dataemployees] dataemployees	[A.5.1] By insiders	[C]	1,08E+11	1,08E+11	1,04E+09	3,67E+06	2,32E+07
[dataemployees] dataemployees	[A.5.1] By insiders	[I]	1,08E+11	1,08E+11	1,04E+09	3,67E+06	2,32E+07
[dataemployees] dataemployees	[A.5.1] By insiders	[V]	1,08E+11	1,08E+11	1,04E+09	3,67E+06	2,32E+07
[ossw] os	[A.11] Unauthorised access	[C]	1,04E+11	1,04E+11	1,20E+09	4,11E+06	2,34E+07
[ossolaris] solaris	[A.19] Disclosure of information	[C]	1,04E+11	1,04E+11	1,28E+09	5,28E+06	5,30E+07
[serverpatients] compaqproliantml370	[A.11] Unauthorised access	[C]	1,04E+11	1,04E+11	1,67E+09	5,52E+06	3,10E+07
[oswindows] oswindows200server	[A.5] Masquerading of identity	[C]	1,04E+11	1,04E+11	2,09E+09	8,48E+07	1,86E+07
[appsfinancialwindowspc] logisticsexternalpatients	[A.11] Unauthorised access	[C]	1,04E+11	1,04E+11	1,20E+09	4,11E+06	2,34E+07
[ospcwindows] ospcwindows	[A.11] Unauthorised access	[C]	1,04E+11	1,04E+11	1,20E+09	4,11E+06	2,34E+07
[ospcwindows] ospcwindows	[A.15] Deliberate alteration of information	[I]	1,04E+11	1,04E+11	1,28E+09	5,28E+06	5,43E+07
[ospcwindows] ospcwindows	[A.19] Disclosure of information	[C]	1,04E+11	1,04E+11	1,28E+09	5,28E+06	5,30E+07
[appsfinancialwindowspc] logisticsexternalpatients	[A.5] Masquerading of identity	[C]	1,04E+11	1,04E+11	2,09E+09	8,48E+07	1,86E+07
[COM.LAN] Local Area Network	[A.19] Disclosure of information	[C]	1,04E+11	1,04E+11	1,40E+09	8,30E+06	3,91E+07
[serverprot] questwinerserver	[A.5] Masquerading of identity	[C]	1,04E+11	1,04E+11	2,09E+09	8,48E+07	1,86E+07
[ospcwindows] ospcwindows	[A.5] Masquerading of identity	[I]	1,04E+11	1,04E+11	2,09E+09	8,48E+07	1,86E+07
[serverblood] compaqproliantml370g3	[A.11] Unauthorised access	[C]	1,04E+11	1,04E+11	1,56E+09	5,26E+06	3,24E+07
[ossw] os	[A.18] Destruction of information	[A]	1,04E+11	1,04E+11	1,34E+09	5,39E+06	5,41E+07
[COM.LAN] Local Area Network	[A.11] Unauthorised access	[C]	1,04E+11	1,04E+11	1,18E+09	4,03E+06	1,60E+07
[serverprot] questwinerserver	[A.19] Disclosure of information	[C]	1,04E+11	1,04E+11	1,42E+09	8,18E+06	4,03E+07
[oswindows] oswindows200server	[A.19] Disclosure of information	[C]	1,04E+11	1,04E+11	1,27E+09	5,28E+06	5,32E+07
[ossolaris] solaris	[A.5] Masquerading of identity	[C]	1,04E+11	1,04E+11	2,09E+09	8,48E+07	1,86E+07
[ossw] os	[A.5] Masquerading of identity	[C]	1,04E+11	1,04E+11	2,09E+09	8,48E+07	1,86E+07
[appsfinancialwindowspc] logisticsexternalpatients	[A.19] Disclosure of information	[C]	1,04E+11	1,04E+11	9,32E+08	4,04E+06	2,73E+07
[ossolaris] solaris	[A.11] Unauthorised access	[C]	1,04E+11	1,04E+11	1,20E+09	4,11E+06	2,34E+07
[serverprot] questwinerserver	[A.11] Unauthorised access	[C]	1,04E+11	1,04E+11	1,62E+09	5,40E+06	3,24E+07
[ossolaris] solaris	[A.15] Deliberate alteration of information	[I]	1,04E+11	1,04E+11	1,28E+09	5,28E+06	5,43E+07
[appsfinancialwindowspc] logisticsexternalpatients	[A.5] Masquerading of identity	[I]	1,04E+11	1,04E+11	2,09E+09	8,48E+07	1,86E+07
[appsfinancialwindowspc] logisticsexternalpatients	[A.15] Deliberate alteration of information	[I]	1,04E+11	1,04E+11	9,32E+08	4,04E+06	2,82E+07
[ossw] os	[A.19] Disclosure of information	[C]	1,04E+11	1,04E+11	1,27E+09	5,26E+06	5,22E+07

[ospcwindows] ospcwindows	[A.5] Masquerading of identity	[C]	1,04E+11	1,04E+11	2,09E+09	8,48E+07	1,86E+07
[serverprot] questwinerserver	[A.18] Destruction of information	[A]	1,04E+11	1,04E+11	1,40E+09	5,54E+06	4,37E+07
[ossolaris] solaris	[A.5] Masquerading of identity	[I]	1,04E+11	1,04E+11	2,09E+09	8,48E+07	1,86E+07
[oswindows] oswindows200server	[A.18] Destruction of information	[A]	1,04E+11	1,04E+11	1,34E+09	5,41E+06	5,50E+07
[oswindows] oswindows200server	[A.11] Unauthorised access	[C]	1,04E+11	1,04E+11	1,20E+09	4,11E+06	2,34E+07
[hospitaldepartments] hospitaldepartments	[A.11] Unauthorised access	[I]	1,04E+11	1,04E+11	1,20E+09	4,08E+06	2,09E+07
[offices] workingroomisthodosias	[A.11] Unauthorised access	[I]	1,04E+11	1,04E+11	1,20E+09	4,08E+06	2,09E+07
[dc] datacenterpliroforikhsorganwsis	[A.11] Unauthorised access	[I]	1,04E+11	1,04E+11	1,20E+09	4,08E+06	2,09E+07
[S_blooddata] s_blooddata	[E.1] User errors	[I]	1,00E+11	1,00E+11	9,54E+08	7,35E+06	2,18E+07
[dc] datacenterpliroforikhsorganwsis	[A.27] Enemy over-run	[A]	1,00E+11	1,00E+11	1,30E+09	4,44E+06	5,63E+07
[datapdpsn] datadpsn	[E.14] Information leaks (> E.19)	[A]	1,00E+11	1,00E+11	7,88E+08	3,70E+06	2,80E+07
[offices] workingroomisthodosias	[A.27] Enemy over-run	[A]	1,00E+11	1,00E+11	1,30E+09	4,44E+06	5,63E+07
[personalcomputer] pcwindows	[A.23] Hardware manipulation	[A]	1,00E+11	1,00E+11	7,88E+08	3,70E+06	2,80E+07
[ospcwindows] ospcwindows	[A.8] Malware diffusion	[A]	1,00E+11	1,00E+11	1,08E+09	3,69E+06	1,37E+07
[s_eprotocol] s_eprotocol	[E.2] System / Security administrator errors	[V]	1,00E+11	1,00E+11	7,70E+08	3,57E+06	1,95E+07
[datapdpsn] datadpsn	[E.18] Destruction of information	[A]	1,00E+11	1,00E+11	7,88E+08	3,70E+06	2,80E+07
[personalcomputer] pcwindows	[E.24] System failure due to exhaustion of resources	[A]	1,00E+11	1,00E+11	1,27E+09	4,32E+06	3,26E+07
[serverprot] questwinerserver	[A.25] Theft	[I]	1,00E+11	1,00E+11	1,74E+09	5,64E+06	5,37E+07
[datapdpsn] datadpsn	[A.6] Abuse of access privileges	[A]	1,00E+11	1,00E+11	7,87E+08	3,68E+06	2,84E+07
[S_blooddata] s_blooddata	[E.1] User errors	[V]	1,00E+11	1,00E+11	7,65E+08	3,56E+06	1,83E+07
[serverpatients] compaqproliantml370	[A.25] Theft	[A]	1,00E+11	1,00E+11	1,74E+09	5,64E+06	5,37E+07
[COM.LAN] Local Area Network	[A.11] Unauthorised access	[A]	9,70E+10	9,70E+10	1,04E+09	3,57E+06	1,25E+07
[COM.LAN] Local Area Network	[A.19] Disclosure of information	[A]	9,70E+10	9,70E+10	1,29E+09	8,17E+06	3,99E+07
[oswindows] oswindows200server	[A.11] Unauthorised access	[I]	9,70E+10	9,70E+10	1,12E+09	3,82E+06	2,17E+07
[serverpatients] compaqproliantml370	[A.11] Unauthorised access	[A]	9,70E+10	9,70E+10	1,45E+09	4,89E+06	2,91E+07
[ossw] os	[A.8] Malware diffusion	[I]	9,70E+10	9,70E+10	1,05E+09	3,58E+06	1,33E+07
[serverprot] questwinerserver	[A.11] Unauthorised access	[I]	9,70E+10	9,70E+10	1,50E+09	5,02E+06	2,98E+07
[COM.LAN] Local Area Network	[A.14] Eavesdropping	[A]	9,70E+10	9,70E+10	2,03E+09	3,18E+07	2,19E+07
[COM.LAN] Local Area Network	[A.15] Deliberate alteration of information	[A]	9,70E+10	9,70E+10	1,29E+09	8,17E+06	3,99E+07
[COM.LAN] Local Area Network	[A.9] [Re-]routing of messages	[A]	8,82E+10	8,82E+10	1,17E+09	7,43E+06	3,63E+07
[COM.LAN] Local Area Network	[A.10] Sequence alteration	[A]	8,82E+10	8,82E+10	1,17E+09	7,43E+06	3,63E+07
[COM.LAN] Local Area Network	[A.12] Traffic analysis	[A]	8,82E+10	8,82E+10	1,15E+09	3,91E+06	2,62E+07
[dataemployees] dataemployees	[A.5.3] By outsiders	[A]	5,00E+10	5,00E+10	4,82E+08	1,71E+06	1,08E+07
[ossw] os	[A.5] Masquerading of identity	[I]	4,85E+10	4,85E+10	8,04E+08	2,12E+07	9,09E+06
[ossw] os	[A.15] Deliberate	[I]	4,85E+10	4,85E+10	5,91E+08	2,44E+06	2,51E+07

	alteration of information						
[serverprot] questwinerserver	[A.23] Hardware manipulation	[C]	4,74E+10	4,74E+10	6,83E+08	4,47E+06	2,09E+07
[serverprot] questwinerserver	[A.23] Hardware manipulation	[A]	4,74E+10	4,74E+10	6,52E+08	2,57E+06	2,22E+07
[serverpatients] compaqproliantml370	[E.2] System / Security administrator errors	[I]	4,51E+10	4,51E+10	6,41E+08	4,04E+06	1,68E+07
[ospcwindows] ospcwindows	[E.2] System / Security administrator errors	[I]	4,51E+10	4,51E+10	5,53E+08	2,29E+06	2,39E+07
[serverprot] questwinerserver	[E.2] System / Security administrator errors	[C]	4,51E+10	4,51E+10	6,10E+08	3,27E+06	1,77E+07
[ossw] os	[E.2] System / Security administrator errors	[C]	4,51E+10	4,51E+10	5,51E+08	2,28E+06	2,30E+07
[oswindows] oswindows200server	[E.20] Software vulnerabilities	[C]	4,51E+10	4,51E+10	7,53E+08	2,46E+06	2,61E+07
[ossolaris] solaris	[E.2] System / Security administrator errors	[C]	4,51E+10	4,51E+10	5,53E+08	2,29E+06	2,33E+07
[COM.LAN] Local Area Network	[E.2] System / Security administrator errors	[I]	4,51E+10	4,51E+10	5,95E+08	3,09E+06	1,74E+07
[ossolaris] solaris	[E.20] Software vulnerabilities	[C]	4,51E+10	4,51E+10	7,53E+08	2,46E+06	2,61E+07
[ospcwindows] ospcwindows	[E.20] Software vulnerabilities	[I]	4,51E+10	4,51E+10	7,53E+08	2,46E+06	2,59E+07
[appsfinancialwindowspc] logisticsexternalpatients	[E.2] System / Security administrator errors	[I]	4,51E+10	4,51E+10	4,08E+08	1,75E+06	1,25E+07
[serverblood] compaqproliantml370g3	[E.2] System / Security administrator errors	[C]	4,51E+10	4,51E+10	5,62E+08	3,84E+06	1,72E+07
[ossw] os	[E.20] Software vulnerabilities	[C]	4,51E+10	4,51E+10	7,53E+08	2,46E+06	2,61E+07
[ospcwindows] ospcwindows	[E.2] System / Security administrator errors	[C]	4,51E+10	4,51E+10	5,53E+08	2,29E+06	2,33E+07
[appsfinancialwindowspc] logisticsexternalpatients	[E.20] Software vulnerabilities	[C]	4,51E+10	4,51E+10	5,67E+08	1,93E+06	1,44E+07
[serverpatients] compaqproliantml370	[E.2] System / Security administrator errors	[C]	4,51E+10	4,51E+10	6,32E+08	4,13E+06	1,50E+07
[ospcwindows] ospcwindows	[E.20] Software vulnerabilities	[C]	4,51E+10	4,51E+10	7,53E+08	2,46E+06	2,61E+07
[ossolaris] solaris	[E.20] Software vulnerabilities	[I]	4,51E+10	4,51E+10	7,53E+08	2,46E+06	2,59E+07
[ossw] os	[E.2] System / Security administrator errors	[A]	4,51E+10	4,51E+10	5,79E+08	2,33E+06	2,46E+07
[ossolaris] solaris	[E.2] System / Security administrator errors	[I]	4,51E+10	4,51E+10	5,53E+08	2,29E+06	2,39E+07
[COM.LAN] Local Area Network	[E.2] System / Security administrator errors	[C]	4,51E+10	4,51E+10	5,95E+08	3,09E+06	1,72E+07
[oswindows] oswindows200server	[E.2] System / Security administrator errors	[C]	4,51E+10	4,51E+10	5,53E+08	2,28E+06	2,34E+07
[appsfinancialwindowspc] logisticsexternalpatients	[E.20] Software vulnerabilities	[I]	4,51E+10	4,51E+10	5,67E+08	1,93E+06	1,43E+07
[serverblood] compaqproliantml370g3	[E.2] System / Security administrator errors	[A]	4,51E+10	4,51E+10	5,57E+08	2,30E+06	1,93E+07
[serverprot] questwinerserver	[E.2] System / Security administrator errors	[A]	4,51E+10	4,51E+10	6,08E+08	2,39E+06	1,92E+07

[oswindows] oswindows200server	[E.2] System / Security administrator errors	[A]	4,51E+10	4,51E+10	5,81E+08	2,34E+06	2,50E+07
[appsfinancialwindowspc] logisticsexternalpatients	[E.2] System / Security administrator errors	[C]	4,51E+10	4,51E+10	4,08E+08	1,75E+06	1,21E+07
[S_blooddata] s_blooddata	[E.2] System / Security administrator errors	[A]	4,30E+10	4,30E+10	3,60E+08	1,58E+06	1,01E+07
[S_blooddata] s_blooddata	[E.2] System / Security administrator errors	[C]	4,30E+10	4,30E+10	3,98E+08	2,42E+06	8,69E+06
[appsfinancialwindowspc] logisticsexternalpatients	[A.7] Misuse	[C]	2,61E+10	2,61E+10	2,33E+08	1,01E+06	6,90E+06
[ospcwindows] ospcwindows	[A.7] Misuse	[I]	2,61E+10	2,61E+10	3,19E+08	1,32E+06	1,37E+07
[hospitaldepartments] hospitaldepartments	[A.7] Misuse	[I]	2,61E+10	2,61E+10	2,12E+08	0.968733	6,97E+06
[serverblood] compaqproliantml370g3	[A.7] Misuse	[C]	2,61E+10	2,61E+10	3,24E+08	2,21E+06	9,81E+06
[ossolaris] solaris	[A.7] Misuse	[I]	2,61E+10	2,61E+10	3,19E+08	1,32E+06	1,37E+07
[COM.LAN] Local Area Network	[A.7] Misuse	[C]	2,61E+10	2,61E+10	3,43E+08	1,77E+06	9,84E+06
[serverpatients] compaqproliantml370	[A.7] Misuse	[C]	2,61E+10	2,61E+10	3,64E+08	2,38E+06	8,59E+06
[ospcwindows] ospcwindows	[A.6] Abuse of access privileges	[C]	2,61E+10	2,61E+10	3,29E+08	1,36E+06	1,51E+07
[ossolaris] solaris	[A.6] Abuse of access privileges	[I]	2,61E+10	2,61E+10	3,29E+08	1,36E+06	1,54E+07
[oswindows] oswindows200server	[A.6] Abuse of access privileges	[C]	2,61E+10	2,61E+10	3,28E+08	1,36E+06	1,52E+07
[COM.LAN] Local Area Network	[A.7] Misuse	[V]	2,61E+10	2,61E+10	3,26E+08	1,94E+06	9,42E+06
[appsfinancialwindowspc] logisticsexternalpatients	[A.7] Misuse	[I]	2,61E+10	2,61E+10	2,33E+08	1,01E+06	7,12E+06
[serverblood] compaqproliantml370g3	[A.6] Abuse of access privileges	[A]	2,61E+10	2,61E+10	3,25E+08	1,34E+06	1,17E+07
[ospcwindows] ospcwindows	[A.7] Misuse	[C]	2,61E+10	2,61E+10	3,19E+08	1,32E+06	1,34E+07
[oswindows] oswindows200server	[A.7] Misuse	[C]	2,61E+10	2,61E+10	3,19E+08	1,32E+06	1,34E+07
[COM.LAN] Local Area Network	[A.6] Abuse of access privileges	[V]	2,61E+10	2,61E+10	3,41E+08	2,27E+06	1,02E+07
[appsfinancialwindowspc] logisticsexternalpatients	[A.6] Abuse of access privileges	[I]	2,61E+10	2,61E+10	2,42E+08	1,04E+06	8,20E+06
[ossolaris] solaris	[A.6] Abuse of access privileges	[C]	2,61E+10	2,61E+10	3,29E+08	1,36E+06	1,51E+07
[ospcwindows] ospcwindows	[A.6] Abuse of access privileges	[I]	2,61E+10	2,61E+10	3,29E+08	1,36E+06	1,54E+07
[COM.LAN] Local Area Network	[A.7] Misuse	[I]	2,61E+10	2,61E+10	3,43E+08	1,77E+06	1,00E+07
[ossw] os	[A.6] Abuse of access privileges	[C]	2,61E+10	2,61E+10	3,27E+08	1,35E+06	1,49E+07
[ossolaris] solaris	[A.7] Misuse	[C]	2,61E+10	2,61E+10	3,19E+08	1,32E+06	1,34E+07
[serverprot] questwinerserver	[A.7] Misuse	[C]	2,61E+10	2,61E+10	3,52E+08	1,88E+06	1,02E+07
[serverpatients] compaqproliantml370	[A.6] Abuse of access privileges	[I]	2,61E+10	2,61E+10	3,73E+08	2,34E+06	9,85E+06
[serverprot] questwinerserver	[A.6] Abuse of access privileges	[A]	2,61E+10	2,61E+10	3,59E+08	1,41E+06	1,23E+07
[appsfinancialwindowspc] logisticsexternalpatients	[A.6] Abuse of access privileges	[C]	2,61E+10	2,61E+10	2,42E+08	1,04E+06	8,02E+06
[COM.LAN] Local Area Network	[A.6] Abuse of access privileges	[I]	2,61E+10	2,61E+10	3,55E+08	1,98E+06	1,06E+07
[ossw] os	[A.7] Misuse	[C]	2,61E+10	2,61E+10	3,17E+08	1,31E+06	1,32E+07
[offices] workingroomisthodosias	[A.7] Misuse	[I]	2,61E+10	2,61E+10	2,12E+08	0.968733	6,97E+06
[hospitaldepartments] hospitaldepartments	[A.7] Misuse	[V]	2,61E+10	2,61E+10	2,12E+08	0.968733	6,98E+06
[ospcwindows] ospcwindows	[E.18] Destruction of information	[V]	2,48E+10	2,48E+10	3,06E+08	1,26E+06	1,35E+07
[appdpsn] appdpsnsolarisml370	[E.19] Information leaks	[C]	2,48E+10	2,48E+10	2,31E+08	1,40E+06	5,12E+06

[ospcwindows] ospcwindows	[E.15] Accidental alteration of the information	[V]	2,48E+10	2,48E+10	3,06E+08	1,26E+06	1,35E+07
[ospcwindows] ospcwindows	[E.19] Information leaks	[C]	2,48E+10	2,48E+10	3,04E+08	1,26E+06	1,28E+07
[ospcwindows] ospcwindows	[E.1] User errors	[I]	2,48E+10	2,48E+10	3,04E+08	1,26E+06	1,32E+07
[appsfinancialwindowspc] logisticsexternalpatients	[E.1] User errors	[C]	2,48E+10	2,48E+10	2,22E+08	0.961740	6,65E+06
[appsfinancialwindowspc] logisticsexternalpatients	[E.8] Malware diffusion	[I]	2,48E+10	2,48E+10	2,19E+08	0.949768	6,22E+06
[appdpsn] appdpsnsolarisml370	[E.18] Destruction of information	[V]	2,48E+10	2,48E+10	1,91E+08	0.888843	4,69E+06
[ossolaris] solaris	[E.8] Malware diffusion	[I]	2,48E+10	2,48E+10	3,01E+08	1,24E+06	1,23E+07
[serverprot] questwinerserver	[E.1] User errors	[C]	2,48E+10	2,48E+10	3,36E+08	1,80E+06	9,75E+06
[oswindows] oswindows200server	[E.1] User errors	[C]	2,48E+10	2,48E+10	3,04E+08	1,26E+06	1,29E+07
[ospcwindows] ospcwindows	[E.8] Malware diffusion	[C]	2,48E+10	2,48E+10	3,01E+08	1,24E+06	1,20E+07
[oswindows] oswindows200server	[E.8] Malware diffusion	[C]	2,48E+10	2,48E+10	3,01E+08	1,24E+06	1,20E+07
[ossolaris] solaris	[E.1] User errors	[C]	2,48E+10	2,48E+10	3,04E+08	1,26E+06	1,28E+07
[ospcwindows] ospcwindows	[E.1] User errors	[C]	2,48E+10	2,48E+10	3,04E+08	1,26E+06	1,28E+07
[ossw] os	[E.1] User errors	[C]	2,48E+10	2,48E+10	3,03E+08	1,25E+06	1,27E+07
[ossw] os	[E.8] Malware diffusion	[A]	2,48E+10	2,48E+10	3,09E+08	1,25E+06	1,21E+07
[appdpsn] appdpsnsolarisml370	[E.15] Accidental alteration of the information	[V]	2,48E+10	2,48E+10	1,91E+08	0.888843	4,69E+06
[oswindows] oswindows200server	[E.19] Information leaks	[C]	2,48E+10	2,48E+10	3,04E+08	1,26E+06	1,29E+07
[ossolaris] solaris	[E.1] User errors	[I]	2,48E+10	2,48E+10	3,04E+08	1,26E+06	1,32E+07
[serverblood] compaqproliantml370g3	[E.23] Defects in hardware maintenance / updating	[A]	2,48E+10	2,48E+10	4,39E+08	1,41E+06	1,75E+07
[ossw] os	[E.8] Malware diffusion	[C]	2,48E+10	2,48E+10	3,00E+08	1,24E+06	1,18E+07
[appsfinancialwindowspc] logisticsexternalpatients	[E.19] Information leaks	[C]	2,48E+10	2,48E+10	2,22E+08	0.961740	6,65E+06
[serverprot] questwinerserver	[E.23] Defects in hardware maintenance / updating	[A]	2,48E+10	2,48E+10	4,39E+08	1,41E+06	1,75E+07
[serverprot] questwinerserver	[E.8] Malware diffusion	[A]	2,48E+10	2,48E+10	3,26E+08	1,29E+06	9,52E+06
[ospcwindows] ospcwindows	[E.8] Malware diffusion	[I]	2,48E+10	2,48E+10	3,01E+08	1,24E+06	1,23E+07
[appdpsn] appdpsnsolarisml370	[E.19] Information leaks	[V]	2,48E+10	2,48E+10	1,91E+08	0.888843	4,69E+06
[oswindows] oswindows200server	[E.8] Malware diffusion	[A]	2,48E+10	2,48E+10	3,10E+08	1,25E+06	1,24E+07
[appsfinancialwindowspc] logisticsexternalpatients	[E.8] Malware diffusion	[C]	2,48E+10	2,48E+10	2,19E+08	0.949768	6,02E+06
[ossolaris] solaris	[E.19] Information leaks	[C]	2,48E+10	2,48E+10	3,04E+08	1,26E+06	1,28E+07
[ospcwindows] ospcwindows	[E.1] User errors	[V]	2,48E+10	2,48E+10	3,06E+08	1,26E+06	1,35E+07
[ossolaris] solaris	[E.1] User errors	[V]	2,48E+10	2,48E+10	3,06E+08	1,26E+06	1,35E+07
[ossolaris] solaris	[E.8] Malware diffusion	[C]	2,48E+10	2,48E+10	3,01E+08	1,24E+06	1,20E+07
[ossw] os	[E.19] Information leaks	[C]	2,48E+10	2,48E+10	3,03E+08	1,25E+06	1,27E+07
[serverprot] questwinerserver	[E.8] Malware diffusion	[C]	2,48E+10	2,48E+10	3,32E+08	1,79E+06	9,09E+06
[appsfinancialwindowspc] logisticsexternalpatients	[E.1] User errors	[I]	2,48E+10	2,48E+10	2,22E+08	0.961740	6,86E+06
[serverpatients]	[E.19] Information	[C]	2,48E+10	2,48E+10	3,48E+08	2,27E+06	8,25E+06

compaqproliantml370	leaks						
[ospcwindows] ospcwindows	[E.8] Malware diffusion	[V]	2,48E+10	2,48E+10	2,96E+08	1,22E+06	1,19E+07
[serverblood] compaqproliantml370g3	[E.25] Equipment loss	[C]	2,48E+10	2,48E+10	3,26E+08	2,92E+06	9,64E+06
[serverprot] questwinerserver	[E.25] Equipment loss	[C]	2,48E+10	2,48E+10	3,58E+08	2,34E+06	1,09E+07
[serverblood] compaqproliantml370g3	[E.25] Equipment loss	[A]	2,48E+10	2,48E+10	3,09E+08	1,28E+06	1,10E+07
[serverprot] questwinerserver	[E.25] Equipment loss	[A]	2,48E+10	2,48E+10	3,42E+08	1,35E+06	1,16E+07
[serverpatients] compaqproliantml370	[E.25] Equipment loss	[C]	2,48E+10	2,48E+10	3,65E+08	2,85E+06	8,35E+06
[ospcwindows] ospcwindows	[E.21] Defects in software maintenance / updating	[I]	2,48E+10	2,48E+10	3,83E+08	1,28E+06	1,60E+07
[ossw] os	[E.21] Defects in software maintenance / updating	[A]	2,48E+10	2,48E+10	3,83E+08	1,28E+06	1,57E+07
[appsfinancialwindowspc] logisticsexternalpatients	[E.21] Defects in software maintenance / updating	[I]	2,48E+10	2,48E+10	2,95E+08	1,01E+06	9,33E+06
[oswindows] oswindows200server	[E.21] Defects in software maintenance / updating	[A]	2,48E+10	2,48E+10	3,83E+08	1,28E+06	1,57E+07
[ossolaris] solaris	[E.21] Defects in software maintenance / updating	[I]	2,48E+10	2,48E+10	3,83E+08	1,28E+06	1,60E+07
[serverprot] questwinerserver	[N.*] Other natural disasters	[A]	2,26E+10	2,26E+10	4,00E+08	1,29E+06	1,67E+07
[serverblood] compaqproliantml370g3	[N.*] Other natural disasters	[A]	2,26E+10	2,26E+10	4,00E+08	1,29E+06	1,68E+07
[COM.LAN] Local Area Network	[E.2] System / Security administrator errors	[V]	2,26E+10	2,26E+10	2,83E+08	1,68E+06	8,25E+06
[ospcwindows] ospcwindows	[E.2] System / Security administrator errors	[V]	2,26E+10	2,26E+10	2,78E+08	1,15E+06	1,23E+07
[personalcomputer] pcwindows	[A.23] Hardware manipulation	[C]	2,15E+10	2,15E+10	1,52E+08	0.763508	4,89E+06
[datapdpsn] datadpsn	[E.15] Accidental alteration of the information	[V]	2,15E+10	2,15E+10	1,52E+08	0.763508	4,91E+06
[datapdpsn] datadpsn	[E.14] Information leaks (> E.19)	[I]	2,15E+10	2,15E+10	1,52E+08	0.763508	4,89E+06
[personalcomputer] pcwindows	[E.24] System failure due to exhaustion of resources	[C]	2,15E+10	2,15E+10	2,72E+08	0.929269	7,36E+06
[serverpatients] compaqproliantml370	[A.25] Theft	[I]	2,15E+10	2,15E+10	3,75E+08	1,21E+06	1,17E+07
[personalcomputer] pcwindows	[E.24] System failure due to exhaustion of resources	[V]	2,15E+10	2,15E+10	2,72E+08	0.929269	7,39E+06
[datapdpsn] datadpsn	[A.6] Abuse of access privileges	[C]	2,15E+10	2,15E+10	1,52E+08	0.763746	5,00E+06
[datapdpsn] datadpsn	[A.6] Abuse of access privileges	[V]	2,15E+10	2,15E+10	1,52E+08	0.763746	5,02E+06
[financial] finlogisticssubcontractor	[A.5.1] By insiders	[A]	2,15E+10	2,15E+10	2,07E+08	0.718204	4,73E+06
[personalcomputer] pcwindows	[E.24] System failure due to exhaustion of resources	[I]	2,15E+10	2,15E+10	2,72E+08	0.929269	7,36E+06
[datapdpsn] datadpsn	[A.6] Abuse of access privileges	[I]	2,15E+10	2,15E+10	1,52E+08	0.763746	5,00E+06
[serverpatients]	[A.25] Theft	[V]	2,15E+10	2,15E+10	3,75E+08	1,21E+06	1,17E+07

compaqproliantml370							
[datapdpsn] datadpsn	[E.14] Information leaks (> E.19)	[C]	2,15E+10	2,15E+10	1,52E+08	0.763508	4,89E+06
[serverpatients] compaqproliantml370	[A.25] Theft	[C]	2,15E+10	2,15E+10	3,75E+08	1,21E+06	1,17E+07
[personalcomputer] pcwindows	[A.23] Hardware manipulation	[V]	2,15E+10	2,15E+10	1,52E+08	0.763508	4,91E+06
[ospcwindows] ospcwindows	[A.8] Malware diffusion	[V]	2,15E+10	2,15E+10	2,32E+08	0.792607	2,96E+06
[serverprot] questwinerserver	[A.25] Theft	[A]	2,15E+10	2,15E+10	3,75E+08	1,21E+06	1,17E+07
[datapdpsn] datadpsn	[E.14] Information leaks (> E.19)	[V]	2,15E+10	2,15E+10	1,52E+08	0.763508	4,91E+06
[serverprot] questwinerserver	[A.25] Theft	[C]	2,15E+10	2,15E+10	3,75E+08	1,21E+06	1,17E+07
[ospcwindows] ospcwindows	[A.8] Malware diffusion	[I]	2,15E+10	2,15E+10	2,32E+08	0.792607	2,96E+06
[personalcomputer] pcwindows	[A.23] Hardware manipulation	[I]	2,15E+10	2,15E+10	1,52E+08	0.763508	4,89E+06
[financial] finlogisticssubcontractor	[A.5.1] By insiders	[C]	2,15E+10	2,15E+10	2,07E+08	0.718204	4,73E+06
[ossw] os	[E.20] Software vulnerabilities	[I]	2,10E+10	2,10E+10	3,50E+08	1,15E+06	1,20E+07
[serverblood] compaqproliantml370g3	[E.2] System / Security administrator errors	[I]	2,10E+10	2,10E+10	2,47E+08	1,06E+06	8,01E+06
[ossw] os	[E.2] System / Security administrator errors	[I]	2,10E+10	2,10E+10	2,56E+08	1,06E+06	1,10E+07
[serverblood] compaqproliantml370g3	[A.11] Unauthorised access	[A]	2,09E+10	2,09E+10	3,12E+08	1,05E+06	6,43E+06
[COM.LAN] Local Area Network	[A.19] Disclosure of information	[V]	2,09E+10	2,09E+10	2,61E+08	1,55E+06	7,54E+06
[COM.LAN] Local Area Network	[A.15] Deliberate alteration of information	[I]	2,09E+10	2,09E+10	2,74E+08	1,42E+06	7,96E+06
[COM.LAN] Local Area Network	[A.14] Eavesdropping	[I]	2,09E+10	2,09E+10	3,96E+08	5,24E+06	4,76E+06
[ossolaris] solaris	[A.11] Unauthorised access	[I]	2,09E+10	2,09E+10	2,40E+08	0.821212	4,74E+06
[appsfinancialwindowspc] logisticsexternalpatients	[A.11] Unauthorised access	[I]	2,09E+10	2,09E+10	2,40E+08	0.821212	4,74E+06
[COM.LAN] Local Area Network	[A.15] Deliberate alteration of information	[V]	2,09E+10	2,09E+10	2,61E+08	1,55E+06	7,54E+06
[COM.LAN] Local Area Network	[A.14] Eavesdropping	[V]	2,09E+10	2,09E+10	3,96E+08	5,24E+06	4,76E+06
[serverprot] questwinerserver	[A.11] Unauthorised access	[A]	2,09E+10	2,09E+10	3,05E+08	1,04E+06	6,62E+06
[serverpatients] compaqproliantml370	[A.11] Unauthorised access	[I]	2,09E+10	2,09E+10	3,41E+08	1,12E+06	6,55E+06
[COM.LAN] Local Area Network	[A.18] Destruction of information	[C]	2,09E+10	2,09E+10	2,74E+08	1,42E+06	7,87E+06
[COM.LAN] Local Area Network	[A.18] Destruction of information	[V]	2,09E+10	2,09E+10	2,61E+08	1,55E+06	7,54E+06
[COM.LAN] Local Area Network	[A.11] Unauthorised access	[I]	2,09E+10	2,09E+10	2,36E+08	0.805848	3,22E+06
[ospcwindows] ospcwindows	[A.11] Unauthorised access	[I]	2,09E+10	2,09E+10	2,40E+08	0.821212	4,74E+06
[COM.LAN] Local Area Network	[A.19] Disclosure of information	[I]	2,09E+10	2,09E+10	2,74E+08	1,42E+06	7,96E+06
[COM.LAN] Local Area Network	[A.15] Deliberate alteration of information	[C]	2,09E+10	2,09E+10	2,74E+08	1,42E+06	7,87E+06
[COM.LAN] Local Area Network	[A.18] Destruction of information	[I]	2,09E+10	2,09E+10	2,74E+08	1,42E+06	7,96E+06
[COM.LAN] Local Area Network	[A.11] Unauthorised access	[V]	2,09E+10	2,09E+10	2,24E+08	0.767541	2,72E+06
[S_blooddata] s_blooddata	[E.2] System / Security administrator errors	[I]	2,00E+10	2,00E+10	1,91E+08	1,47E+06	4,36E+06

[COM.LAN] Local Area Network	[A.12] Traffic analysis	[I]	1,90E+10	1,90E+10	2,48E+08	0.839831	5,71E+06
[COM.LAN] Local Area Network	[A.9] [Re-]routing of messages	[C]	1,90E+10	1,90E+10	2,49E+08	1,29E+06	7,15E+06
[COM.LAN] Local Area Network	[A.12] Traffic analysis	[V]	1,90E+10	1,90E+10	2,48E+08	0.839831	5,71E+06
[COM.LAN] Local Area Network	[A.10] Sequence alteration	[C]	1,90E+10	1,90E+10	2,49E+08	1,29E+06	7,15E+06
[COM.LAN] Local Area Network	[A.10] Sequence alteration	[V]	1,90E+10	1,90E+10	2,37E+08	1,41E+06	6,85E+06
[COM.LAN] Local Area Network	[A.9] [Re-]routing of messages	[I]	1,90E+10	1,90E+10	2,49E+08	1,29E+06	7,23E+06
[COM.LAN] Local Area Network	[A.10] Sequence alteration	[I]	1,90E+10	1,90E+10	2,49E+08	1,29E+06	7,23E+06
[COM.LAN] Local Area Network	[A.9] [Re-]routing of messages	[V]	1,90E+10	1,90E+10	2,37E+08	1,41E+06	6,85E+06
[aimodosia] workingroomaimodosia	[N.1] Fire	[A]	1,22E+10	1,22E+10	1,59E+08	0,00E+00	6,14E+06
[aimodosia] workingroomaimodosia	[N.2] Water	[A]	1,22E+10	1,22E+10	2,15E+08	0,00E+00	6,68E+06
[ossw] os	[A.22] Software manipulation	[V]	1,21E+10	1,21E+10	1,48E+08	0.612492	6,52E+06
[ossolaris] solaris	[A.6] Abuse of access privileges	[A]	1,21E+10	1,21E+10	1,59E+08	0.640065	7,43E+06
[ospcwindows] ospcwindows	[A.6] Abuse of access privileges	[A]	1,21E+10	1,21E+10	1,59E+08	0.640065	7,43E+06
[serverblood] compaqproliantml370g3	[A.6] Abuse of access privileges	[I]	1,21E+10	1,21E+10	1,44E+08	0.617257	4,81E+06
[ossw] os	[A.6] Abuse of access privileges	[I]	1,21E+10	1,21E+10	1,52E+08	0.628949	7,12E+06
[serverprot] questwinerserver	[A.7] Misuse	[I]	1,21E+10	1,21E+10	1,58E+08	0.634760	4,89E+06
[ospcwindows] ospcwindows	[A.7] Misuse	[A]	1,21E+10	1,21E+10	1,56E+08	0.627518	6,84E+06
[ossw] os	[A.7] Misuse	[V]	1,21E+10	1,21E+10	1,48E+08	0.612492	6,52E+06
[ossw] os	[A.6] Abuse of access privileges	[V]	1,21E+10	1,21E+10	1,53E+08	0.632225	7,42E+06
[serverpatients] compaqproliantml370	[A.7] Misuse	[A]	1,21E+10	1,21E+10	1,54E+08	0.619741	4,61E+06
[appsfinancialwindowspc] logisticsexternalpatients	[A.7] Misuse	[A]	1,21E+10	1,21E+10	1,15E+08	0.480381	3,65E+06
[appsfinancialwindowspc] logisticsexternalpatients	[A.6] Abuse of access privileges	[A]	1,21E+10	1,21E+10	1,18E+08	0.491115	4,03E+06
[ossw] os	[A.7] Misuse	[I]	1,21E+10	1,21E+10	1,48E+08	0.610250	6,33E+06
[ossolaris] solaris	[A.7] Misuse	[A]	1,21E+10	1,21E+10	1,56E+08	0.627518	6,84E+06
[ossw] os	[E.19] Information leaks	[V]	1,15E+10	1,15E+10	1,42E+08	0.584618	6,27E+06
[oswindows] oswindows200server	[E.1] User errors	[V]	1,15E+10	1,15E+10	1,42E+08	0.586571	6,39E+06
[ossw] os	[E.1] User errors	[I]	1,15E+10	1,15E+10	1,41E+08	0.582477	6,09E+06
[ossolaris] solaris	[E.1] User errors	[A]	1,15E+10	1,15E+10	1,49E+08	0.598229	6,54E+06
[ospcwindows] ospcwindows	[E.1] User errors	[A]	1,15E+10	1,15E+10	1,49E+08	0.598229	6,54E+06
[oswindows] oswindows200server	[E.18] Destruction of information	[V]	1,15E+10	1,15E+10	1,42E+08	0.586571	6,39E+06
[ossw] os	[E.1] User errors	[V]	1,15E+10	1,15E+10	1,42E+08	0.584618	6,27E+06
[ossw] os	[E.8] Malware diffusion	[I]	1,15E+10	1,15E+10	1,39E+08	0.575827	5,66E+06
[oswindows] oswindows200server	[E.8] Malware diffusion	[V]	1,15E+10	1,15E+10	1,37E+08	0.567828	5,63E+06
[ossw] os	[E.15] Accidental alteration of the information	[V]	1,15E+10	1,15E+10	1,42E+08	0.584618	6,27E+06
[oswindows] oswindows200server	[E.15] Accidental alteration of the information	[I]	1,15E+10	1,15E+10	1,42E+08	0.584437	6,19E+06
[ossw] os	[E.18] Destruction of information	[V]	1,15E+10	1,15E+10	1,42E+08	0.584618	6,27E+06
[serverpatients] compaqproliantml370	[E.18] Destruction of information	[A]	1,15E+10	1,15E+10	1,54E+08	0.606526	4,06E+06

[ossw] os	[E.8] Malware diffusion	[V]	1,15E+10	1,15E+10	1,37E+08	0.565875	5,52E+06
[serverprot] questwinerserver	[E.15] Accidental alteration of the information	[I]	1,15E+10	1,15E+10	1,51E+08	0.605660	4,70E+06
[appdpsn] appdpsnsolarisml370	[E.18] Destruction of information	[A]	1,15E+10	1,15E+10	1,04E+08	0.444775	2,57E+06
[appsfinancialwindowspc] logisticsexternalpatients	[E.1] User errors	[A]	1,15E+10	1,15E+10	1,10E+08	0.458013	3,50E+06
[ossw] os	[E.21] Defects in software maintenance / updating	[I]	1,15E+10	1,15E+10	1,78E+08	0.594596	7,48E+06
[offices] workingroomisthodosias	[A.27] Enemy over-run	[C]	1,08E+10	1,08E+10	1,36E+08	0.464748	4,78E+06
[dataemployees] dataemployees	[A.5.3] By outsiders	[I]	1,08E+10	1,08E+10	1,03E+08	0.359102	2,37E+06
[COM.LAN] Local Area Network	[A.5] Masquerading of identity	[V]	1,08E+10	1,08E+10	1,21E+08	0.442787	4,24E+06
[dataemployees] dataemployees	[A.5.3] By outsiders	[C]	1,08E+10	1,08E+10	1,03E+08	0.359102	2,37E+06
[dc] datacenterpliroforikhsorganwsis	[A.27] Enemy over-run	[C]	1,08E+10	1,08E+10	1,36E+08	0.464748	4,78E+06
[ospcwindows] ospcwindows	[E.20] Software vulnerabilities	[A]	1,05E+10	1,05E+10	1,75E+08	0.572972	5,94E+06
[ossw] os	[E.2] System / Security administrator errors	[V]	1,05E+10	1,05E+10	1,29E+08	0.531471	5,70E+06
[appsfinancialwindowspc] logisticsexternalpatients	[E.20] Software vulnerabilities	[A]	1,05E+10	1,05E+10	1,32E+08	0.449850	3,33E+06
[ossolaris] solaris	[E.20] Software vulnerabilities	[A]	1,05E+10	1,05E+10	1,75E+08	0.572972	5,94E+06
[ossw] os	[E.20] Software vulnerabilities	[V]	1,05E+10	1,05E+10	1,75E+08	0.572972	6,42E+06
[financial] finlogisticssubcontractor	[A.5.3] By outsiders	[V]	1,00E+10	1,00E+10	9,63E+07	0.334308	2,25E+06
[hospitaldepartments] hospitaldepartments	[A.27] Enemy over-run	[A]	1,00E+10	1,00E+10	1,30E+08	0,00E+00	5,65E+06
[COM.LAN] Local Area Network	[E.15] Accidental alteration of the information	[A]	1,00E+10	1,00E+10	1,30E+08	0.703031	4,17E+06
[hospitaldepartments] hospitaldepartments	[N.1] Fire	[A]	1,00E+10	1,00E+10	1,31E+08	0,00E+00	5,06E+06
[serverprot] questwinerserver	[A.25] Theft	[V]	1,00E+10	1,00E+10	1,74E+08	0.563945	5,51E+06
[financial] finlogisticssubcontractor	[A.5.1] By insiders	[V]	1,00E+10	1,00E+10	9,63E+07	0.334217	2,23E+06
[ossw] os	[A.19] Disclosure of information	[V]	9,70E+09	9,70E+09	1,19E+08	0.489993	5,22E+06
[ossw] os	[A.8] Malware diffusion	[V]	9,70E+09	9,70E+09	1,05E+08	0.357669	1,34E+06
[ossw] os	[A.5] Masquerading of identity	[V]	9,70E+09	9,70E+09	9,34E+07	0.324258	2,16E+06
[ossw] os	[A.15] Deliberate alteration of information	[V]	9,70E+09	9,70E+09	1,19E+08	0.489993	5,22E+06
[ossw] os	[A.11] Unauthorised access	[I]	9,70E+09	9,70E+09	1,12E+08	0.382330	2,24E+06
[ossw] os	[A.18] Destruction of information	[V]	9,70E+09	9,70E+09	1,19E+08	0.489993	5,22E+06
[serverblood] compaqproliantml370g3	[A.11] Unauthorised access	[I]	9,70E+09	9,70E+09	1,45E+08	0.489168	3,09E+06
[ossw] os	[A.11] Unauthorised access	[V]	9,70E+09	9,70E+09	1,05E+08	0.360980	2,30E+06
[COM.LAN] Local Area Network	[A.12] Traffic analysis	[C]	3,79E+09	3,79E+09	4,96E+07	0.167966	1,16E+06
[serverprot] questwinerserver	[A.7] Misuse	[A]	2,61E+09	2,61E+09	3,51E+07	0.138125	1,13E+06
[serverblood] compaqproliantml370g3	[A.7] Misuse	[A]	2,61E+09	2,61E+09	3,21E+07	0.132984	1,13E+06
[ossw] os	[A.6] Abuse of access	[A]	2,61E+09	2,61E+09	3,41E+07	0.137098	1,61E+06

	privileges						
[oswindows] oswindows200server	[A.6] Abuse of access privileges	[A]	2,61E+09	2,61E+09	3,42E+07	0.137492	1,64E+06
[serverpatients] compaqproliantml370	[A.7] Misuse	[I]	2,61E+09	2,61E+09	3,46E+07	0.139319	0.976669
[ossw] os	[A.7] Misuse	[A]	2,61E+09	2,61E+09	3,34E+07	0.134403	1,49E+06
[oswindows] oswindows200server	[A.7] Misuse	[A]	2,61E+09	2,61E+09	3,35E+07	0.134793	1,51E+06
[oswindows] oswindows200server	[E.1] User errors	[A]	2,48E+09	2,48E+09	3,19E+07	0.128505	1,44E+06
[ospcwindows] ospcwindows	[E.15] Accidental alteration of the information	[I]	2,48E+09	2,48E+09	3,05E+07	0.125833	1,34E+06
[ossolaris] solaris	[E.15] Accidental alteration of the information	[I]	2,48E+09	2,48E+09	3,05E+07	0.125833	1,34E+06
[appsfinancialwindowspc] logisticsexternalpatients	[E.15] Accidental alteration of the information	[I]	2,48E+09	2,48E+09	2,23E+07	0.096273	0.697874
[serverpatients] compaqproliantml370	[E.15] Accidental alteration of the information	[I]	2,48E+09	2,48E+09	3,30E+07	0.132954	0.938661
[appdpsn] appdpsnsolarisml370	[E.15] Accidental alteration of the information	[I]	2,48E+09	2,48E+09	2,19E+07	0.096081	0.567760
[serverprot] questwinerserver	[E.1] User errors	[A]	2,48E+09	2,48E+09	3,34E+07	0.131662	1,08E+06
[ossw] os	[E.1] User errors	[A]	2,48E+09	2,48E+09	3,18E+07	0.128132	1,42E+06
[S_blooddata] s_blooddata	[E.18] Destruction of information	[A]	2,48E+09	2,48E+09	2,23E+07	0.095114	0.550869
[ossw] os	[E.20] Software vulnerabilities	[A]	2,26E+09	2,26E+09	3,76E+07	0.123189	1,30E+06
[oswindows] oswindows200server	[E.20] Software vulnerabilities	[A]	2,26E+09	2,26E+09	3,76E+07	0.123189	1,30E+06
[serverpatients] compaqproliantml370	[E.3] Monitoring errors (log)	[I]	2,26E+09	2,26E+09	3,00E+07	0.120868	0.853329
[COM.LAN] Local Area Network	[E.15] Accidental alteration of the information	[C]	2,15E+09	2,15E+09	2,75E+07	0.110675	0.823933
[secretary] secretary	[A.27] Enemy over-run	[A]	2,15E+09	2,15E+09	2,80E+07	0,00E+00	1,22E+06
[COM.LAN] Local Area Network	[E.15] Accidental alteration of the information	[V]	2,15E+09	2,15E+09	2,58E+07	0.107111	0.793410
[secretary] secretary	[N.1] Fire	[A]	2,15E+09	2,15E+09	2,81E+07	0,00E+00	1,09E+06
[secretary] secretary	[N.2] Water	[A]	2,15E+09	2,15E+09	3,81E+07	0,00E+00	1,19E+06
[COM.LAN] Local Area Network	[A.14] Eavesdropping	[C]	2,09E+09	2,09E+09	2,71E+07	0.092381	0.492353
[serverpatients] compaqproliantml370	[A.3] Manipulation of activity records (log)	[V]	1,94E+09	1,94E+09	2,36E+07	0,00E+00	0.658726
[serverblood] compaqproliantml370g3	[A.7] Misuse	[I]	1,21E+09	1,21E+09	1,42E+07	0.061037	0.469721
[S_blooddata] s_blooddata	[E.15] Accidental alteration of the information	[I]	1,15E+09	1,15E+09	1,01E+07	0.044491	0.258786
[ossw] os	[E.15] Accidental alteration of the information	[I]	1,15E+09	1,15E+09	1,41E+07	0.058266	0.612826
[hospitaldepartments] hospitaldepartments	[A.27] Enemy over-run	[C]	1,08E+09	1,08E+09	1,36E+07	0,00E+00	0.486093
[aimodosia] workingroomaimodosia	[A.26] Destructive attack	[A]	1,08E+09	1,08E+09	1,42E+07	0.048273	0.514387
[secretary] secretary	[A.27] Enemy over-run	[C]	1,08E+09	1,08E+09	1,36E+07	0,00E+00	0.486093
[serverpatients] compaqproliantml370	[A.23] Hardware manipulation	[V]	1,08E+09	1,08E+09	1,32E+07	0,00E+00	0.396541
[COM.LAN] Local Area Network	[A.5] Masquerading of identity	[A]	1,00E+09	1,00E+09	1,12E+07	0.038495	0.398307

[serverpatients] compaqproliantml370	[A.26] Destructive attack	[A]	1,00E+09	1,00E+09	1,70E+07	0.055259	0.562664
[COM.LAN] Local Area Network	[E.19] Information leaks	[A]	1,00E+09	1,00E+09	1,26E+07	0.050832	0.423861
[COM.LAN] Local Area Network	[E.24] System failure due to exhaustion of resources	[A]	1,00E+09	1,00E+09	1,34E+07	0.045736	0.496467
[dc] datacenterpliroforikhsorganwsis	[A.26] Destructive attack	[A]	8,82E+08	8,82E+08	1,17E+07	0.039731	0.423363
[secretary] secretary	[A.26] Destructive attack	[I]	8,82E+08	8,82E+08	1,14E+07	0.038690	0.306934
[offices] workingroomisthodosias	[A.26] Destructive attack	[A]	8,82E+08	8,82E+08	1,17E+07	0.039731	0.423363
[aimodosia] workingroomaimodosia	[A.26] Destructive attack	[C]	3,79E+08	3,79E+08	4,88E+06	0.016637	0.131982
[aimodosia] workingroomaimodosia	[A.26] Destructive attack	[I]	2,78E+08	2,78E+08	3,58E+06	0.012187	0.097934
[aimodosia] workingroomaimodosia	[A.26] Destructive attack	[V]	2,78E+08	2,78E+08	3,58E+06	0.012187	0.097934
[COM.LAN] Local Area Network	[E.19] Information leaks	[V]	2,15E+08	2,15E+08	2,58E+06	0.010713	0.080548
[COM.LAN] Local Area Network	[E.15] Accidental alteration of the information	[I]	2,15E+08	2,15E+08	2,75E+06	0.011073	0.084219
[serverpatients] compaqproliantml370	[A.26] Destructive attack	[V]	2,15E+08	2,15E+08	3,45E+06	0.011357	0.083042
[COM.LAN] Local Area Network	[A.5] Masquerading of identity	[C]	2,15E+08	2,15E+08	2,40E+06	0.008277	0.085918
[COM.LAN] Local Area Network	[E.24] System failure due to exhaustion of resources	[I]	2,15E+08	2,15E+08	3,74E+06	0.012122	0.110953
[serverblood] compaqproliantml370g3	[A.23] Hardware manipulation	[A]	2,15E+08	2,15E+08	2,68E+06	0.011085	0.099427
[COM.LAN] Local Area Network	[E.19] Information leaks	[C]	2,15E+08	2,15E+08	2,75E+06	0.011073	0.083152
[serverpatients] compaqproliantml370	[A.26] Destructive attack	[I]	2,15E+08	2,15E+08	3,45E+06	0.011357	0.083042
[COM.LAN] Local Area Network	[A.5] Masquerading of identity	[I]	2,15E+08	2,15E+08	2,40E+06	0.008277	0.085918
[COM.LAN] Local Area Network	[E.24] System failure due to exhaustion of resources	[V]	2,15E+08	2,15E+08	3,74E+06	0.012122	0.111271
[COM.LAN] Local Area Network	[E.19] Information leaks	[I]	2,15E+08	2,15E+08	2,75E+06	0.011073	0.084219
[serverpatients] compaqproliantml370	[A.26] Destructive attack	[C]	2,15E+08	2,15E+08	3,45E+06	0.011357	0.083042
[dc] datacenterpliroforikhsorganwsis	[A.27] Enemy over-run	[V]	2,15E+08	2,15E+08	2,73E+06	0.009295	0.100093
[offices] workingroomisthodosias	[A.27] Enemy over-run	[V]	2,15E+08	2,15E+08	2,73E+06	0.009295	0.100093
[COM.LAN] Local Area Network	[E.24] System failure due to exhaustion of resources	[C]	2,15E+08	2,15E+08	3,74E+06	0.012122	0.110953
[dataemployees] dataemployees	[A.5.3] By outsiders	[V]	2,15E+08	2,15E+08	2,07E+06	0.007189	0.048817
[serverblood] compaqproliantml370g3	[A.23] Hardware manipulation	[C]	2,15E+08	2,15E+08	2,54E+06	0.010913	0.086889
[offices] workingroomisthodosias	[A.26] Destructive attack	[V]	1,90E+08	1,90E+08	2,44E+06	0.008318	0.066844
[dc] datacenterpliroforikhsorganwsis	[A.26] Destructive attack	[I]	1,90E+08	1,90E+08	2,44E+06	0.008318	0.066844
[secretary] secretary	[A.26] Destructive attack	[C]	1,90E+08	1,90E+08	2,44E+06	0.008318	0.066844
[offices] workingroomisthodosias	[A.26] Destructive attack	[I]	1,90E+08	1,90E+08	2,44E+06	0.008318	0.066844
[dc] datacenterpliroforikhsorganwsis	[A.26] Destructive attack	[C]	1,90E+08	1,90E+08	2,44E+06	0.008318	0.066844
[offices] workingroomisthodosias	[A.26] Destructive attack	[C]	1,90E+08	1,90E+08	2,44E+06	0.008318	0.066844
[dc]	[A.26] Destructive	[V]	1,90E+08	1,90E+08	2,44E+06	0.008318	0.066844

datacenterpliroforikhsorganwsis	attack						
[secretary] secretary	[A.26] Destructive attack	[A]	1,90E+08	1,90E+08	2,51E+06	0.008542	0.091573
[aimodosia] workingroomaimodosia	[N.*] Other natural disasters	[A]	1,22E+08	1,22E+08	2,17E+06	0,00E+00	0.075324
[serverblood] compaqproliantml370g3	[A.23] Hardware manipulation	[V]	1,00E+08	1,00E+08	1,18E+06	0.005085	0.043711
[offices] workingroomisthodosias	[N.*] Other natural disasters	[A]	1,00E+08	1,00E+08	1,79E+06	0,00E+00	0.062332
[serverprot] questwinerserver	[N.1] Fire	[I]	1,00E+08	1,00E+08	1,74E+06	0,00E+00	0.056540
[dc] datacenterpliroforikhsorganwsis	[N.2] Water	[A]	1,00E+08	1,00E+08	1,77E+06	0,00E+00	0.056015
[personalcomputer] pcwindows	[A.26] Destructive attack	[A]	1,00E+08	1,00E+08	1,24E+06	0,00E+00	0.048982
[hospitaldepartments] hospitaldepartments	[A.26] Destructive attack	[A]	1,00E+08	1,00E+08	1,32E+06	0,00E+00	0.048290
[serverpatients] compaqproliantml370	[A.3] Manipulation of activity records (log)	[A]	1,00E+08	1,00E+08	1,27E+06	0,00E+00	0.038791
[serverpatients] compaqproliantml370	[A.23] Hardware manipulation	[A]	1,00E+08	1,00E+08	1,28E+06	0,00E+00	0.040636
[hospitaldepartments] hospitaldepartments	[N.*] Other natural disasters	[A]	1,00E+08	1,00E+08	1,79E+06	0,00E+00	0.062332
[dc] datacenterpliroforikhsorganwsis	[N.*] Other natural disasters	[A]	1,00E+08	1,00E+08	1,79E+06	0,00E+00	0.062332
[secretary] secretary	[N.*] Other natural disasters	[I]	1,00E+08	1,00E+08	1,74E+06	0,00E+00	0.047400
[serverprot] questwinerserver	[N.2] Water	[I]	1,00E+08	1,00E+08	1,74E+06	0,00E+00	0.056540
[personalcomputer] pcwindows	[N.1] Fire	[A]	1,00E+08	1,00E+08	1,24E+06	0,00E+00	0.048982
[serverpatients] compaqproliantml370	[N.1] Fire	[A]	1,00E+08	1,00E+08	1,77E+06	0,00E+00	0.075674
[serverpatients] compaqproliantml370	[N.2] Water	[A]	1,00E+08	1,00E+08	1,77E+06	0,00E+00	0.075674
[serverprot] questwinerserver	[E.20] Software vulnerabilities	[I]	1,00E+08	1,00E+08	1,64E+06	0,00E+00	0.059704
[offices] workingroomisthodosias	[N.1] Fire	[A]	1,00E+08	1,00E+08	1,31E+06	0,00E+00	0.051446
[COM.LAN] Local Area Network	[E.10] Sequence errors	[A]	1,00E+08	1,00E+08	1,26E+06	0,00E+00	0.042666
[COM.LAN] Local Area Network	[E.9] [Re-]routing errors	[A]	1,00E+08	1,00E+08	1,26E+06	0,00E+00	0.042666
[serverblood] compaqproliantml370g3	[A.23] Hardware manipulation	[I]	1,00E+08	1,00E+08	1,19E+06	0.005091	0.040589
[serverprot] questwinerserver	[E.21] Defects in software maintenance / updating	[I]	1,00E+08	1,00E+08	1,53E+06	0,00E+00	0.048685
[personalcomputer] pcwindows	[E.23] Defects in hardware maintenance / updating	[A]	1,00E+08	1,00E+08	1,17E+06	0,00E+00	0.030942
[personalcomputer] pcwindows	[N.2] Water	[A]	1,00E+08	1,00E+08	1,24E+06	0,00E+00	0.048982
[offices] workingroomisthodosias	[N.2] Water	[A]	1,00E+08	1,00E+08	1,77E+06	0,00E+00	0.056015
[hospitaldepartments] hospitaldepartments	[N.2] Water	[A]	1,00E+08	1,00E+08	1,77E+06	0,00E+00	0.056015
[serverpatients] compaqproliantml370	[E.23] Defects in hardware maintenance / updating	[A]	1,00E+08	1,00E+08	1,77E+06	0,00E+00	0.071776
[dc] datacenterpliroforikhsorganwsis	[N.1] Fire	[A]	1,00E+08	1,00E+08	1,31E+06	0,00E+00	0.051446
[secretary] secretary	[A.26] Destructive attack	[V]	8,82E+07	8,82E+07	1,14E+06	0.003869	0.031090
[aimodosia] workingroomaimodosia	[N.*] Other natural disasters	[C]	4,30E+07	4,30E+07	0.749775	0,00E+00	0.020382
[aimodosia] workingroomaimodosia	[N.*] Other natural disasters	[I]	3,15E+07	3,15E+07	0.549254	0,00E+00	0.014931

[aimodosia] workingroomaimodosia	[N.*] Other natural disasters	[V]	3,15E+07	3,15E+07	0.549254	0,00E+00	0.014931
[COM.LAN] Local Area Network	[E.10] Sequence errors	[C]	2,15E+07	2,15E+07	0.275450	0,00E+00	0.008315
[hospitaldepartments] hospitaldepartments	[N.*] Other natural disasters	[V]	2,15E+07	2,15E+07	0.374887	0,00E+00	0.010191
[serverpatients] compaqproliantml370	[E.23] Defects in hardware maintenance / updating	[C]	2,15E+07	2,15E+07	0.380011	0,00E+00	0.015894
[serverpatients] compaqproliantml370	[A.3] Manipulation of activity records (log)	[I]	2,15E+07	2,15E+07	0.285292	0,00E+00	0.008099
[personalcomputer] pcwindows	[E.23] Defects in hardware maintenance / updating	[V]	2,15E+07	2,15E+07	0.252282	0,00E+00	0.006653
[serverpatients] compaqproliantml370	[N.1] Fire	[C]	2,15E+07	2,15E+07	0.374887	0,00E+00	0.012156
[personalcomputer] pcwindows	[N.2] Water	[C]	2,15E+07	2,15E+07	0.252282	0,00E+00	0.006653
[hospitaldepartments] hospitaldepartments	[N.2] Water	[C]	2,15E+07	2,15E+07	0.380011	0,00E+00	0.009865
[offices] workingroomisthodosias	[N.2] Water	[I]	2,15E+07	2,15E+07	0.380011	0,00E+00	0.009865
[dc] datacenterpliroforikhsorganwsis	[N.1] Fire	[C]	2,15E+07	2,15E+07	0.280146	0,00E+00	0.009467
[serverblood] compaqproliantml370g3	[A.26] Destructive attack	[C]	2,15E+07	2,15E+07	0.345043	0,00E+00	0.008304
[serverpatients] compaqproliantml370	[A.23] Hardware manipulation	[I]	2,15E+07	2,15E+07	0.287205	0,00E+00	0.008296
[offices] workingroomisthodosias	[N.*] Other natural disasters	[C]	2,15E+07	2,15E+07	0.374887	0,00E+00	0.010191
[offices] workingroomisthodosias	[N.*] Other natural disasters	[V]	2,15E+07	2,15E+07	0.374887	0,00E+00	0.010191
[serverblood] compaqproliantml370g3	[N.1] Fire	[C]	2,15E+07	2,15E+07	0.374887	0,00E+00	0.012156
[dc] datacenterpliroforikhsorganwsis	[N.2] Water	[C]	2,15E+07	2,15E+07	0.380011	0,00E+00	0.009865
[dc] datacenterpliroforikhsorganwsis	[N.2] Water	[V]	2,15E+07	2,15E+07	0.380011	0,00E+00	0.009865
[hospitaldepartments] hospitaldepartments	[N.*] Other natural disasters	[I]	2,15E+07	2,15E+07	0.374887	0,00E+00	0.010191
[serverprot] questwinerserver	[E.20] Software vulnerabilities	[C]	2,15E+07	2,15E+07	0.351717	0,00E+00	0.012939
[serverprot] questwinerserver	[N.1] Fire	[A]	2,15E+07	2,15E+07	0.381031	0,00E+00	0.016148
[personalcomputer] pcwindows	[N.1] Fire	[C]	2,15E+07	2,15E+07	0.252282	0,00E+00	0.006653
[serverblood] compaqproliantml370g3	[N.2] Water	[A]	2,15E+07	2,15E+07	0.381031	0,00E+00	0.016270
[offices] workingroomisthodosias	[N.1] Fire	[C]	2,15E+07	2,15E+07	0.280146	0,00E+00	0.009467
[personalcomputer] pcwindows	[N.2] Water	[V]	2,15E+07	2,15E+07	0.252282	0,00E+00	0.006653
[COM.LAN] Local Area Network	[E.9] [Re-]routing errors	[I]	2,15E+07	2,15E+07	0.275450	0,00E+00	0.008422
[hospitaldepartments] hospitaldepartments	[N.2] Water	[V]	2,15E+07	2,15E+07	0.380011	0,00E+00	0.009865
[serverblood] compaqproliantml370g3	[N.1] Fire	[A]	2,15E+07	2,15E+07	0.381031	0,00E+00	0.016270
[dc] datacenterpliroforikhsorganwsis	[N.1] Fire	[V]	2,15E+07	2,15E+07	0.280146	0,00E+00	0.009467
[serverprot] questwinerserver	[E.20] Software vulnerabilities	[A]	2,15E+07	2,15E+07	0.351717	0,00E+00	0.012785
[serverpatients] compaqproliantml370	[N.2] Water	[C]	2,15E+07	2,15E+07	0.374887	0,00E+00	0.012156
[COM.LAN] Local Area Network	[E.10] Sequence errors	[V]	2,15E+07	2,15E+07	0.257937	0,00E+00	0.008055
[serverpatients] compaqproliantml370	[E.23] Defects in hardware maintenance / updating	[V]	2,15E+07	2,15E+07	0.380011	0,00E+00	0.015894

[serverprot] questwinerserver	[N.2] Water	[A]	2,15E+07	2,15E+07	0.381031	0,00E+00	0.016148
[personalcomputer] pcwindows	[A.26] Destructive attack	[C]	2,15E+07	2,15E+07	0.252282	0,00E+00	0.006653
[personalcomputer] pcwindows	[N.1] Fire	[V]	2,15E+07	2,15E+07	0.252282	0,00E+00	0.006653
[hospitaldepartments] hospitaldepartments	[A.26] Destructive attack	[C]	2,15E+07	2,15E+07	0.276848	0,00E+00	0.007579
[serverpatients] compaqproliantml370	[A.3] Manipulation of activity records (log)	[C]	2,15E+07	2,15E+07	0.281943	0,00E+00	0.007203
[hospitaldepartments] hospitaldepartments	[N.2] Water	[I]	2,15E+07	2,15E+07	0.380011	0,00E+00	0.009865
[personalcomputer] pcwindows	[N.2] Water	[I]	2,15E+07	2,15E+07	0.252282	0,00E+00	0.006653
[offices] workingroomisthodosias	[N.2] Water	[C]	2,15E+07	2,15E+07	0.380011	0,00E+00	0.009865
[serverpatients] compaqproliantml370	[N.1] Fire	[I]	2,15E+07	2,15E+07	0.374887	0,00E+00	0.012156
[serverpatients] compaqproliantml370	[N.2] Water	[V]	2,15E+07	2,15E+07	0.374887	0,00E+00	0.012156
[hospitaldepartments] hospitaldepartments	[A.26] Destructive attack	[I]	2,15E+07	2,15E+07	0.276848	0,00E+00	0.007579
[personalcomputer] pcwindows	[A.26] Destructive attack	[I]	2,15E+07	2,15E+07	0.252282	0,00E+00	0.006653
[serverpatients] compaqproliantml370	[A.23] Hardware manipulation	[C]	2,15E+07	2,15E+07	0.283505	0,00E+00	0.007401
[offices] workingroomisthodosias	[N.1] Fire	[V]	2,15E+07	2,15E+07	0.280146	0,00E+00	0.009467
[COM.LAN] Local Area Network	[E.10] Sequence errors	[I]	2,15E+07	2,15E+07	0.275450	0,00E+00	0.008422
[dc] datacenterpliroforikhsorganwsis	[N.1] Fire	[I]	2,15E+07	2,15E+07	0.280146	0,00E+00	0.009467
[COM.LAN] Local Area Network	[E.9] [Re-]routing errors	[V]	2,15E+07	2,15E+07	0.257937	0,00E+00	0.008055
[serverpatients] compaqproliantml370	[E.23] Defects in hardware maintenance / updating	[I]	2,15E+07	2,15E+07	0.380011	0,00E+00	0.015193
[serverprot] questwinerserver	[N.1] Fire	[C]	2,15E+07	2,15E+07	0.374887	0,00E+00	0.012156
[serverblood] compaqproliantml370g3	[N.2] Water	[C]	2,15E+07	2,15E+07	0.374887	0,00E+00	0.012156
[personalcomputer] pcwindows	[E.23] Defects in hardware maintenance / updating	[C]	2,15E+07	2,15E+07	0.252282	0,00E+00	0.006653
[dc] datacenterpliroforikhsorganwsis	[N.*] Other natural disasters	[I]	2,15E+07	2,15E+07	0.374887	0,00E+00	0.010191
[serverprot] questwinerserver	[E.21] Defects in software maintenance / updating	[A]	2,15E+07	2,15E+07	0.329863	0,00E+00	0.010464
[serverprot] questwinerserver	[N.2] Water	[C]	2,15E+07	2,15E+07	0.374887	0,00E+00	0.012156
[personalcomputer] pcwindows	[N.1] Fire	[I]	2,15E+07	2,15E+07	0.252282	0,00E+00	0.006653
[COM.LAN] Local Area Network	[E.9] [Re-]routing errors	[C]	2,15E+07	2,15E+07	0.275450	0,00E+00	0.008315
[personalcomputer] pcwindows	[A.26] Destructive attack	[V]	2,15E+07	2,15E+07	0.252282	0,00E+00	0.006653
[hospitaldepartments] hospitaldepartments	[N.*] Other natural disasters	[C]	2,15E+07	2,15E+07	0.374887	0,00E+00	0.010191
[personalcomputer] pcwindows	[E.23] Defects in hardware maintenance / updating	[I]	2,15E+07	2,15E+07	0.252282	0,00E+00	0.006653
[serverpatients] compaqproliantml370	[N.1] Fire	[V]	2,15E+07	2,15E+07	0.374887	0,00E+00	0.012156
[serverblood] compaqproliantml370g3	[A.25] Theft	[A]	2,15E+07	2,15E+07	0.374887	0,00E+00	0.012156
[hospitaldepartments] hospitaldepartments	[A.26] Destructive attack	[V]	2,15E+07	2,15E+07	0.276848	0,00E+00	0.007579
[serverpatients]	[N.2] Water	[I]	2,15E+07	2,15E+07	0.374887	0,00E+00	0.012156

compaqproliantml370							
[secretary] secretary	[N.*] Other natural disasters	[C]	2,15E+07	2,15E+07	0.374887	0,00E+00	0.010191
[offices] workingroomisthodosias	[N.*] Other natural disasters	[I]	2,15E+07	2,15E+07	0.374887	0,00E+00	0.010191
[offices] workingroomisthodosias	[N.1] Fire	[I]	2,15E+07	2,15E+07	0.280146	0,00E+00	0.009467
[serverprot] questwinerserver	[E.21] Defects in software maintenance / updating	[C]	2,15E+07	2,15E+07	0.329863	0,00E+00	0.010583
[serverblood] compaqproliantml370g3	[A.25] Theft	[C]	2,15E+07	2,15E+07	0.374887	0,00E+00	0.012156
[dc] datacenterpliroforikhsorganwsis	[N.2] Water	[I]	2,15E+07	2,15E+07	0.380011	0,00E+00	0.009865
[secretary] secretary	[N.*] Other natural disasters	[A]	2,15E+07	2,15E+07	0.384547	0,00E+00	0.013401
[dc] datacenterpliroforikhsorganwsis	[N.*] Other natural disasters	[C]	2,15E+07	2,15E+07	0.374887	0,00E+00	0.010191
[serverblood] compaqproliantml370g3	[A.26] Destructive attack	[A]	2,15E+07	2,15E+07	0.364473	0,00E+00	0.012163
[dc] datacenterpliroforikhsorganwsis	[N.*] Other natural disasters	[V]	2,15E+07	2,15E+07	0.374887	0,00E+00	0.010191
[serverblood] compaqproliantml370g3	[N.2] Water	[I]	1,00E+07	1,00E+07	0.174366	0,00E+00	0.005654
[secretary] secretary	[N.*] Other natural disasters	[V]	1,00E+07	1,00E+07	0.174366	0,00E+00	0.004740
[serverblood] compaqproliantml370g3	[A.25] Theft	[I]	1,00E+07	1,00E+07	0.174366	0,00E+00	0.005654
[serverblood] compaqproliantml370g3	[A.26] Destructive attack	[V]	1,00E+07	1,00E+07	0.160485	0,00E+00	0.003862
[serverblood] compaqproliantml370g3	[A.25] Theft	[V]	1,00E+07	1,00E+07	0.174366	0,00E+00	0.005654
[serverblood] compaqproliantml370g3	[N.1] Fire	[I]	1,00E+07	1,00E+07	0.174366	0,00E+00	0.005654
[serverprot] questwinerserver	[E.21] Defects in software maintenance / updating	[V]	1,00E+07	1,00E+07	0.153425	0,00E+00	0.005012
[serverblood] compaqproliantml370g3	[A.26] Destructive attack	[I]	1,00E+07	1,00E+07	0.160485	0,00E+00	0.003862
[serverprot] questwinerserver	[N.2] Water	[V]	1,00E+07	1,00E+07	0.174366	0,00E+00	0.005654
[serverprot] questwinerserver	[E.20] Software vulnerabilities	[V]	1,00E+07	1,00E+07	0.163589	0,00E+00	0.006322
[serverblood] compaqproliantml370g3	[N.1] Fire	[V]	1,00E+07	1,00E+07	0.174366	0,00E+00	0.005654
[serverprot] questwinerserver	[N.1] Fire	[V]	1,00E+07	1,00E+07	0.174366	0,00E+00	0.005654
[serverblood] compaqproliantml370g3	[N.2] Water	[V]	1,00E+07	1,00E+07	0.174366	0,00E+00	0.005654

Παράρτημα Ζ: Αξιολόγηση των αντίμετρων

evaluation of safeguards

project: [nos1] nos1

10.5 Safeguards

10.5.1 Aspect

Aspect the safeguard deals with:

— M for management
— T for technical
— PHY for physical security
— PER for personnel management

10.5.2 Type of protection

— PR – prevention
— DR – deterrence
— EL – elimination
— IM – impact minimization
— CR – correction
— RC – recovery

— AD – administrative
— AW – awareness
— DC – detection
— MN – monitoring

— std – policy
— proc – procedure
— cert – certification or accreditation

Project data

nos1	nos1
library	[std] INFOSEC library (8.11.2013)

License

maturity levels

- L0 - non existent
- L1 - initial / ad hoc
- L2 - repeatable but intuitive
- L3 - defined process
- L4 - managed and measurable
- L5 - optimised

Security domains

- [base] Base

Project phases

- [current] current situation
- [target] target situation

Security domain: [base] Base

[H] General Protections

safeguard	**A**	**R**	**[current]**	**[target]**
[H.IA] Identification and authentication	M	8	L2	L4
[H.IA.1] There is a policy on identification and authentication	M	3	L2	L4
[H.IA.2] There are procedures for identification and authentication tasks	M	3	L2	L4
[H.IA.3] User identification	M	5	L2	L4
[H.IA.4] Management of user identification and authentication	M	5	L2	L4

[H.IA.4.1] There is a registry of users with their ID	M	2	L2	L4
[H.IA.4.2] Creation, activation, modification and disposal of user accounts	M	5	L2	L4
[H.IA.4.3] User identity and the required privileges are verified before giving the authenticator	M	4	L2	L4
[H.IA.4.4] Limit to the number of authenticators required per user	M	3	L2	L4
[H.IA.4.5] Secure distribution of authenticators	M	3	L2	L4
[H.IA.4.6] Written commitment to maintain authenticator confidentiality	M	2	L2	L4
[H.IA.4.7] Confirmation of authenticator reception by the interested parties	M	2	L2	L4
[H.IA.4.8] Authenticator control by the interested parties	M	2	L2	L4
[H.IA.4.9] Communication of incidents which affect authenticators (loss, infringement, etc.)	M	2	L2	L4
[H.IA.4.a] Accounts are suspended if they are revealed to third parties or are suspected of having been revealed to third parties	M	5	L2	L4
[H.IA.5] Special accounts (administration)	M	5	L2	L4
[H.IA.6] Trusted authentication path	T	6	L2	L4
[H.IA.7] {xor} Required authentication factors:	M	8	L2	L4
[H.IA.7.1] Something you have - physical token (e.g. card)	M	6 (u)	L2	L4
[H.IA.7.2] Something you know (e.g. password)	M	8 (u)		
[H.IA.7.3] Software certificates (public-key cryptography)	M	8		
[H.IA.7.4] Something you are - biometrics (e.g. fingerprint)	M	8		
[H.IA.7.5] 2 factors: token + password	M	8		
[H.IA.7.6] 2 factors: token + certificates	M	8		
[H.IA.7.7] 2 factors: one-time password (OTP) + token	M	8		
[H.IA.7.8] 2 factors: one-time password (OTP) over separate channel	M	8		
[H.IA.7.9] 2 factors: biometrics + password	M	8		
[H.IA.7.a] 3 factors: biometrics + token + password	M	8 (o)		
[H.AC] Logical access control	T	6	L2	L4
[H.AC.1] There is a policy on access control	T	3	L2	L4
[H.AC.2] There are procedures for access control tasks	T	3	L2	L4
[H.AC.3] Access authorizations are defined and documented	M	3	L2	L4
[H.AC.4] Restricted access to information	T	5	L2	L4
[H.AC.5] Restriction of use of system utilities	T	4	L2	L4
[H.AC.6] Access to system settings is restricted	T		L2	L4
[H.AC.8] Control of work outside the regular schedule (authorisation and monitoring)	T	4	L2	L4
[H.AC.9] Privilege management	T	5	L2	L4
[H.AC.a] Review of user access rights	T	4	L2	L4
[H.AC.b] {xor} Access control model	T	6	L2	L4
[H.AC.c] Logon on terminals	T	6	L2	L4
[H.AC.d] Connection time is limited	T	4	L2	L4
[H.AC.e] There is a limit on the number of concurrent sessions by one user	T	4	L2	L4
[H.AC.f] Unattended user equipment	T	6	L2	L4
[H.AC.g] Automatic terminal disconnection	T	6	L2	L4
[H.tools] Security tools	T	8	L2	L4
[H.tools.AV] Tool against harmful code (malware)	T	8	L2	L4
[H.tools.IDS] IDS/IPS: Intrusion detection / prevention tool	T	7	L2	L4
[H.tools.CC] Configuration scanning tool	T		L2	L4
[H.tools.TM] Traffic monitoring tool	T	5	L2	L4
[H.tools.DLP] DLP: Data Loss Prevention tool	T	5	L2	L4
[H.tools.HP] Honey net / honey pot	T	4	L2	L4
[H.tools.SFV] Security functions verification	T	6	L2	L4
[H.VM] Vulnerability management	M	6	L2	L4

[H.VM.1] There are people dedicated to vulnerability management	M	3	L2	L4
[H.VM.2] Mechanisms are planned to be informed of vulnerabilities ...	M	4	L2	L4
[H.tools.VA] Vulnerability analysis tool	T	6	L2	L4
[H.VM.4] The potential impact is analysed (risk assessment)	M	3	L2	L4
[H.VM.5] Penetration testing	M	4	L2	L4
[H.VM.6] There are procedures for reaction	M	3	L2	L4
[H.VM.7] Repairing detected vulnerabilities	M	5	L2	L4
[H.AU] Logging and audit	T	6	L2	L4
[H.AU.1] Administration	T	4	L2	L4
[H.AU.2] Tools	T	6	L2	L4
[H.AU.3] Information	T	5	L2	L4
[H.AU.4] Activities	T	4	L2	L4

[D] Protection of Data / Information

safeguard	**A**	**R**	**[current]**	**[target]**
[800-53:sec_attr] Security attributes	M	6	L2	L4
[800-53:AC16] The information system supports and maintains the binding of security attributes to information in storage, in process, and in transmission	M	6	L2	L4
[800-53:SC16] The information system associates security attributes with information exchanged between information systems	M	6	L2	L4
[D.2] There is an inventory of information assets	M	3	L2	L4
[D.3] Regulations	M	4	L2	L4
[D.3.1] Information is classified	M	4	L2	L4
[D.3.2] Security attributes	M	3	L2	L4
[D.3.3] IPR: intellectual property rights for information are protected	M	2	L2	L4
[D.3.4] There is a policy on retention of data	M		L2	L4
[D.I] Integrity guarantees	M	5	L2	L4
[D.5] Confidentiality protection	M	5	L2	L4
[D.C] Encryption of information	M	5	L2	L4
[D.C.1] There is a policy for the use of cryptographic controls	M	2	L2	L4
[D.C.2] There are procedures for information encryption	M	2	L2	L4
[D.C.3] Persons are assigned to responsibilities	M	2	L2	L4
[D.C.4] Encryption mechanism	T	5	L2	L4
[D.5.2] Cleaning of released documents	M	4	L2	L4
[D.5.3] Marking of information	M	5	L2	L4
[D.backup] Backup copies of the data	M	8	L2	L4
[D.backup.1] Protection of the information	M		L2	L4
[D.backup.1.1] Backups are protected in accordance with the information they contain	M		L2	L4
[D.backup.1.2] Backups are encrypted	M		L2	L4
[D.backup.1.3] Prior authorisation is required to access to backup copies	M		L2	L4
[D.backup.2] Protection of the availability of the information	M	8	L2	L4
[D.backup.2.1] There is a policy for backups	M	5	L2	L4
[D.backup.2.2] There are procedures for preparing backup copies, their protection and conservation	M	5	L2	L4
[D.backup.2.3] Management of backup copies	M	8	L2	L4
[D.backup.2.3.1] Making copies of information consistent with their availability requirements	M	6	L2	L4
[D.backup.2.3.2] Making copies of decryption keys	M	5	L2	L4
[D.backup.2.3.3] Making copies of the signature verification information	M	5	L2	L4
[D.backup.2.3.4] Backups, and backup procedures, are saved in separate locations so that the original data and the copies shall not be affected by the same incident	M	8	L2	L4
[D.backup.2.3.5] Backup copies are regularly tested	M	5	L2	L4
[D.backup.2.3.6] Restore procedures are regularly tested	M	6	L2	L4
[D.backup.2.4] {xor} Backup mechanism	T	7	L2	L4

[D.DS] Usage of electronic signatures	T	6	L2	L4
[D.DS.1] There is a policy on electronic signatures	T	2	L2	L4
[D.DS.2] There are procedures for the usage of electronic signatures	T	2	L2	L4
[D.DS.3] Persons are assigned to responsibilities	T	2	L2	L4
[D.DS.4] The probative value of the signature is guaranteed	T	3	L2	L4
[D.DS.5] {xor} Electronic certificate	T	5	L2	L4
[D.DS.6] {xor} Algorithm implementation	T	5	L2	L4
[D.DS.7] {xor} Digital signature mechanism	T	6	L2	L4
[D.DS.8] Algorithm vulnerabilities are regularly reviewed	T	3	L2	L4
[D.DS.9] Certified / accredited algorithms are used	T	4	L2	L4
[D.DS.a] Certified products or services are used	T	5	L2	L4
[D.TS] Usage of time stamping services	M	5	L2	L4
[D.TS.1] There is a policy on time stamping	M	3	L2	L4
[D.TS.2] Time stamping procedures	M	2	L2	L4
[D.TS.3] Persons are assigned to responsibilities	M	2	L2	L4
[D.TS.4] The probative value of the time-stamp is guaranteed	M	3	L2	L4
[D.TS.5] Time stamps are regularly renewed	M	5	L2	L4
[D.TS.6] {xor} Electronic time stamping mechanism	T	5	L2	L4
[D.TS.7] Algorithm vulnerabilities are regularly reviewed	M	3	L2	L4
[D.TS.8] Certified products or services are used	T	3	L2	L4

[K] Cryptographic keys management

safeguard	**A**	**R**	**[current]**	**[target]**
[K.IC] Management of information encryption keys	M		L2	L4
[K.IC.1] There is a policy on key management	M		L2	L4
[K.IC.2] There are procedures for key management	M		L2	L4
[K.IC.3] For each key, the responsible persons are identified	M		L2	L4
[K.IC.4] Operation	M		L2	L4
[K.IC.5] {xor} Key generation	T		L2	L4
[K.IC.6] {xor} Key distribution	T		L2	L4
[K.IC.7] {xor} Key storage	T		L2	L4
[K.IC.8] Key deletion	T		L2	L4
[K.IC.9] Copies of keys are retained	M		L2	L4
[K.DS] Management of information signing keys	M		L2	L4
[K.DS.1] There is a policy on key management	M		L2	L4
[K.DS.2] There are procedures for key management	M		L2	L4
[K.DS.3] For each key, the responsible persons are identified	M		L2	L4
[K.DS.4] Operation	M		L2	L4
[K.DS.5] {xor} Key generation	T		L2	L4
[K.DS.6] {xor} Key distribution	T		L2	L4
[K.DS.7] {xor} Key storage	T		L2	L4
[K.DS.8] Key deletion	T		L2	L4
[K.DS.9] Copies of keys are retained	M		L2	L4
[K.disk] Management of keys for cryptographic containers (virtual disks)	M		L2	L4
[K.disk.1] There is a policy on key management	M		L2	L4
[K.disk.2] There are procedures for key management	M		L2	L4
[K.disk.3] For each key, the responsible persons are identified	M		L2	L4
[K.disk.4] Operation	M		L2	L4
[K.disk.5] The keys are generated in an area separated of operation	M		L2	L4
[K.disk.6] {xor} Key generation	T		L2	L4
[K.disk.7] {xor} Key distribution	T		L2	L4
[K.disk.8] {xor} Key storage	T		L2	L4
[K.disk.9] Key deletion	T		L2	L4
[K.disk.a] Copies of keys are retained	M		L2	L4
[K.comms] Management of communications keys	M		L2	L4

[K.comms.1] There is a policy on key management	M		L2	L4
[K.comms.2] There are procedures for key management	M		L2	L4
[K.comms.3] For each key, the responsible persons are identified	M		L2	L4
[K.comms.4] Operation	M		L2	L4
[K.comms.5] The keys are generated in an area separated of operation	M		L2	L4
[K.comms.6] {xor} Key generation	T		L2	L4
[K.comms.7] {xor} Key distribution	T		L2	L4
[K.comms.8] {xor} Key storage	T		L2	L4
[K.comms.9] Key deletion	T		L2	L4
[K.comms.a] Copies of keys are retained	M		L2	L4
[K.509] Certificate management	T		L2	L4
[K.509.1] There is a policy on the use of certificates	T		L2	L4
[K.509.2] There are procedures for using certificates	T		L2	L4
[K.509.3] Certificates are revoked when compromised, or there is suspicion of it	T		L2	L4
[K.509.4] Certificates have a limited validity period and are regularly renewed	T		L2	L4
[K.509.5] Certificates are retained for accountability	T		L2	L4

[S] Protection of Services

safeguard	**A**	**R**	**[current]**	**[target]**
[S.1] Service usage	M	5	L3	L4
[S.1.1] Usage of e-mail	M	4	L3	L4
[S.1.1.1] There is a policy on use	M	3	L3	L4
[S.1.1.2] Deploy mechanism to detect unacceptable usage	T	4	L3	L4
[S.1.1.3] Regular verification that policy is applied	M	4	L3	L4
[S.1.1.4] Train users on service usage	M	3	L3	L4
[S.1.1.5] Define procedures for policy violation	M	3	L3	L4
[S.1.1.6] Define disciplinary procedures for policy violation	M	3	L3	L4
[S.1.1.7] Protection of information	M	4	L3	L4
[S.1.1.8] Measures against spam reception	M	4	L3	L4
[S.1.1.9] Measures against malware in e-mail clients	M	4	L3	L4
[S.1.1.a] Software	T	4	L3	L4
[COM.Internet] Web browsing	M	5	L3	L4
[COM.Internet.1] There is a policy on use	M	3	L3	L4
[COM.Internet.3] Content control tool with up-to-date filters	T	5	L3	L4
[COM.Internet.7] Execution of mobile code (e.g. applets) is controlled	T	4	L3	L4
[S.TW] Tele-working	M	4	L3	L4
[S.TW.1] There is a person responsible for service management	M	2	L3	L4
[S.TW.2] There is a policy of use	M	3	L3	L4
[S.TW.3] Users are trained on service usage	M	2	L3	L4
[S.TW.4] Unacceptable use is detected	T	3	L3	L4
[S.TW.5] Policy compliance is regularly verified	M	4	L3	L4
[S.TW.6] There are procedures to manage tele-working	M	3	L3	L4
[S.TW.7] Disciplinary measures are applied in case of non-compliance	M	2	L3	L4
[S.TW.8] Prior authorisation is required	M	2	L3	L4
[S.TW.9] Study of specific site characteristics	M	4	L3	L4
[S.voip] Voice over IP	T		L3	L4
[S.voip.1] Prior authorisation is required for using VoIP	T		L3	L4
[S.voip.2] VoIP usage monitoring	T		L3	L4
[S.voip.3] Separation of LAN voice and data networks (VLAN)	T		L3	L4
[S.voip.4] Authentication among devices	T		L3	L4
[S.voip.5] Cryptographic protection	T		L3	L4
[S.voip.5.1] There is a policy for the use of cryptographic controls	T		L3	L4
[S.voip.5.2] Persons are assigned to responsibilities	T		L3	L4

[S.voip.5.3] {xor} Encryption mechanism	T		L3	L4
[S.voip.5.4] Algorithm vulnerabilities are regularly reviewed	T		L3	L4
[S.voip.5.5] Certified / accredited algorithms are used	T		L3	L4
[S.2] Provision of services	M		L3	L4
[S.2.1] There is a policy establishing the acceptable use of services	M		L3	L4
[S.2.2] There is an inventory of services	M		L3	L4
[S.cont] Availability assurance	M		L3	L4
[S.cont.1] DoS protection	M		L3	L4
[S.cont.2] Resource management	M		L3	L4
[S.SC] Security profiles are applied	T		L3	L4
[S.op] Exploitation	M		L3	L4
[S.op.1] Plan for regular vulnerability scanning	M		L3	L4
[S.op.2] Install intrusion alarms	M		L3	L4
[S.op.3] Non-repudiation	T		L3	L4
[S.op.4] Training of staff in service configuration	M		L3	L4
[S.CM] Change management (upgrades and replacements)	M		L3	L4
[S.CM.1] There is a policy on change control	M		L3	L4
[S.CM.2] Responsible persons are appointed	M		L3	L4
[S.CM.3] There are procedures to apply changes	M		L3	L4
[S.CM.4] Regular monitoring (external services)	M		L3	L4
[S.CM.5] Evaluation of potential impact of change	M		L3	L4
[S.CM.6] The rule of ‘minimum functionality’ is maintained at all times	M		L3	L4
[S.CM.7] The rule of ‘secure by default’ is maintained at all times	M		L3	L4
[S.CM.8] It is verified that the change does not disable the mechanisms for detection, monitoring and logging	M		L3	L4
[S.CM.9] Change process is designed to minimise service interruption	M		L3	L4
[S.CM.a] Performed by authorised personnel	M		L3	L4
[S.CM.b] Regression testing is carried out	T		L3	L4
[S.CM.c] Service updates are logged	M		L3	L4
[S.CM.d] Documentation	M		L3	L4
[S.CM.e] All related operating procedures are updated	M		L3	L4
[S.CM.f] All affected recovery procedures are updated	M		L3	L4
[S.end] Termination	M		L3	L4
[S.www] Protecting Web services and applications	M		L3	L4
[S.www.2] Electronic publishing of information (www)	M		L3	L4
[S.www.4] Protection of the configuration	M		L3	L4
[S.email] Protection of electronic mail	M		L3	L4
[S.email.1] There is a person responsible for service administration	M		L3	L4
[S.email.2] Service usage is logged	M		L3	L4
[S.email.3] Protection of the configuration	M		L3	L4
[S.email.4] Anti-spam controls	T		L3	L4
[S.email.5] Deploy controls against malware in the server	T		L3	L4
[S.email.6] Non-repudiation services	M		L3	L4
[S.email.7] {xor} Guarantee service availability according to policy	M		L3	L4
[S.2.a] Electronic commerce security	M		L3	L4
[S.2.a.1] Requirements are taken into account	T		L3	L4
[S.2.a.2] Drafting and approval of a document which states the terms agreed by the parties	T		L3	L4
[S.2.a.3] Controls for process development (price fixing, contracting, etc.)	T		L3	L4
[S.2.a.4] Implementation of authentication mechanisms for the parties	T		L3	L4
[S.2.a.5] Establishment of authorisation mechanisms in the process	T		L3	L4
[S.2.a.6] Activities are logged	T		L3	L4
[S.2.b] Protection of Electronic Data Interchange (EDI)	M		L3	L4
[S.2.b.4] Software	T		L3	L4
[S.dir] Directory protection	T		L3	L4

[S.dir.4] Integrity of stored data	T		L3	L4
[S.dns] DNS protection	T		L3	L4
[S.dns.5] Response authentication	T		L3	L4
[S.dns.6] Response integrity guarantee	T		L3	L4
[S.dns.7] Software	T		L3	L4
[S.dns.8] Architecture	T		L3	L4
[S.dns.8.1] Public server is in the DMZ	T		L3	L4
[S.dns.8.2] Internal server isolated from outside	T		L3	L4
[S.dns.8.3] Internal server does not respond to external queries	T		L3	L4
[S.dns.8.4] {xor} Guarantee service according to policy	T		L3	L4
[S.2.e] Public key infrastructure	T		L3	L4
[S.3] Services provided by third parties	M		L3	L4
[S.3.1] Overview	M		L3	L4
[S.3.1.1] There is an inventory of subcontracted services	M		L3	L4
[S.3.1.2] External services require previous authorisation	M		L3	L4
[S.3.1.3] Identification of the sensitive or critical applications which the Organisation should maintain	M		L3	L4
[S.3.1.4] Risk identification	M		L3	L4
[S.3.2] Service provision contracts	M		L3	L4
[S.3.2.1] Policy on information security	M		L3	L4
[S.3.2.2] The obligations corresponding to the parties in the agreements	M		L3	L4
[S.3.2.3] Inclusion of the security requirements in contracts	M		L3	L4
[S.3.2.4] Definition and inclusion in the contract of the process to assess the fulfilment of the security measures	M		L3	L4
[S.3.2.5] Intellectual property rights, copy protection and protection in collaborative tasks	M		L3	L4
[S.3.2.6] Personal data protection	M		L3	L4
[S.3.2.7] Involvement of third parties (subcontractors)	M		L3	L4
[S.3.2.8] Description of each available service	M		L3	L4
[S.3.2.9] Responsibilities regarding HW and SW installation and maintenance	M		L3	L4
[S.3.2.a] Assignation of responsibilities in the supervision of the fulfilment of the contract	M		L3	L4
[S.3.3] Operation	M		L3	L4
[S.3.4] Change management control	M		L3	L4
[S.3.5] Server authentication	T		L3	L4
[S.3.5.1] Server is authenticated before transferring any information	T		L3	L4
[S.3.5.2] {xor} Authentication mechanism	T		L3	L4
[S.3.5.2.1] Shared secret	T		L3	L4
[S.3.5.2.2] Cryptography: digital signature	T			
[S.3.5.3] Authentication data and software are protected	T		L3	L4
[S.3.5.3.1] {xor} Mechanism implementation	T		L3	L4
[S.3.5.3.1.1] uses a software application	T		L3	L4
[S.3.5.3.1.2] hardware token	T			
[S.3.5.3.2] Usage is password-protected	T		L3	L4
[S.3.5.3.3] The mechanism is disabled when compromised, or there is suspicion of it	T		L3	L4
[S.3.5.3.4] Certified or accredited products are used	T		L3	L4
[S.3.5.4] Measures are taken to prevent the hijacking of established sessions	T		L3	L4
[S.3.6] Continuity of operations	M		L3	L4
[S.3.7] Termination	M		L3	L4
[S.3.7.1] Prior authorisation is required	M		L3	L4
[S.3.7.2] Business impact is assessed in advance	M		L3	L4
[S.3.7.3] Planned to minimise service interruption	M		L3	L4
[S.3.7.4] Information is removed from the provider	M		L3	L4
[S.3.7.5] Service is deactivated by authorised personnel	M		L3	L4

[S.3.7.6] All related operating procedures are updated	M		L3	L4
[S.3.7.7] All affected recovery procedures are updated	M		L3	L4

[SW] Protection of Software

safeguard	**A**	**R**	**[current]**	**[target]**
[SW.1] There is an inventory of software	M	3	L2	L4
[SW.2] There is a policy on the use of applications	M	2	L2	L4
[SW.3] Procedures for the usage of software applications	M	2	L2	L4
[SW.4] Protection of intellectual property rights (IPR)	M	3	L2	L4
[SW.backup] Backup copies (SW)	M	5	L2	L4
[SW.start] Deployment	M	3	L2	L4
[SW.SC] Security profiles are applied	T	7	L2	L4
[SW.op] Exploitation	M	5	L2	L4
[SW.op.1] There is a policy controlling operating software	M	2	L2	L4
[SW.op.2] Production systems have no development tool	M	4	L2	L4
[SW.op.3] {xor} The integrity of executable code is controlled	M	4	L2	L4
[SW.op.4] The system uses different technology components to avoid single points of technological failure	T	4	L2	L4
[SW.op.5] Isolation of sensitive systems	M	3	L2	L4
[SW.op.6] Security of applications	M	4	L2	L4
[SW.op.7] Application data files security	T	5	L2	L4
[SW.op.8] Security of configuration files	T		L2	L4
[SW.op.9] Security of system files	T	5	L2	L4
[SW.op.a] Mobile code execution (e.g. applets) is controlled	T	3	L2	L4
[SW.op.b] Collaborative computing (e.g. conferencing)	T	3	L2	L4
[SW.op.c] Inter-process communications security	T	5	L2	L4
[SW.op.d] Procedure for detection of vulnerabilities and response	M	3	L2	L4
[SW.op.e] Staff training on application configuration	M	2	L2	L4
[SW.CM] Changes (updates & maintenance)	M	4	L2	L4
[SW.CM.1] There is a policy on change control	M	2	L2	L4
[SW.CM.2] There are procedures to apply changes	M	2	L2	L4
[SW.CM.3] Permanent tracking of updates and patches (SW)	M	3	L2	L4
[SW.CM.4] Evaluation of the potential impact of change	M	3	L2	L4
[SW.CM.5] Actions addressing high risks are prioritized	M	4	L2	L4
[SW.CM.6] The rule of ‘minimum functionality’ is maintained at all times	M	3	L2	L4
[SW.CM.7] The rule of ‘secure by default’ is maintained at all times	M	3	L2	L4
[SW.CM.8] It is verified that the change does not disable the mechanisms for detection, monitoring and logging	M	3	L2	L4
[SW.CM.9] Change process is designed to minimise service interruption	M	2	L2	L4
[SW.CM.a] Version control for every software update	M	3	L2	L4
[SW.CM.b] Performed by authorised personnel	M	3	L2	L4
[SW.CM.c] Copies of previous versions of software are retained as precautionary measure for contingencies	M	4	L2	L4
[SW.CM.d] A copy of previous configuration is retained	T	3	L2	L4
[SW.CM.e] It is previously tested in an environment that is not in production	T	3	L2	L4
[SW.CM.f] Regression testing is carried out	T	3	L2	L4
[SW.CM.g] SW updates are logged	M		L2	L4
[SW.CM.h] Documentation	M	2	L2	L4
[SW.CM.i] All related operating procedures are updated	M	3	L2	L4
[SW.CM.j] All affected recovery procedures are updated	M	2	L2	L4
[SW.end] Termination	M	3	L2	L4

[HW] Protection of Hardware

safeguard	A	R	[current]	[target]
[HW.1] There is an inventory of hardware	M	2	L2	L4
[HW.2] There is a policy on the right usage of equipment	M	2	L2	L4
[HW.3] Procedures for the usage of equipment	M	2	L2	L4
[HW.start] Move to production	M	4	L2	L4
[HW.SC] Security profiles are applied	T	7	L2	L4
[HW.cont] Availability guarantees	M	6	L2	L4
[HW.cont.1] The system is generously dimensioned and the acquisition of spare parts is planned	M	6	L2	L4
[HW.cont.2] Periodic maintenance follows manufacturer's specifications	M	4	L2	L4
[HW.cont.3] Maintenance only by authorised personnel	M	4	L2	L4
[HW.cont.4] Regularly run diagnostic routines	M	2	L2	L4
[HW.cont.5] Failures and incidents are monitored	M	2	L2	L4
[HW.cont.6] Faults, real or suspected, are logged along with the preventive and corrective maintenance	M	2	L2	L4
[HW.cont.7] Backup copies of configuration information	M	5	L2	L4
[HW.cont.8] Backups are made of the decryption keys	M	3	L2	L4
[HW.cont.9] {xor} Substitute options	M	3	L2	L4
[HW.cont.9.1] Alternative equipment	M	3	L2	L4
[HW.cont.9.2] Alternative preconfigured equipment with synchronous or asynchronous disk replication	M	3		
[HW.cont.9.3] Redundant system in alternative site	M	3		
[HW.cont.9.4] Service contract with system provider takes business requirements into account	M	3		
[HW.cont.a] {xor} High availability	M	4	L2	L4
[HW.cont.b] Backup means are subject to the same degree of protection than the usual ones	M	2	L2	L4
[HW.cont.c] There is a maximum time established for backup means to take over control	M	2	L2	L4
[HW.7] Cryptographic containers (HW, virtual HW)	M	6	L2	L4
[HW.9] Installation	M	3	L2	L4
[HW.op] Operation	M	4	L2	L4
[HW.op.1] Authorisation process for information processing resources	M	2	L2	L4
[HW.op.2] The system uses different technology components to avoid single points of technological failure	T	4	L2	L4
[HW.op.3] Physical protection of equipment	PHY	4	L2	L4
[HW.op.4] Office equipment security	M	3	L2	L4
[HW.op.5] Protection of equipment off-site	PHY	4	L2	L4
[HW.op.6] Protection of network devices	M		L2	L4
[HW.op.7] Cryptographic devices	T		L2	L4
[HW.CM] Changes (updates and maintenance)	M	4	L2	L4
[HW.CM.1] There is a policy on change control	M	2	L2	L4
[HW.CM.2] There are procedures to apply changes	M	2	L2	L4
[HW.CM.3] The recommendations of the manufacturer or supplier are followed	M	3	L2	L4
[HW.CM.4] Regular tracking of updates (HW)	M	3	L2	L4
[HW.CM.5] Evaluation of change impact	M	3	L2	L4
[HW.CM.6] Actions addressing high risks are prioritized	M	4	L2	L4
[HW.CM.7] The rule of 'minimum functionality' is maintained at all times	M	3	L2	L4
[HW.CM.8] The rule of 'secure by default' is maintained at all times	M	3	L2	L4
[HW.CM.9] It is verified that the change does not disable the mechanisms for detection, monitoring and logging	M	3	L2	L4
[HW.CM.a] Change process is designed to minimise service interruption	M	2	L2	L4

[HW.CM.b] Performed by authorised personnel	M	3	L2	L4
[HW.CM.c] A copy of previous configuration is retained	T	3	L2	L4
[HW.CM.d] It is previously tested in an environment that is not in production	T	3	L2	L4
[HW.CM.e] Regression testing is carried out	T	3	L2	L4
[HW.CM.f] Every change is logged	M	2	L2	L4
[HW.CM.g] Documentation	M	2	L2	L4
[HW.CM.h] HW change is subject to version control	M	2	L2	L4
[HW.CM.i] All related operating procedures are updated	M	3	L2	L4
[HW.CM.j] All affected recovery procedures are updated	M	2	L2	L4
[HW.end] Termination	M	3	L2	L4
[HW.PCD] Mobile computers	M		L2	L4
[HW.PCD.1] There is an inventory of mobile equipment, identifying the person responsible for each one	M		L2	L4
[HW.PCD.2] Prior authorisation is required	M		L2	L4
[HW.PCD.3] All equipment is marked with the maximum level of information that can be stored or processed	M		L2	L4
[HW.PCD.4] Potential risks have been analysed	M		L2	L4
[HW.PCD.5] Security measures are identified	M		L2	L4
[HW.PCD.6] Training and awareness on risks	M		L2	L4
[HW.PCD.7] Follows a training plan on the appropriate measures	M		L2	L4
[HW.PCD.8] Applicable controls	M		L2	L4
[HW.PCD.8.1] Security measures are identified for the physical protection of the device	M		L2	L4
[HW.PCD.8.2] Violation detectors are installed	M		L2	L4
[HW.PCD.8.3] Access control requirements are established	M		L2	L4
[HW.PCD.8.4] A perimeter defence system is used (e.g. firewall)	M		L2	L4
[HW.PCD.8.5] Encryption requirements are established	M		L2	L4
[HW.PCD.8.6] Backup requirements are established	M		L2	L4
[HW.PCD.8.7] Antivirus software	M		L2	L4
[HW.PCD.9] User guides	M		L2	L4
[HW.PCD.a] Incident management in mobile computing	M		L2	L4
[HW.e] Virtual machines	M		L2	L4
[HW.e.1] To create new virtual machines	M		L2	L4
[HW.e.1.1] prior authorisation is required	M		L2	L4
[HW.e.1.2] a specific privilege is required	M		L2	L4
[HW.e.2] Host classification is the highest of its virtual machines	M		L2	L4
[HW.e.3] Virtual equipment is managed as real equipment	M		L2	L4
[HW.e.3.1] Task segregation is maintained between users and administrators	M		L2	L4
[HW.e.3.2] Security configuration	M		L2	L4
[HW.e.3.3] Security tools	M		L2	L4
[HW.e.3.4] Security patches	M		L2	L4
[HW.e.3.5] Software maintenance	M		L2	L4
[HW.e.4] Software-based virtual networks between virtual machines, are managed as real networks	M		L2	L4
[HW.e.4.1] A specific privilege is required to establish them	M		L2	L4
[HW.e.4.2] Security configuration	M		L2	L4
[HW.e.4.3] Security tools	M		L2	L4
[HW.e.5] It is taken into account the impact on the system as a whole of a denial-of-service attack on virtual equipments	M		L2	L4
[HW.e.6] It is taken into account the impact on the resilience of the system as a whole as a consequence of attacks on virtual equipments	M		L2	L4
[HW.e.7] The hypervisor is properly secured	M		L2	L4
[HW.e.7.1] Access to hypervisor is controlled	M		L2	L4
[HW.e.7.2] Access to shared resources is controlled	M		L2	L4
[HW.e.8] Access to virtual images is controlled	M		L2	L4

[HW.e.9] Backups of virtual machine images are protected	M		L2	L4
[HW.e.a] Virtual servers and clients are not installed on the same host	M		L2	L4
[HW.e.b] Do not install on the same host computer, servers that require different levels of security	M		L2	L4
[HW.e.c] No physical network cards are shared between virtual machines that require different levels of security	M		L2	L4
[HW.e.d] The local area network (SAN) used as virtualization support, is isolated and only accessible by the host machine	M		L2	L4
[HW.e.e] Border and internal equipment are not installed on the same physical host (e.g. firewalls)	M		L2	L4
[HW.e.f] Termination	M		L2	L4
[HW.e.f.1] Termination is logged	M		L2	L4
[HW.e.f.2] {xor} Media holding the virtual image is subject to the mechanisms foreseen to sanitize media	M		L2	L4
[HW.pabx] PABX protection	M		L2	L4
[HW.pabx.3] Logical access is controlled	M		L2	L4
[HW.pabx.4] Restricted maintenance accounts	M		L2	L4
[HW.h] Voice, facsimile and video	M	3	L2	L4
[HW.h.1] Ban on confidential conversations in public places or without appropriate protection measures	M	3	L2	L4

[COM] Protection of Communications

safeguard	A	R	[current]	[target]
[COM.1] There is an inventory of communication services	M	2	L2	L4
[COM.2] There is a policy on the right usage of communications	M	3	L2	L4
[COM.3] There are procedures for the usage of communications	M	3	L2	L4
[COM.start] Acceptance of new services	M	4	L2	L4
[COM.SC] Security profiles are applied	T	8	L2	L4
[COM.cont] Availability guarantees	M	6	L2	L4
[COM.cont.1] Single points of failure (SPF) are identified and avoided	M	6	L2	L4
[COM.cont.2] The system is generously dimensioned and the acquisition of spare parts is planned	M	4	L2	L4
[COM.cont.3] Periodic maintenance follows manufacturer's specifications	M	4	L2	L4
[COM.cont.4] Links and network devices are monitored	M	5	L2	L4
[COM.cont.5] Actual and suspected failures are logged	M		L2	L4
[COM.cont.6] Preventive and corrective maintenance actions are logged	M		L2	L4
[COM.cont.7] There are backup copies of routing information	M	4	L2	L4
[COM.cont.8] There are backup copies of authentication keys	M	4	L2	L4
[COM.cont.9] There are backup copies of decryption keys	M	4	L2	L4
[COM.cont.a] {xor} Redundancy	T	4	L2	L4
[COM.cont.b] Backup means are subject to the same degree of protection than the usual ones	M	2	L2	L4
[COM.cont.c] There is a maximum time established for backup means to take over control	M	2	L2	L4
[COM.aut] Channel authentication	T	6	L2	L4
[COM.aut.1] Prior authorisation is required	T	2	L2	L4
[COM.aut.2] User's identity is verified before receiving the authentication means	T	3	L2	L4
[COM.aut.3] Authentication of the origin of the connection	T	3	L2	L4
[COM.aut.4] {xor} Authentication mechanism	T	6	L2	L4
[COM.aut.4.1] Something you know (e.g. passwords)	T	5 (u)	L2	L4
[COM.aut.4.2] Software certificates (public-key cryptography)	T	5		
[COM.aut.4.3] 2 factors: token + password	T	6		
[COM.aut.4.4] 2 factors: token + certificates	T	6		
[COM.aut.4.5] 2 factors: one-time password (OTP) plus token	T	6		
[COM.aut.4.6] 2 factors: one-time password (OTP) over separate channel	T	6		
[COM.aut.5] Authentication channel	T	4	L2	L4
[COM.aut.6] Measures are taken to prevent the hijacking of sessions established	T	3	L2	L4
[COM.I] {xor} Protection of the integrity of the data in the channel	T	6	L2	L4
[COM.C] The confidentiality of the data is cryptographically protected in the channel	M	6	L2	L4
[COM.C.1] There is a policy for the use of cryptographic controls	M	4	L2	L4
[COM.C.2] Persons are assigned to responsibilities	M	4	L2	L4
[COM.C.3] {xor} Implementation of algorithms	T	6	L2	L4
[COM.C.4] {xor} Shared secret (symmetric encryption)	T	6	L2	L4
[COM.C.5] Algorithm vulnerabilities are regularly reviewed	M	5	L2	L4
[COM.C.6] Certified / accredited algorithms are used	T	5	L2	L4
[COM.C.7] a certified or accredited product is used	T	5	L2	L4
[COM.op] Operation	T	5	L2	L4
[COM.op.1] Network access control	T	4	L2	L4
[COM.op.1.1] There is a policy for use of network services	T	2	L2	L4
[COM.op.1.2] Prior authorisation is required for media and devices to have access to networks and services	T	2	L2	L4
[COM.op.1.3] Remote access	T	4	L2	L4

[COM.op.1.4] {xor} Protection of remote diagnosis ports	T	3	L2	L4
[COM.op.1.5] Authentication of network nodes	T	4	L2	L4
[COM.op.1.6] Routing control	T	3	L2	L4
[COM.op.2] Network services security	T	4	L2	L4
[COM.op.2.1] Monitoring of network services	T	3	L2	L4
[COM.op.2.2] Security is regularly reviewed	T	4	L2	L4
[COM.op.3] Protection is provided against traffic analysis	T	5	L2	L4
[COM.op.4] Staff is trained on communications configuration	T	3	L2	L4
[COM.CM] Changes (updates and maintenance)	M	5	L2	L4
[COM.CM.1] There is a policy on change control	M	2	L2	L4
[COM.CM.2] There are procedures to apply changes	M	2	L2	L4
[COM.CM.3] Updates are continuously monitored	M	3	L2	L4
[COM.CM.4] Change impact is evaluated	M	3	L2	L4
[COM.CM.5] Actions addressing high risks are prioritized	M	5	L2	L4
[COM.CM.6] The rule of ‘minimum functionality’ is maintained at all times	M	3	L2	L4
[COM.CM.7] The rule of ‘secure by default’ is maintained at all times	M	3	L2	L4
[COM.CM.8] It is verified that the change does not disable the mechanisms for detection, monitoring and logging	M	3	L2	L4
[COM.CM.9] Change procedures are designed to minimise service interruption	M	3	L2	L4
[COM.CM.a] Activities are performed by authorised personnel	M	4	L2	L4
[COM.CM.b] A copy of previous configuration is retained	T	3	L2	L4
[COM.CM.c] It is previously tested in an environment that is not in production	T	4	L2	L4
[COM.CM.d] Regression testing is carried out	M	4	L2	L4
[COM.CM.e] Every action is logged	M		L2	L4
[COM.CM.f] Documentation	M	2	L2	L4
[COM.CM.g] All related operating procedures are updated	M	3	L2	L4
[COM.CM.h] All affected recovery procedures are updated	M	3	L2	L4
[COM.end] Termination	M	3	L2	L4
[COM.wifi] Wireless Security (WiFi)	M		L2	L4
[COM.wifi.1] Prior authorisation is required to deploy access points (AP)	M		L2	L4
[COM.wifi.2] When access points are deployed, the signal reach is taken into account to minimize exposure to attacks	M		L2	L4
[COM.wifi.3] Prior authorisation is required for connecting clients	M		L2	L4
[COM.wifi.4] Default keys from cards and access points are removed prior to deployment	T		L2	L4
[COM.wifi.5] Unused ports and services are disabled	M		L2	L4
[COM.wifi.6] Non-essential management protocols are disabled	M		L2	L4
[COM.wifi.7] SNMP protocol restrictions on wireless networks	M		L2	L4
[COM.wifi.8] Access points are regularly verified (via broadcast or tools)	T		L2	L4
[COM.wifi.9] Ad-hoc connection mode is disabled in user devices	T		L2	L4
[COM.wifi.a] Authentication of wireless devices (MAC filtering, authentication server, etc.)	T		L2	L4
[COM.wifi.b] IP addresses are controlled	M		L2	L4
[COM.mobile] Mobile telephony	M		L2	L4
[COM.mobile.1] Confidentiality	M		L2	L4
[COM.mobile.2] Review of the detailed invoices in search of unknown telephone numbers	M		L2	L4
[COM.mobile.3] Verification that all telephone calls made are shown in the invoice	M		L2	L4
[COM.mobile.4] {xor} Ban on usage in security areas	M		L2	L4
[COM.mobile.5] Periodic terminal inspection to detect tampering	M		L2	L4
[COM.mobile.6] Ban on connection to computers which have sensitive data	M		L2	L4
[COM.mobile.7] Immediate communication of card or terminal theft	M		L2	L4
[COM.mobile.8] Terminal and card exchange among users	M		L2	L4
[COM.mobile.9] Telephone numbers are not published in telephone books	M		L2	L4
[COM.DS] Segregation of networks into domains	T	6	L2	L4

[IP] Interconnection points

safeguard	A	R	[current]	[target]
[IP.1] Administration	M	4	L2	L4
[IP.1.1] Connections require previous authorisation	M	2	L2	L4
[IP.1.2] There is an inventory of authorised connections	M	2	L2	L4
[IP.1.3] Authorised connections are regularly monitored	T	4	L2	L4
[IP.1.4] Users and processes authorized to use the interconnection only enjoy minimum essential rights	M	2	L2	L4
[IP.1.5] Authorised users and processes are regularly reviewed	M	3	L2	L4
[IP.1.6] Authorizations are regularly renewed or canceled	M	2	L2	L4
[IP.2] Establishing a connection	M	5	L2	L4
[IP.2.1] Users are identified and authenticated before connection is established	M	5	L2	L4
[IP.2.2] Processes are identified and authenticated before connection is established	M	5	L2	L4
[IP.2.3] Each server is identified and authenticated before establishing the link	M	5	L2	L4
[IP.SPP] Traffic: Data exchange	T	5	L2	L4
[IP.SPP.1] Any other node in the network is considered untrusted, and there is a local control of data exchanged	T	3	L2	L4
[IP.SPP.2] Format of exchanged data is validated	T	3	L2	L4
[IP.SPP.3] Authorized traffic	T	3	L2	L4
[IP.SPP.4] Incoming and outgoing traffic are under control	T	5	L2	L4
[IP.SPP.5] Mediation - The point of interconnection will mediate the following processes:	T	3	L2	L4
[IP.SPP.5.1] Users identification and authentication	T	3	L2	L4
[IP.SPP.5.2] Identification and authentication of the nodes	T	3	L2	L4
[IP.SPP.5.3] Access authorization	T	3	L2	L4
[IP.SPP.5.4] While lists	T	3	L2	L4
[IP.SPP.5.5] Black lists	T	3	L2	L4
[IP.SPP.5.6] Security labels of the objects exchanged	T	3	L2	L4
[IP.SPP.5.7] Network control information (level 3)	T	3	L2	L4
[IP.SPP.5.8] Application control information (level 7)	T	3	L2	L4
[IP.SPP.6] Management data traffic	T	3	L2	L4
[IP.SPP.6.1] Origin is authenticated	T	3	L2	L4
[IP.SPP.6.2] Information integrity is protected	T	3	L2	L4
[IP.SPP.6.3] Confidentiality is protected	T	3	L2	L4
[IP.SPP.7] Internet IP addresses are hidden (NAT or equivalent service)	T	2	L2	L4
[IP.SPP.8] Internet IP ports are hidden (PAT or equivalent service)	T	2	L2	L4
[IP.BS] Protection of border device(s)	M	6	L2	L4
[IP.BS.1] Product is under control	M	4	L2	L4
[IP.BS.2] Hardening	M	6	L2	L4
[IP.BS.3] The system uses different technology components to avoid single points of technological failure	T	4	L2	L4
[IP.BS.4] Administration	M	4	L2	L4
[IP.BS.5] A specific contingency plan is established	T	4	L2	L4
[IP.BS.6] Certified / accredited products are used	T	3	L2	L4
[IP.5] Virtual private networks	M	3	L2	L4
[IP.5.1] Secure configuration	M	3	L2	L4
[IP.5.1.1] unused services are eliminated	M	3	L2	L4
[IP.5.1.2] default user accounts are eliminated	M	3	L2	L4
[IP.5.1.3] unused software is eliminated	M	3	L2	L4
[IP.5.1.4] approved parameters are set	M	3	L2	L4
[IP.5.1.5] logs are enabled	M	3	L2	L4
[IP.5.1.6] configuration is reviewed regularly and when there are changes (new versions and security patches)	M	3	L2	L4
[IP.5.2] Channel authentication	M	3	L2	L4
[IP.5.2.1] passwords are not included in any automatic access setup procedure	M	3	L2	L4

[IP.5.2.2] interconnected systems (either fixed or mobile) authenticate each other	M	3	L2	L4
[IP.5.2.3] local network is authenticated using a software certificate	M	3	L2	L4
[IP.5.2.4] authentication uses approved cryptographic mechanisms and parameters	M	3	L2	L4
[IP.5.3] Channel encryption - Protection of confidentiality	M	3	L2	L4
[IP.5.3.1] approved cryptographic algorithms and parameters are used	M	3	L2	L4
[IP.5.3.2] fixed LANs use hardware cipher devices	M	3	L2	L4
[IP.5.4] Protection of the integrity of data	M	3	L2	L4
[IP.5.5] When the session that supports the flow of information through the virtual channel is closed, the user session is also closed through interconnection	M	3	L2	L4
[IP.5.6] Management traffic used to monitor and manage network devices is strongly authenticated and encrypted when it travels through public networks	M	3	L2	L4
[IP.6] When a remote equipment is connected:	M	3	L2	L4
[IP.6.1] There is a policy on ...	M	3	L2	L4
[IP.6.1.1] which networks and network services are accessible	M	3	L2	L4
[IP.6.1.2] the authorization process	M	3	L2	L4
[IP.6.1.3] security management controls	M	3	L2	L4
[IP.6.1.4] security procedures related to the interconnection	M	3	L2	L4
[IP.6.2] Software patches are revised to be up to date	M	3	L2	L4
[IP.6.3] Security configuration is verified	M	3	L2	L4

[AUX] Auxiliary Means

safeguard	A	R	[current]	[target]
[AUX.1] There is an inventory of auxiliary means	M	3	L2	L4
[AUX.cont] Availability guarantees	T		L2	L4
[AUX.cont.1] The recommendations of the manufacturer or supplier are followed	T		L2	L4
[AUX.power] Power supply	PHY	5	L2	L4
[AUX.power.1] System dimensioning takes future needs into account	PHY	3	L2	L4
[AUX.power.2] Installation in accordance with current regulations	PHY	2	L2	L4
[AUX.power.3] Protection of system power lines against fluctuations and overload	PHY	4	L2	L4
[AUX.power.4] General power switch for system located at entrance to each area	PHY	3	L2	L4
[AUX.power.5] Labelled switches, protected against accidental activation	PHY	3	L2	L4
[AUX.power.6] Backup power supply	PHY	5	L2	L4
[AUX.AC] Air conditioning	PHY		L2	L4
[AUX.wires] Protection of wiring	PHY	6	L2	L4
[AUX.7] Prevention against theft	M		L2	L4

[L] Protection of the installations

safeguard	A	R	[current]	[target]
[L.1] There are security policies	PHY	2	L2	L4
[L.2] There is an inventory of locations	PHY	5	L2	L4
[L.3] Moving into operation	PHY	5	L2	L4
[L.3.2] Prior authorisation is required	PHY	2	L2	L4
[L.3.5] Protection plan	PHY	4	L2	L4
[L.3.5.1] Fitting out plan	PHY	3	L2	L4
[L.3.5.2] Security plan	PHY	3	L2	L4
[L.3.5.3] Emergency plan	PHY	4	L2	L4
[L.3.5.3.1] Evacuation plan	PHY	3	L2	L4
[L.3.5.3.2] Communication plan	PHY	3	L2	L4
[L.3.5.3.3] Physical access to facilities in case of emergency	PHY	4	L2	L4
[L.3.5.3.4] There is an emergency plan to deal with violence	PHY	3	L2	L4
[L.design] Design	PHY	5	L2	L4
[L.design.1] Areas are designed in accordance with relevant health and safety rules and regulations	PHY	3	L2	L4
[L.design.2] Soundproofing of sensitive areas	PHY	5	L2	L4

[L.design.3] Separation of areas where dangerous activities are carried out (refuse areas, fuel stores, etc.)	PHY	5	L2	L4
[L.design.4] warehouses	PHY	3	L2	L4
[L.design.4.1] the stores are always manned when open	PHY	3	L2	L4
[L.design.5] ventilation	PHY	3	L2	L4
[L.design.5.1] There are filters on HVAC ducts	PHY	3	L2	L4
[L.design.5.2] There are anthrax detectors and filters	PHY	3	L2	L4
[L.design.5.3] There are detectors of dangerous chemicals	PHY	3	L2	L4
[L.5] Protection against disasters	PHY	7	L2	L4
[L.5.1] Emergency lighting covers all areas required to guarantee continuity of critical missions	PHY	5	L2	L4
[L.5.2] Protection against fire	PHY	7	L2	L4
[L.5.3] Protection against flood	PHY	7	L2	L4
[L.5.4] Protection against natural and environmental disasters	PHY	5	L2	L4
[L.5.5] Protection against environmental contamination	PHY	5	L2	L4
[L.5.6] Protection against electromagnetic contamination	T	5	L2	L4
[L.5.7] Protection against explosives	PHY	5	L2	L4
[L.5.8] Waste disposal	PHY	4	L2	L4
[L.5.8.1] The site has a program of recovery and recycling of waste	PHY	4	L2	L4
[L.5.8.2] Rubbish bins can be closed at night	PHY	4	L2	L4
[L.5.9] Insurance	PHY	4	L2	L4
[L.cont] Continuity of operations	PHY	5	L2	L4
[L.cont.1] The implications for business continuity are analysed	PHY	4	L2	L4
[L.cont.2] A protocol is in place for contingency	PHY	4	L2	L4
[L.cont.3] Alternative facilities are prepared	PHY	5	L2	L4
[L.cont.4] Alternative facilities are subject to the same degree of protection than the usual ones	PHY	4	L2	L4
[L.cont.5] The site has a plan to deal with any sudden or unannounced strikes	PHY	5	L2	L4

[PPS] Perimeter protection

safeguard	**A**	**R**	**[current]**	**[target]**
[PPS.2] Design	PHY	5	L2	L4
[PPS.2.2] Minimum number of entrances	PHY	4	L2	L4
[PPS.2.4] Security and public access areas to be separated	PHY	4	L2	L4
[PPS.2.5] Sensitive equipment is in isolated areas	PHY	3	L2	L4
[PPS.2.6] Separation of areas managed by others	PHY	3	L2	L4
[PPS.2.8] Separate access for persons and vehicles	PHY	3	L2	L4
[PPS.2.9] Loading / unloading	PHY	5	L2	L4
[PPS.5] External barriers	PHY		L2	L4
[PPS.5.1] Clearly delimited perimeter with a fence, wall or similar	PHY		L2	L4
[PPS.5.2] The perimeter of the settlement has signs indicating the boundaries of private property	PHY		L2	L4
[PPS.5.3] Fence is continuous even where the terrain is not leveled	PHY		L2	L4
[PPS.5.4] Protection to prevent unauthorized access by exploiting rivers, lakes, trees, buildings and other structures or terrain features	PHY		L2	L4
[PPS.5.5] Free area of at least 3 meters all around the perimeter on both sides of the fence	PHY		L2	L4
[PPS.5.6] It is prevented from entering through the roof	PHY		L2	L4
[L.IA] {xor} Authentication mechanism	T		L2	L4
[L.IA.1] PIN	T		L2	L4
[L.IA.2] Card (token)	T			
[L.IA.3] Card + PIN	T			

[L.IA.3.1] Something you have (e.g. card)	T			
[L.IA.3.1.1] The user takes responsibility for the custody of the card	T			
[L.IA.3.1.2] Difficult to clone	T			
[L.IA.3.1.3] When not in use, the card is stored in a secure separate place	T			
[L.IA.3.2] PIN	T			
[L.IA.3.2.1] PINs are easy to remember but hard to guess	T			
[L.IA.3.2.1.1] {xor} PINs have a minimum length	T			
[L.IA.3.2.1.1.1] 4 characters	T			
[L.IA.3.2.1.1.2] 6 characters	T			
[L.IA.3.2.1.1.3] 8 characters	T			
[L.IA.3.2.1.2] Passwords have no relation to the user identification, i.e. names or date of birth	T			
[L.IA.3.2.1.3] The same characters do not appear consecutively in passwords	T			
[L.IA.3.2.1.4] Passwords are not easily vulnerable to dictionary attacks	T			
[L.IA.3.2.2] Users guarantee PIN confidentiality	T			
[L.IA.3.2.2.1] ... are not shared	T			
[L.IA.3.2.2.2] ... are not written down on paper (unless encoded)	T			
[L.IA.3.2.2.3] ... are not stored in files (unless encrypted)	T			
[L.IA.3.2.2.4] ... are not stored on PDAs (except with a strong access protection)	T			
[L.IA.3.2.3] The same PIN is not used in several systems	T			
[L.IA.3.2.4] Different PINS are used for private and working roles	T			
[L.IA.3.2.5] {xor} PINs have a maximum usage period	T			
[L.IA.3.2.5.1] less than 1 year	T			
[L.IA.3.2.5.2] less than 6 months (180 days)	T			
[L.IA.3.2.5.3] less than 3 months (90 days)	T			
[L.IA.3.2.5.4] less than 1 month (30 days)	T			
[L.IA.3.2.6] Initial PINs are temporary with a limited duration (minimum and maximum)	T			
[L.IA.3.2.7] The PINs stored in the system are encoded	T			
[L.IA.3.3] The mechanism is disabled when compromised, or there is suspicion of it	T			
[L.IA.4] Something you are - biometrics	T			
[L.IA.4.1] {xor} Mechanism	T			
[L.IA.4.2] The mechanism is disabled when compromised, or there is suspicion of it	T			
[L.IA.5] Card + biometrics	T			
[L.IA.5.1] Something you have (e.g. card)	T			
[L.IA.5.1.1] The user takes responsibility for the custody of the card	T			
[L.IA.5.1.2] Difficult to clone	T			
[L.IA.5.1.3] When not in use, the token is stored in a secure separate place	T			
[L.IA.5.2] {xor} Biometrics	T			
[L.IA.5.2.1] Fingerprint	T			
[L.IA.5.2.2] Hand geometry	T			
[L.IA.5.2.3] Iris	T			
[L.IA.5.2.4] Retina	T			
[L.IA.5.2.5] Keyboard typing	T			
[L.IA.5.2.6] Voice	T			
[L.IA.5.2.7] Handwriting	T			
[L.IA.5.2.8] Other ...	T			
[L.IA.5.3] The mechanism is disabled when compromised, or there is suspicion of it	T			
[L.AC] Physical access control	PHY	7	L2	L4
[L.AC.1] Access via reception area	PHY	3	L2	L4
[L.AC.2] The reception is manned during working hours	PHY	3	L2	L4

[L.AC.3] Access control	PHY	5	L2	L4
[L.AC.3.1] There is a policy on access control	PHY	2	L2	L4
[L.AC.3.2] There are procedures in place for access control	PHY	2	L2	L4
[L.AC.3.3] Access authorizations are defined and documented	PHY	2	L2	L4
[L.AC.3.4] Prior verification of personnel access authorisation	PHY	3	L2	L4
[L.AC.3.5] Access is logged	PHY		L2	L4
[L.AC.3.6] Access log is regularly reviewed	PHY		L2	L4
[L.AC.3.7] Any suspected or attempted unauthorised physical access is investigated	PHY	2	L2	L4
[L.AC.3.8] Accepted persons are permanently accompanied (escorts), according to policy	PHY	5	L2	L4
[L.AC.3.9] Security searches at the entrance	PHY	5	L2	L4
[L.AC.3.a] Security searches at the exit	PHY	5	L2	L4
[L.AC.3.b] Automatic access control system	PHY	5	L2	L4
[L.AC.3.c] There is a video monitoring system	PHY	3	L2	L4
[L.AC.3.d] Emergency procedures guarantee that only authorised personnel can gain access to installations	PHY	3	L2	L4
[L.AC.3.e] Turnstiles at the entrances	PHY	3	L2	L4
[L.AC.3.f] Motorized barriers to entry	PHY	3	L2	L4
[L.AC.3.g] Full-height turnstiles at the entrances	PHY	3	L2	L4
[L.AC.3.h] X-ray inspection devices at the entrances	PHY	3	L2	L4
[L.AC.3.i] Casual inspection of the vehicles in the input and output	PHY	3	L2	L4
[L.AC.3.j] Bollards for pedestrian entrances	PHY	3	L2	L4
[L.AC.4] Control of visitors	M	4	L2	L4
[L.AC.5] Passes or identification	PHY	6	L2	L4
[L.AC.6] Access is closed outside of working hours	PHY	5	L2	L4
[L.AC.7] They are closed and checked periodically when empty	PHY	3	L2	L4
[L.AC.8] Avoid that physical access for operation or maintenance opens access to other assets	PHY	7	L2	L4
[L.AC.9] Emergency exits guarantee that only authorised personnel can gain access to installations	PHY	3	L2	L4
[L.AC.a] It is required that the working position is clear	PHY	3	L2	L4
[L.AC.b] Unsupervised work is avoided	PHY	6	L2	L4
[L.AC.c] Ban on recording equipment (photographic, video, audio, telephones, etc.) except with special permission	PHY	5	L2	L4
[PPS.a] Perimeter intrusion detection system	PHY	5	L2	L4
[PPS.f] Site security is not the responsibility of a single guard	PHY	5	L2	L4

[PS] Personnel

safeguard	**A**	**R**	**[current]**	**[target]**
[PS.1] Personnel management policy (for security)	PER		L2	L4
[PS.2] Personnel management procedures (for security)	PER		L2	L4
[PS.3] Personnel list	PER		L2	L4
[H.ST] Segregation of tasks	T		L2	L4
[H.ST.1] All critical processes require at least 2 people	T		L2	L4
[H.ST.2] Segregation of tasks into roles	T		L2	L4
[H.ST.3] Control of the effectivity of the separation architecture	T		L2	L4
[PS.5] Work positions	PER		L2	L4
[PS.5.1] There is an inventory job positions	PER		L2	L4
[PS.5.2] Identification and specification of work positions	PER		L2	L4
[PS.5.3] Security responsibilities are identified for all work positions	PER		L2	L4
[PS.5.4] Identification of security requirements for work positions are taken into account	PER		L2	L4
[PS.5.5] There is a binding policy for jobs	PER		L2	L4
[PS.5.6] There are defined information security-related performance measures for	PER		L2	L4

employees				
[PS.5.7] Security requirements for work positions are regularly reviewed	PER		L2	L4
[PS.6] Hiring	PER		L2	L4
[PS.6.3] Personnel selection and personnel policy	PER		L2	L4
[PS.6.4] Terms and conditions of employment relationship	PER		L2	L4
[PS.6.4.1] Inclusion of the scope, the reach and the period of security responsibilities	PER		L2	L4
[PS.6.4.2] Inclusion of legal obligations and rights of both parties	PER		L2	L4
[PS.6.4.3] Written undertaking to comply with policy	PER		L2	L4
[PS.6.4.4] Confidentiality agreements	PER		L2	L4
[PS.6.4.5] Disciplinary procedure	PER		L2	L4
[PS.6.5] Termination of employment relationship	PER		L2	L4
[PS.7] Personnel transfer	PER		L2	L4
[PS.AT] Training and awareness	PER		L2	L4
[PS.9] Prevention and reaction procedures	PER		L2	L4
[PS.9.1] to harmful software	PER		L2	L4
[PS.9.1.1] viruses	PER		L2	L4
[PS.9.1.2] spam	PER		L2	L4
[PS.9.1.3] others ...	PER		L2	L4
[PS.9.2] phishing	PER		L2	L4
[PS.9.3] to extortion	PER		L2	L4
[PS.9.4] to social engineering attacks	PER		L2	L4
[PS.cont] Ensuring availability	PER		L2	L4
[PS.cont.1] Enough slack is provided in the design of work teams	PER		L2	L4
[PS.cont.2] Staff availability is continuously monitored	PER		L2	L4
[PS.cont.3] Redundancy	PER		L2	L4
[PS.cont.4] Alternative personnel are subject to the same security guarantees	PER		L2	L4

[H.IR] Incident management (ICT)

safeguard	**A**	**R**	**[current]**	**[target]**
[H.IR.1] There is a policy covering all potential types of incidents	M	2	L2	L4
[H.IR.2] There are procedures for incident management	M	5	L2	L4
[H.IR.2.1] Reaction to harmful code (malware)	M	3	L2	L4
[H.IR.2.2] Reaction to denial of service (DoS) attacks	M	5	L2	L4
[H.IR.2.3] Reaction to system faults and loss of service	M	5	L2	L4
[H.IR.2.4] Reaction to errors resulting from inexact or incomplete business data	M	4	L2	L4
[H.IR.2.5] Reaction to breaches of confidentiality	M	4	L2	L4
[H.IR.2.6] Reaction to alarms from the intrusion detection system	M	3	L2	L4
[H.IR.2.7] Reaction to alarms from the intrusion prevention system	M	3	L2	L4
[H.IR.2.8] Reaction to alarms from file-integrity monitoring systems	M	3	L2	L4
[H.IR.2.9] Reaction to any evidence of unauthorized activity	M	3	L2	L4
[H.IR.2.a] Reaction to software failures	M	4	L2	L4
[H.IR.2.b] Reaction to detection of unauthorized wireless access points	M	3	L2	L4
[H.IR.2.c] Detection and response to industrial espionage	M	3	L2	L4
[H.IR.2.d] Detection and response to personal data theft activities	M	3	L2	L4
[H.IR.2.e] Reaction to other incidents	M	3	L2	L4
[H.IR.2.f] Coordination with other affected information systems	M	3	L2	L4
[H.IR.3] Containment of incident	M	6	L2	L4
[H.IR.3.1] Designated personnel are available for 24/7 incident response and monitoring coverage	M	3	L2	L4
[H.IR.3.2] System fails into a controlled state	M	3	L2	L4
[H.IR.3.3] Jobs in the affected system are suspended until the incident has been resolved	M	6	L2	L4
[H.IR.3.4] The affected system is isolated until the incident has been resolved	M	6	L2	L4
[H.IR.4] Management procedure	M	4	L2	L4

[H.IR.4.1] The cause is analysed and identified	M	2	L2	L4
[H.IR.4.2] Analysis of the impact of the incident	M	3	L2	L4
[H.IR.4.3] Planning and implementation of measures	M	2	L2	L4
[H.IR.4.4] Communication with the affected parties involved in the recovery	M	4	L2	L4
[H.IR.4.5] There is communication with those involved in the recovery of the incident	M	3	L2	L4
[H.IR.4.6] The actions are communicated to the relevant authority in the organisation	M	2	L2	L4
[H.IR.4.7] Evidence	M		L2	L4
[H.IR.5] Cooperation with other organisations	M	5	L2	L4
[H.IR.6] Communication of security incidents	M	3	L2	L4
[H.IR.7] Communication of security deficiencies	M	2	L2	L4
[H.IR.8] Software fault communication	M	3	L2	L4
[H.IR.9] Incidents are logged	M		L2	L4
[H.IR.a] Faults and corrective measures are logged and reviewed	M	3	L2	L4
[H.IR.b] Formal control of the recovery process when an incident occurs	M	3	L2	L4
[H.IR.c] Training and awareness	PER	3	L2	L4
[H.IR.c.1] Awareness on detection and communication of incidents	PER	2	L2	L4
[H.IR.c.2] Detection and handling training	PER	2	L2	L4
[H.IR.c.3] System singularities are taken into account	PER	3	L2	L4
[H.IR.c.3.1] Security requirements	PER	2	L2	L4
[H.IR.c.3.2] Legal and contractual responsibilities	PER	2	L2	L4
[H.IR.c.3.3] Potential threats	PER	2	L2	L4
[H.IR.c.3.4] Identified vulnerabilities	PER	2	L2	L4
[H.IR.c.3.5] Incidents	PER	3	L2	L4
[H.IR.c.4] Incident handling procedures are regularly exercised (tested)	PER	2	L2	L4
[H.IR.d] Incidents are used to learn, and improve	M	3	L2	L4
[H.IR.e] Measures are taken to prevent recurrence	M	4	L2	L4

[BC] Business continuity (contingency)

safeguard	A	R	[current]	[target]
[BC.1] There is a policy on business continuity	M	3	L2	L4
[BC.2] The inventory is regularly updated	M	3	L2	L4
[BC.BIA] Business impact analysis (BIA)	M	2	L2	L4
[BC.4] Preparatory activities	M	3	L2	L4
[BC.5] Reaction (crisis management)	M	3	L2	L4
[BC.DRP] Disaster Recovery Plan (DRP)	M	5	L2	L4
[BC.DRP.1] Persons are assigned to responsibilities	M	2	L2	L4
[BC.DRP.2] Coordination between all areas in the organisation	M	4	L2	L4
[BC.DRP.3] Development of the documentation	M	2	L2	L4
[BC.DRP.4] Notification and activation	M	2	L2	L4
[BC.DRP.5] Recovery	T	5	L2	L4
[BC.DRP.5.1] Recovery activities	T	2	L2	L4
[BC.DRP.5.2] Recovery procedures are thoroughly defined	T	2	L2	L4
[BC.DRP.5.3] Required resources	T	3	L2	L4
[BC.DRP.5.4] There are alternative facilities	PHY	5	L2	L4
[BC.DRP.5.5] Backup copies: frequency and storage	T	5	L2	L4
[BC.DRP.5.6] There are alternative storage resources	T	5	L2	L4
[BC.DRP.5.7] There are alternative processing resources	T	5	L2	L4
[BC.DRP.5.8] There are alternative communication resources	T	5	L2	L4
[BC.DRP.5.9] There is alternative personnel	PER	5	L2	L4
[BC.DRP.5.a] Alternative working place(s)	PHY	5	L2	L4
[BC.DRP.6] Training plan	M	2	L2	L4

[BC.DRP.7] Plans are regularly exercised (tested)	M	4	L2	L4
[BC.7] Restitution	T	2	L2	L4

[G] Organisation

safeguard	A	R	[current]	[target]
[G.1] Internal organisation	M	6	L2	L4
[PM-7] Enterprise Architecture	M	6	L2	L4
[G.1.2] Information security management committee	M	2	L2	L4
[G.1.3] Internal coordination	M	2	L2	L4
[G.1.4] Identified roles	M	3	L2	L4
[G.1.5] Allocation of responsibilities in information security	M	2	L2	L4
[G.1.6] Specialist advice in security is available	M	2	L2	L4
[G.2] Technical documentation (components)	M	3	L2	L4
[G.2.1] Documentation of the system: treated information, processes, formats, applications, equipment and communications networks	M	2	L2	L4
[G.2.1.1] Documentation of the facilities	M	2	L2	L4
[G.2.1.2] Documentation of communications	M	2	L2	L4
[G.2.1.3] Interconnection points (between trust zones)	M	2	L2	L4
[G.2.1.4] Documentation of logical access points to the system	M	2	L2	L4
[G.2.1.5] Access control documentation	M	2	L2	L4
[G.2.2] Acceptance criteria for new versions or systems	M	2	L2	L4
[G.2.3] Security of system documentation	M	3	L2	L4
[G.3] Organizational documents (policies & procedures)	M	3	L2	L4
[G.3.1] Reference framework	M	2	L2	L4
[G.3.2] Security Policy of the Organization	M	3	L2	L4
[G.3.3] Security policies	M	2	L2	L4
[G.3.4] Security Operating Procedures (SecOPs)	M	2	L2	L4
[G.3.5] Personnel compliance is regularly reviewed	M	2	L2	L4
[G.4] Personal data protection	M	6	L2	L4
[PIA] Conducting a PIA	M	6	L2	L4
[PIA:a] Content	M	6	L2	L4
[PIA:a.1] PIAs must analyse and describe:	M	6	L2	L4
[PIA:a.1.1] what information is to be collected (e.g., nature and source);	M	6	L2	L4
[PIA:a.1.2] why the information is being collected (e.g., to determine eligibility);	M	6	L2	L4
[PIA:a.1.3] intended use of the information (e.g., to verify existing data);	M	6	L2	L4
[PIA:a.1.4] with whom the information will be shared (e.g., another agency for a specified programmatic purpose);	M	6	L2	L4
[PIA:a.1.5] what opportunities individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent;	M	6	L2	L4
[PIA:a.1.6] how the information will be secured (e.g., administrative and technological controls); and	M	6	L2	L4
[PIA:a.1.7] whether a system of records is being created under the Privacy Act, 5 U.S.C. 552a.	M	6	L2	L4
[PIA:a.2] Analysis: PIAs must identify what choices the agency made regarding an IT system or collection of information as a result of performing the PIA.	M	6	L2	L4
[PIA:b] Agencies should commence a PIA when they begin to develop a new or significantly modified IT system or information collection:	M	6	L2	L4
[PIA:b.1] Specificity. The depth and content of the PIA should be appropriate for the nature of the information to be collected and the size and complexity of the IT system.	M	6	L2	L4
[PIA:b.1.1] IT development stage. PIAs conducted at this stage:	M	6	L2	L4
[PIA:b.1.1.3] may need to be updated before deploying the system to consider elements not identified at the concept stage (e.g., retention or disposal of information), to reflect a new information collection, or to address choices made in designing the	M	6	L2	L4

system or information collection as a result of the analysis.				
[PIA:b.1.1.1] should address privacy in the documentation related to systems development, including, as warranted and appropriate, statement of need, functional requirements analysis, alternatives analysis, feasibility analysis, benefits/cost analysis, and, especially, initial risk assessment;	M	6	L2	L4
[PIA:b.1.1.2] should address the impact the system will have on an individual's privacy, specifically identifying and evaluating potential threats relating to each of the elements identified in section II.C.1.a.(i)-(vii) above, to the extent these elements are known at the initial stages of development;	M	6	L2	L4
[PIA:b.1.2] Major information systems. PIAs conducted for these systems should reflect more extensive analyses of:	M	6	L2	L4
[PIA:b.1.2.1] the consequences of collection and flow of information,	M	6	L2	L4
[PIA:b.1.2.2] the alternatives to collection and handling as designed,	M	6	L2	L4
[PIA:b.1.2.3] the appropriate measures to mitigate risks identified for each alternative and,	M	6	L2	L4
[PIA:b.1.2.4] the rationale for the final design choice or business process.	M	6	L2	L4
[PIA:b.1.3] Routine database systems. Agencies may use a standardized approach (e.g., checklist or template) for PIAs involving simple systems containing routine information and involving limited use and access.	M	6	L2	L4
[PIA:b.2] Information life cycle analysis/collaboration. Agencies must consider the information "life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) in evaluating how information handling practices at each stage may affect individuals' privacy. To be comprehensive and meaningful, privacy impact assessments require collaboration by program experts as well as experts in the areas of information technology, IT security, records management and privacy.	M	6	L2	L4
[PIA:c] Review and publication	M	6	L2	L4
[PIA:c.1] Agencies must ensure that:	M	6	L2	L4
[PIA:c.1.1] the PIA document and, if prepared, summary are approved by a "reviewing official" (the agency CIO or other agency head designee, who is other than the official procuring the system or the official who conducts the PIA);	M	6	L2	L4
[PIA:c.1.2] for each covered IT system for which 2005 funding is requested, and consistent with previous guidance from OMB, the PIA is submitted to the Director of OMB no later than October 3, 2003 (submitted electronically to PIA@omb.eop.gov along with the IT investment's unique identifier as described in OMB Circular A-11, instructions for the Exhibit 3008); and	M	6	L2	L4
[PIA:c.1.3] the PIA document and, if prepared, summary, are made publicly available (consistent with executive branch policy on the release of information about systems for which funding is proposed).	M	6	L2	L4
[PIA:c.1.3.1] Agencies may determine to not make the PIA document or summary publicly available to the extent that publication would raise security concerns, reveal classified (i.e., national security) information or sensitive information (e.g., potentially damaging to a national interest, law enforcement effort or competitive business interest) contained in an assessment. Such information shall be protected and handled consistent with the Freedom of Information Act (FOIA).	M	6	L2	L4
[PIA:c.1.3.2] Agencies should not include information in identifiable form in their privacy impact assessments, as there is no need for the PIA to include such information. Thus, agencies may not seek to avoid making the PIA publicly available on these grounds.	M	6	L2	L4
[RM] Risk management	M	3	L2	L4
[RM.1] There is a policy for risk management	M	3	L2	L4
[RM.2] Persons are assigned to responsibilities	M	3	L2	L4
[RM.3] There are written procedures to carry out risk analysis and management tasks	M	3	L2	L4
[RM.4] Assets	M	3	L2	L4
[RM.5] Threats: identification and valuation	M	3	L2	L4
[RM.6] Safeguards	M	3	L2	L4
[RM.7] Risk assessment	M	3	L2	L4

[RM.8] Regular review	M	3	L2	L4
[G.plan] Security planning	M	6	L2	L4
[G.plan.1] There is a planning policy (for security)	M	2	L2	L4
[G.plan.2] There are procedures for security planning	M	2	L2	L4
[G.plan.3] Capacity planning	M	3	L2	L4
[G.plan.4] Critical components: lack of alternative suppliers	M	2	L2	L4
[G.plan.5] Security-related activity planning	M	6	L2	L4
[PM-4] Plan of Action and Milestones Process	M	6	L2	L4
[SA-2] Allocation of Resources	M	6	L2	L4
[CM-9] Configuration Management Plan	M	6	L2	L4
[G.exam] Security inspections	M	4	L2	L4
[G.8] Safeguarding the Organisation records (vital records)	M	3	L2	L4
[G.8.1] There is an inventory	M	2	L2	L4
[G.8.2] Secure storage	M	3	L2	L4
[G.8.3] Legal and contractual requirements are taken into account	M	2	L2	L4
[G.8.4] Business continuity requirements are taken into account	M	2	L2	L4
[G.8.5] Guides for retention, storage, processing and removal of the registries	M	2	L2	L4
[G.8.6] Log retention for the established period	M	2	L2	L4

[E] External Relations

safeguard	A	R	[current]	[target]
[E.1] Establishment of agreements to exchange information and software	M		L2	L4
[E.2] External access	M		L2	L4

[NEW] Acquisition / development

safeguard	A	R	[current]	[target]
[NEW.S] Services: Acquisition or development	M		L2	L4
[NEW.S.1] Resource allocation	M		L2	L4
[NEW.S.2] Functional requirements are determined previously	M		L2	L4
[NEW.S.3] Security requirements are aligned with business needs	M		L2	L4
[NEW.S.4] Technical security requirements are identified	M		L2	L4
[S.start] Acceptance and commissioning	M		L2	L4
[NEW.SW] Software: Acquisition or development	M	5	L2	L4
[NEW.SW.1] Functional requirements are determined previously	M	2	L2	L4
[NEW.SW.2] Security requirements are aligned with business needs	M	2	L2	L4
[NEW.SW.3] Technical security requirements are identified	M	3	L2	L4
[NEW.SW.5] Acquisition (SW)	M	3	L2	L4
[NEW.SW.6] Development	M	5	L2	L4
[NEW.SW.8] Operating system independent applications are preferred	M	3	L2	L4
[NEW.HW] Equipment: Acquisition or development	M	4	L2	L4
[NEW.HW.1] Functional requirements are determined previously	M	2	L2	L4
[NEW.HW.2] Security requirements are aligned with business needs	M	2	L2	L4
[NEW.HW.3] Technical security requirements are identified	M	3	L2	L4
[NEW.HW.4] HW acquisition	M	3	L2	L4
[NEW.HW.5] HW development	M	4	L2	L4
[NEW.COM] Communications: Acquisition or contracting	T	3	L2	L4
[NEW.MP] Acquisition of media	M		L2	L4
[NEW.C] Certified / accredited products are used	M	4	L2	L4

Παράρτημα Η : Ελάχιστες Ασφαλείς Διαδικασίες

security procedures
project: [nos1] nos1
Project data

nos1	nos1
library	[std] INFOSEC library (8.11.2013)

License
maturity levels
L0 - non existent
L1 - initial / ad hoc
L2 - repeatable but intuitive
L3 - defined process
L4 - managed and measurable
L5 - optimised
Security domains
[base] Base
Project phases
[current] current situation
[target] target situation
Security domain: [base] Base
[H] General Protections

security procedure
Identification and authentication
There are procedures for identification and authentication tasks
Logical access control
There are procedures for access control tasks
There is a procedure for granting privileges
There is a procedure for cancellation of privileges
There is a procedure for the temporary suspension of privileges
There is a procedure for the reactivation of suspended privileges
Vulnerability management
There are procedures for reaction
preventive measures
emergency measures to high risk
plan of action against moderate risks
Logging and audit
Administration
There are procedures for system audit and accountability
Guides for retention, storage, processing and removal of the registries

[D] Protection of Data / Information

security procedure
Regulations
Information is classified
There are procedures for the treatment of classified information
IPR: intellectual property rights for information are protected
There is a procedure for backups
Integrity guarantees
There are procedures for integrity protection
Confidentiality protection
Encryption of information
There are procedures for information encryption
Encryption procedure
Decryption procedure

Backup copies of the data
Protection of the availability of the information
There are procedures for preparing backup copies, their protection and conservation
Backup procedure
Data recovery procedure
Procedure for local storage of backups
Procedure for remote storage of backups
Procedure to remove backup copies that are no longer required
Usage of electronic signatures
There are procedures for the usage of electronic signatures
Signature procedures
Signature verification procedures
Usage of time stamping services
Time stamping procedures
Time stamping procedure
Date verification procedure

[K] Cryptographic keys management

security procedure
Management of information encryption keys
There are procedures for key management
Management of information signing keys
There are procedures for key management
Management of keys for cryptographic containers (virtual disks)
There are procedures for key management
Management of communications keys
There are procedures for key management
Certificate management
There are procedures for using certificates

[S] Protection of Services

security procedure
Service usage
Usage of e-mail
Define procedures for policy violation
Tele-working
There are procedures to manage tele-working
Physical security
Provision of storage equipment and furniture
Hardware and software support
Provision of communications, including secure remote access methods
Incident management
Backup and business continuity procedures
Audit and security monitoring procedures
Procedures for returning equipment and revoking access rights when activities have ceased
There is a procedure for action in case of non-compliance
Provision of services
Availability assurance
DoS protection
Operating procedures
Monitoring procedures
Reaction procedure
Coordination procedures are followed with the supplier (or suppliers) of communications services
Change management (upgrades and replacements)
There are procedures to apply changes

There is a formal procedure to approve changes
The details of the change are communicated to all affected personnel
Services provided by third parties
Continuity of operations
Establishing a protocol in case of contingency

[SW] Protection of Software

security procedure
Procedures for the usage of software applications
Normal use
Specific security procedures
Action in case of malfunction
Protection of intellectual property rights (IPR)
There is a procedure to copy information subject to IPR
Backup copies (SW)
Procedures to prepare backup copies
Backup procedures
Restoration procedure
Procedures for backup retention and destruction
Procedures for destruction of backups
Exploitation
Security of applications
Input data validation
Procedures to respond for validation errors
Validation of output data
Procedures for filling-in output validation questionnaires
Changes (updates & maintenance)
There are procedures to apply changes
There is a formal procedure to approve changes
The details of the change are communicated to all affected personnel

[HW] Protection of Hardware

security procedure
Procedures for the usage of equipment
Normal use
Specific security procedures
Action in case of malfunction
Move to production
There are procedures to move onto operation / production
Changes (updates and maintenance)
There are procedures to apply changes
There is a formal procedure to approve changes
The details of the change are communicated to all affected personnel
Mobile computers
Incident management in mobile computing
There are procedures for managing incidents

[COM] Protection of Communications

security procedure
There are procedures for the usage of communications
Normal use
Specific security procedures
Action in case of malfunction
Changes (updates and maintenance)
There are procedures to apply changes
There is a formal procedure to approve changes
The details of the change are communicated to all affected personnel

[AUX] Auxiliary Means

security procedure
Availability guarantees
Protection of wiring
There is a procedure for amending the wiring

[L] Protection of the installations

security procedure
Continuity of operations
A protocol is in place for contingency

[PPS] Perimeter protection

security procedure
Physical access control
Access control
There are procedures in place for access control
Passes or identification
There are procedures for issue, control, registry, deactivation and cancellation of passes

[PS] Personnel

security procedure
Personnel management procedures (for security)
Hiring
Terms and conditions of employment relationship
Disciplinary procedure
Sanctions for breach of contract
Sanctioning procedure
Communication of the procedure
Training and awareness
Training and awareness procedures

[BC] Business continuity (contingency)

security procedure
Reaction (crisis management)
Crisis management plan
Disaster Recovery Plan (DRP)
Notification and activation
There is a notification procedure
There is a procedure for plan activation
Recovery
Recovery procedures are thoroughly defined

[G] Organisation

security procedure
Risk management
There are written procedures to carry out risk analysis and management tasks
Security planning
There are procedures for security planning
Security inspections
There are procedures for security certification, accreditation, and assessment
Safeguarding the Organisation records (vital records)
Guides for retention, storage, processing and removal of the registries

[E] External Relations

security procedure
Establishment of agreements to exchange information and software
There are procedures for notification of shipment, transmission and reception
There are procedures to ensure the accountability and non-repudiation

Βιβλιογραφία

1. Λαμπρινουδάκης Κ., Ανάλυση και Διαχείριση Επικυνδυνότητας Πληροφοριακών Συστημάτων,Σημειώσεις Πανεπιστημίου Πειραιώς, Τμήμα Ψηφιακών Συστημάτων.

2. Σ.Κάτσικας «Ασφάλεια Υπολογιστών», Πάτρα, 2011

3. https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_EAR_Pilar.html

4. NIST SP 800-30

5. Behnia, A., et al. (2012). "A survey of information security risk analysis methods." SmartCR **2**(1): 79-94.

6. Crespo, F. L., et al. (2006). "MAGERIT–version 2, Methodology for Information Systems Risk Analysis and Management, Book I–The Method." Ministerio de administraciones públicas.

7. GOBIERNO DE ESPANA, Miguel A. AmutioJavier Candau, J. A. M. (2014). Magerit-version3.0 Methodology for Information Systems Risk Analysis and Management.

8. Ionita, D. (2013). Current established risk assessment methodologies and tools.

9. Marek, P. and J. Paulina (2006). The OCTAVE methodology as a risk analysis tool for business resources. International Multiconference Computer Science and IT, Hong Kong.

10. Antolík, Štefan. "COMPARISON OF TOOLS FOR INFORMATION SECURITY MANAGEMENT SYSTEM." *UNIVERSITY OF DEFENCE/CZECH REPUBLIC*: 7.

11. Mareile Kaufmann,(20-02-2012) D3.2 – Catalogue of evaluated methodologies and tools, ValueSec

12. ISO 31000:2009 Risk management—Principles and guidelines.

13.ISO/IEC Guide 73:2009 Risk management – Vocabulary.

14. ISO/IEC 31010:2009 Risk management—Risk assessment techniques.

15. ISO/IEC 27005:2011 Information technology - Security techniques - Information security risk management.

16. NIST SP 800-39:2011 Managing Information Security Risk: Organization, Mission, and Information System View http://csrc.nist.gov/publications/PubsSPs.html

17. NIST SP 800-37 Rev. 1, 2010 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach http://csrc.nist.gov/publications/PubsSPs.html

18. NIST SP 800-30:2002 Risk Management Guide for Information Technology Systems. http://csrc.nist.gov/publications/PubsSPs.html

19.ISACA:2010 The Risk IT Framework http://www.isaca.org/

20.ISACA:2009 The Risk IT Practitioner Guide http://www.isaca.org/

21.AS/NZS 4360:2004 Risk management

22. CRAMM User Guide, Issue 5.1, July, 2005.

23. OCTAVE, CERT
www.cert.org/octave

24. Callio Secura 17799

www.callio.com

25. COBRA

www.riskworld.net

26. CRAMM

www.cramm.com

27. PILAR Basic version 5.4 5
Glossary of Terms

http://www.pilar-tools.com/en/glossary/index.html

PILAR
http://www.pilar-tools.com/en/tools/pilar/doc.htm

28. EBIOS

http://ssi.gouv.fr/guide/ebios-2010

29. Cloud eAssurance

www.cloudeAssurance.com

30. CCS Risk Manager

http://www.symantec.com/theme.jsp?themeid=control-compliance-suite.

31. Μαρία Καρύδα, Αγγελική Τσώχου, Κωνσταντίνος Λαμπρινουδάκης, Στέφανος Γκρίτζαλης, 31-12-2005, Μελέτη Σχεδίου Ασφάλειας του Γενικού Νοσοκομείου Κορίνθου για τη λειτουργία αρχείων με ευαίσθητα δεδομένα.