ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Μέθοδος Ανάλυσης & Διαχείρισης Επικινδυνότητας Πληροφοριακών Συστημάτων MAGERIT : Μελέτη περίπτωσης Γενικού Νοσοκομείου με χρήση του εργαλείου EAR/Pilar

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

των

Ιωάννη Σκοπελίτη
Ιωάννη Βάσιλα

Επιβλέπων : Μαρία Καρύδα, Αναπληρώτρια Καθηγήτρια

Μέλη εξεταστικής επιτροπής:

Σάμος, Φεβρουάριος 2023

ΠΕΡΙΕΧΟΜΕΝΑ

ΛΙΣΤΑ ΕΙΚΟΝΩΝ

ΛΙΣΤΑ ΠΙΝΑΚΩΝ

1. ΕΙΣΑΓΩΓΗ

1.1 Σκοπός

Στην παρούσα εργασία θα μελετηθεί η ανάλυση και η διαχείριση επικινδυνότητας του πληροφοριακού συστήματος (ΠΣ) ενός Γενικού Νοσοκομείου (ΓΝ) των Αθηνών.

Θα ακολουθηθούν διαδικασίες, αρχές και μέτρα για την προστασία των πληροφοριακών συστημάτων και θα προκύψει η έννοια της ασφάλειας σε αυτά, με σκοπό την ομαλή λειτουργία και την εξασφάλιση των βασικών αρχών ασφάλειας κατά Διαθεσιμότητα , Ακεραιότητα και Εμπιστευτικότητα των δεδομένων.

Στη μελέτη αυτή η Ανάλυση και Διαχείριση της Επικινδυνότητας θα υλοποιηθεί με χρήση της μεθοδολογίας **MAGERIT** και το αντίστοιχο εργαλείο της, **EAR/Pilar.**

Μέσα από την εκπόνηση της συγκεκριμένης μεθοδολογίας στο ΠΣ θα προσδιοριστούν τα κρίσιμα αγαθά του συστήματος, οι απειλές, τα αδύνατα σημεία του και θα προταθούν στο τέλος κάποια μέτρα-αντίμετρα προστασίας για ασφαλέστερη λειτουργία του συστήματος.

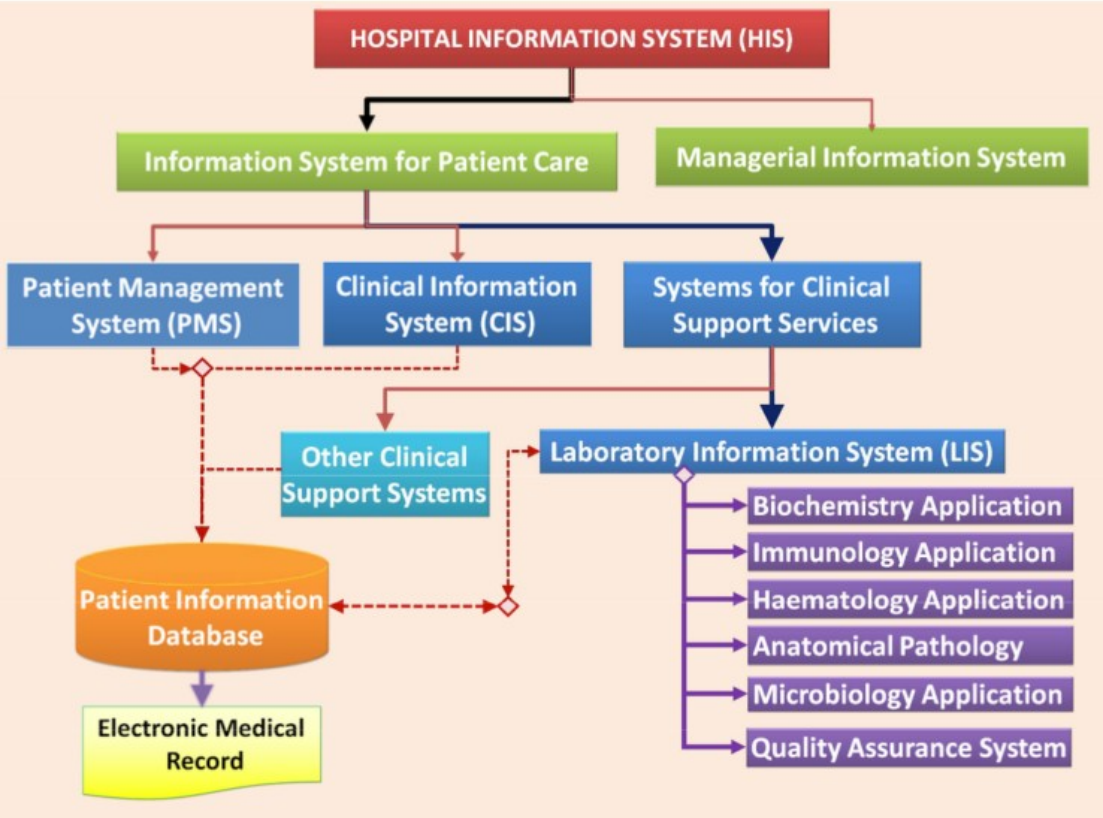
Το Πληροφοριακό Σύστημα αποτελείται από τις εφαρμογές και όλα τα υπολογιστικά συστήματα του ΠΣ του εν λόγω νοσοκομείου.

Λόγω του ότι οι πληροφορίες και δεδομένα αποθηκεύονται από έναν οργανισμό, όπως στην περίπτωση του νοσοκομείου, αυξάνεται η ανάγκη προστασίας τους. Ειδικότερα όταν αυτά τα δεδομένα είναι ευαίσθητα προσωπικά δεδομένα και ειδικά τα ιατρικά δεδομένα ασθενών.

Όπως όλοι οι οργανισμοί έτσι και στη περίπτωση αυτή, το νοσοκομείο πρέπει να εφαρμόσει συστήματα με αρχιτεκτονικές ασφαλείας για την αξιόπιστη παροχή υπηρεσιών προς τους πολίτες. Οι ευπάθειες στην αρχιτεκτονική ασφαλείας αλλά και η μη ορθή εφαρμογή του σχεδίου ασφαλείας, πλήττουν τα υφιστάμενα περιουσιακά στοιχεία. Ως συνέπεια αυτών, οι οργανισμοί καλούνται να αντιμετωπίσουν κόστη αρκετών χιλιάδων ευρώ: για την διόρθωση των διαρροών, την απώλεια των ευαίσθητων προσωπικών δεδομένων, την αποκατάσταση της φήμης, καθώς και μηνύσεις και απώλεια αξιόπιστης παροχής υπηρεσιών.

Κάποια από τα δεδομένα που έχουν αντίκτυπο κατά την παραβίαση του ΠΣ του Νοσοκομείου είναι: ονοματεπώνυμα, ιστορικά ασθενών, διευθύνσεις, emails, αριθμούς τηλεφώνων αλλά και αριθμούς κοινωνικής ασφάλισης. Η απόκτηση των πληροφοριών αυτών, αποτελεί στόχο για τους επιτιθέμενους με σκοπό να τις αξιοποιήσουν προς όφελος τους. Αποτέλεσμα αυτών είναι: οι ηλεκτρονικές επιθέσεις να έχουν αυξηθεί ραγδαία τα τελευταία χρόνια. Ο αντίκτυπος των περιστατικών παραβίασης των δεδομένων είναι σημαντικός τόσο για τους οργανισμούς όσο και για τα άτομα.

Το Νοσοκομείο που μελετήθηκε διαθέτει ένα ολοκληρωμένο πληροφοριακό σύστημα με τα υποσυστήματα ιατρικού και εργαστηρίων, νοσηλευτικού, διοικητικού-οικονομικού, τεχνικού όπως το παράδειγμα παρακάτω:



Εικόνα 1. [Dr Abdollah Salleh, 2014

Ως κύριος στόχος ενός οργανισμού είναι η διαφύλαξη και η προστασία των δεδομένων για την εύρυθμη λειτουργία του. Για το λόγο αυτό και στην περίπτωση αυτή, η προστασία και η διασφάλιση των περιουσιακών στοιχείων του νοσοκομείου.

1.2 Δομή Διπλωματικής

Η δομή της διπλωματικής εργασίας χωρίζεται σε πέντε βασικά κεφάλαια και σε επιμέρους αυτών:

Στο **1ο κεφάλαιο** θα γίνει συνοπτική αναφορά στην ορολογία των βασικών εννοιών της ανάλυσης και διαχείρισης κινδύνου.

Στο **2ο κεφάλαιο** θα γίνει ανάλυση της μεθοδολογίας **MAGERIT** με το αντίστοιχο εργαλείο **EAR/Pilar.**

Στο **3ο κεφάλαιο** θα καθοριστούν τα κρίσιμα συστήματα του ΠΣ-ΓΝ, τα αγαθά και η αποτίμηση τους κατά την MAGERIT. Επίσης, θα παρουσιαστούν τα σενάρια των απειλών σε αυτά. Στην συνέχεια, θα αναλυθεί και θα παρουσιαστεί ο βαθμός επικινδυνότητας και η τελική αποτίμηση για κάθε περιουσιακό στοιχείο.

Τέλος, θα αναφερθούν οι κατηγορίες μέτρων όπου θα προκύπτουν τα απαραίτητα μέτρα ασφαλείας για το συγκεκριμένο ΠΣ-ΓΝ. και θα περιληφθούν στο σχέδιο ασφαλείας αυτού.

Στο **4ο κεφάλαιο** θα γίνει εκτίμηση της διαχείρισης επικινδυνότητας και του σχεδίου ασφαλείας, με κάποιες προτεινόμενες βελτιώσεις του συγκεκριμένου ΠΣ του Γενικού Νοσοκομείου.

Στο **5ο κεφάλαιο** Συμπεράσματα.

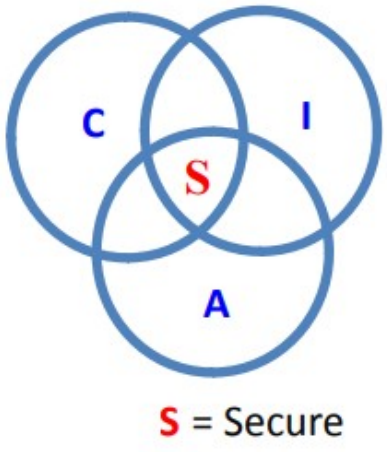
1.3 Έννοιες – Ορισμοί

Η ασφάλεια των πληροφοριακών συστημάτων βασίζεται σε τρεις βασικές ιδιότητες οι οποίες είναι απαραίτητες για την ορθή λειτουργία του Π.Σ.,[Χαράμης Γ. 2001]:

- **Εμπιστευτικότητα (C*onfidentiality):*** *Διασφαλίζει ότι τα δεδομένα δεν αποκαλύπτονται σε μη εξουσιοδοτημένες οντότητες,*

- **Ακεραιότητα *(Integrity):*** *Εξασφαλίζει τη μη τροποποίηση των δεδομένων από μη εξουσιοδοτημένους χρήστες*

- **Διαθεσιμότητα *(Availability):*** *Μπορεί να έχει πρόσβαση σε δεδομένα όποτε τα χρειαστεί.*



Εικόνα 2. CIA [Γεώργιος Καμπουράκης]

Οι παραπάνω τρεις ιδιότητες δεν επαρκούν, για να οριστεί η ασφάλεια πληροφοριών [Μουλίνος, 2003]. Μπορούν να προστεθούν η **αυθεντικότητα (authenticity):** η απόδειξη της προέλευσης και του ιδιοκτήτη της πληροφορίας, η **εγκυρότητα (validity):** η πληροφορία αφορά την πραγματικότητα και είναι επίκαιρη, και η **μη αποποίηση (non-repudiation):** η αδυναμία άρνησης ενεργειών που έχουν εκτελεστεί για την τροποποίηση, την αποστολή ή τη λήψη μίας πληροφορίας.

Οι βασικές έννοιες για την ασφάλεια της πληροφορίας των πληροφοριακών συστημάτων, για την ανάλυση κινδύνων. [Γκρίτζαλης, 1996],[Καμπουράκης The Book of Five Rings]:

- **Πληροφοριακό Σύστημα,** *Ένα σύνολο αλληλοεπιδρώντων στοιχείων (εφαρμογές, διαδικασίες, υπηρεσίες, άνθρωποι, δεδομένα, λογισμικό, υλικός εξοπλισμός), το οποίο επεξεργάζεται δεδομένα και παράγει πληροφορίες για λογαριασμό 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.*

- **Αξία (value)**, *ονομάζεται η σημαντικότητα ενός αντικειμένου, με οικονομικό ή άλλο τρόπο.*

- **Αγαθό (asset)**, *αποτελεί κάθε πληροφορία, δεδομένο ή υπολογιστικός πόρος που έχει μια εκτιμώμενη αξία χρηματική η μη.*

- **Κίνδυνος (danger)**, *ονομάζεται το ενδεχόμενο ένα αγαθό να υποστεί ζημιά.*

- **Ζημία (harm)**, *ονομάζεται ο περιορισμός της αξίας ενός αγαθού.*

- **Επίπτωση (impact)**, *ονομάζεται η απώλεια ενός αγαθού ή το αυξημένο κόστος ή άλλη ζημιά που μπορεί να συμβεί ως αποτέλεσμα μια συγκεκριμένης προσβολής.*

- **Μέσο προστασίας – Αντίμετρο (safeguard)**, *ονομάζεται κάθε ενέργεια που αποσκοπεί στον αποκλεισμό μιας προσβολής ή στην ελαχιστοποίηση των συνεπειών της.*

- **Ευπάθεια (vulnerability)**, *ονομάζεται ένα συγκεκριμένο χαρακτηριστικό ενός πληροφοριακού συστήματος, το οποίο ενδεχομένως να επιτρέψει την πραγματοποίηση κάποιας προσβολής. Ευπάθεια είναι η αδυναμία ενός περιουσιακού στοιχείου, η έλλειψη ελέγχων η οποία θα μπορούσε να διευκολύνει ή επιτρέψει να συμβεί μια απειλή.*

- **Απειλή (threat)**, *ονομάζεται η ενδεχόμενη απώλεια ενός ή περισσότερων από τις παραμέτρους που ορίζουν την ασφάλεια ενός πληροφοριακού συστήματος. 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.*

• **Ανάλυση Κινδύνου,** *ενός πληροφοριακού συστήματος είναι η διαδικασία αξιολόγησης των κινδύνων ασφαλείας που εισάγει το σύστηνα καθώς και το κόστος.*

• **Επικινδυνότητα - 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,** *(διοικητικό, οργανωτικό, τεχνικό) που εφαρμόζεται για την προστασία του πληροφοριακού συστήματος και την αντιμετώπιση των απειλών ή για να μειώσει τις δυνητικές επιπτώσεις. Περιλαμβάνουν οποιαδήποτε διεργασία, πολιτική, συσκευή, πρακτική, ή άλλες ενέργειες οι οποίες τροποποιούν τον κίνδυνο.*

• **Εναπομένων Κίνδυνος,** *είναι ο συνολικός κίνδυνος μείον τους ληφθέντες κινδύνους.*

• **Πολιτική Ασφαλείας,** *είναι 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,** *είναι το έγγραφο που περιγράφει τα οργανωτικά και τεχνικά μέτρα, και τα μέτρα φυσικής ασφάλειας που εφαρμόζονται ή πρόκειται για την κάλυψη των βασικών αρχών και κανόνων που αναφέρονται στην πολιτική ασφαλείας. Συμπεριλαμβάνει τις απαραίτητες ενέργειες για την υλοποίηση του.*

Για την επιλογή της κατάλληλης μεθόδου εκτίμησης και διαχείρισης κινδύνου από τον εκάστοτε οργανισμό απαιτείτε η εξέταση πολλών παραμέτρων όπως: το ανθρώπινο δυναμικό το εύρος λειτουργίας το μέγεθος και την πολυπλοκότητα του ΠΣ.

1.4 Πρότυπα για τη Διαχείριση Επικινδυνότητας ISO/IEC

Υπάρχουν πρότυπα ISO/IEC που σχετίζονται με την ασφάλεια [Tsohou et al, 2010]. Αυτά που σχετίζονται άμεσα με την διαχείριση και την ανάλυση επικινδυνότητας πρέπει να ικανοποιούν τα εξής κριτήρια [Ionita, 2013] :

• Να περιγράφουν μια μέθοδο ανάλυσης και διαχείρισης επικινδυνότητας

• Πρέπει να περιέχουν μια ειδική μέθοδο αποτίμησης επικινδυνότητας

• Πρέπει να υπάρχει πλήρης τεκμηρίωση στα Αγγλικά

• Πρέπει να χρησιμοποιούνται σε πάνω από μία χώρες.

• Να απευθύνονται σε υπεύθυνους ασφαλείας ή σε θέσεις χρηστών που να έχουν συμμετοχή στις αποφάσεις σχετικά με τον προϋπολογισμό για την ασφάλεια.

Τα πρότυπα που πληρούν και τα 5 κριτήρια είναι τα: **ISO/IEC 27002** και **27005**.

Υποστηρίζουν την βασική ορολογία της ανάλυσης και διαχείρισης επικινδυνότητας και παρέχουν τις βασικές αρχές για την υλοποίηση μίας μεθόδου διαχείρισης επικινδυνότητας [Tsohou et al, 2010].

1.4.1 ISO/IEC 27002

ISO/IEC 27002:2013

Το πρότυπο ISO/IEC 27002 προέρχεται από το πρότυπο BS7799, το οποίο ενσωματώθηκε στο πρότυπο ISO/IEC 17799 και έτσι προέκυψε η ονομασία του.

Στόχος του είναι να το χρησιμοποιούν οι οργανισμοί ως σημείο αναφοράς για τον καθορισμό και την εφαρμογή ελέγχων για την αντιμετώπιση κινδύνων ασφάλειας πληροφοριών, σε ένα σύστημα διαχείρισης ασφάλειας πληροφοριών (ISMS) που βασίζεται στο ISO/IEC 27001.

Επιπλέον, προορίζεται για χρήση στην ανάπτυξη κατευθυντήριων γραμμών διαχείρισης ασφάλειας πληροφοριών για τον κλάδο και τον οργανισμό, λαμβάνοντας υπόψη το συγκεκριμένο περιβάλλον κινδύνου ασφάλειας πληροφοριών.

Το πρότυπο περιγράφει μια σειρά από **14 διατάξεις ασφαλείας**. Για κάθε διάταξη υπάρχει και μια σειρά από υποκατηγορίες για τις οποίες ορίζονται οι στόχοι του ελέγχου καθώς και κατευθυντήριες γραμμές για την εφαρμογή τους. Επίσης το πρότυπο δίνει μερικές προτάσεις βέλτιστων πρακτικών για τη διεξαγωγή μιας επίσημης αποτίμησης επικινδυνότητας καθώς και τρόπους μετρίασης της.

Control Groups	
5. Policies	12. Operations
6. Organisation	13. Communications
7. Human resources	14. Dev and maintenance
8. Asset management	15. Suppliers
9. Access Control	16. Incidents
10. Cryptography	17. Business Continuity
11. Physical	18. Compliance

Εικόνα 3. Διατάξεις Ασφάλειας [ISO 27002:2013]

https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/NQA-Webinar-A-guide-to-the-changes-to-ISO-27002.pdf

Πλεονεκτήματα ISO/IEC 27002:

• Υποστηρίζεται από μια εκτενή ταξινομία, εννοιολογικό μοντέλο και ένα πλαίσιο διαχείρισης επικινδυνότητας (ISO 13335).

Μειονεκτήματα:

• Περιγράφει την διαδικασία αποτίμησης της επικινδυνότητας μόνο σε υψηλό επίπεδο,

• Επικεντρώνεται κυρίως σε ελέγχους και αντιμετώπιση επικινδυνότητας αντί σε αναγνώριση και ανάλυση επικινδυνότητας,

• Λόγω αυτού, χρειάζεται να συνδυαστεί μαζί με μια μέθοδο αποτίμησης επικινδυνότητας η οποία καλύπτει την ανάλυση και αναγνώριση με λεπτομέρεια, ώστε τα αποτελέσματα να γίνουν κατανοητά από τη διοίκηση του οργανισμού.

ISO/IEC 27002:2022

Διαφορές μεταξύ της έκδοσης 2013 και της νέας 2022

https://msecb.com/iso-270022022-what-has-been-updated-and-what-is-new/

Οι διαφορές μεταξύ της παλαιότερης έκδοσης και της πρόσφατα δημοσιευμένης ξεκινούν με τον τίτλο του προτύπου και συνεχίζονται με τον αριθμό των στοιχείων ελέγχου, τα θέματα και την εισαγωγή χαρακτηριστικών.

- **Τίτλος Προτύπου**

ISO/IEC 27002:2013 Τεχνολογία πληροφοριών — Τεχνικές ασφάλειας — Κώδικας πρακτικής για ελέγχους ασφάλειας πληροφοριών.

ISO/IEC 27002:2022 Ασφάλεια πληροφοριών, κυβερνοασφάλεια και προστασία της ιδιωτικής ζωής — Έλεγχοι ασφάλειας πληροφοριών.

Αντικατοπτρίζει την ευρεία πρόθεση εντοπισμού, πρόληψης και αντίδρασης σε κυβερνοεπιθέσεις και προστασίας δεδομένων γενικά.

- **Στοιχεία Ελέγχου**

Η έκδοση του 2013 αποτελούνταν από 114 στοιχεία ελέγχου, ενώ η έκδοση του 2022 έχει συνολικά 93. Ορισμένα στοιχεία ελέγχου έχουν ενημερωθεί ή συγχωνευθεί, αλλά κανένα από τα στοιχεία ελέγχου δεν έχει διαγραφεί και έχουν προστεθεί 11 νέα στοιχεία ελέγχου.

Για την καλύτερη κατανομή των ευθυνών εντός του οργανισμού για τη βελτίωση της ασφάλειας των πληροφοριών και την απλούστευση της εφαρμογής, ο αριθμός των ομάδων ελέγχου μειώθηκε από 14 σε 4 κατηγορίες:

Control Groups	
5. Policies	12. Operations
6. Organisation	13. Communications
7. Human resources	14. Dev and maintenance
8. Asset management	15. Suppliers
9. Access Control	16. Incidents
10. Cryptography	17. Business Continuity
11. Physical	18. Compliance

Theme clauses	
5. Organisational	7. Physical
6. People	8. Technology

Εικόνα 4. ISO 27002:2013 --> 2022

https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/NQA-Webinar-A-guide-to-the-changes-to-ISO-27002.pdf

Στις παρακάτω κατηγορίες:

- **Οργανωτική**
- **Άτομα**
- **Φυσική**
- **Τεχνολογικά**

Η εισαγωγή χαρακτηριστικών στο νέο πρότυπο ISO/IEC 27002:2022 το καθιστούν πιο βολικό στη χρήση από οργανισμούς. Συνδέονται με συγκεκριμένους ελέγχους για την καλύτερη κατανόηση και ταξινόμηση και την εφαρμογή των ελέγχων από τις επιχειρήσεις.

1.4.2 ISO/IEC 27005

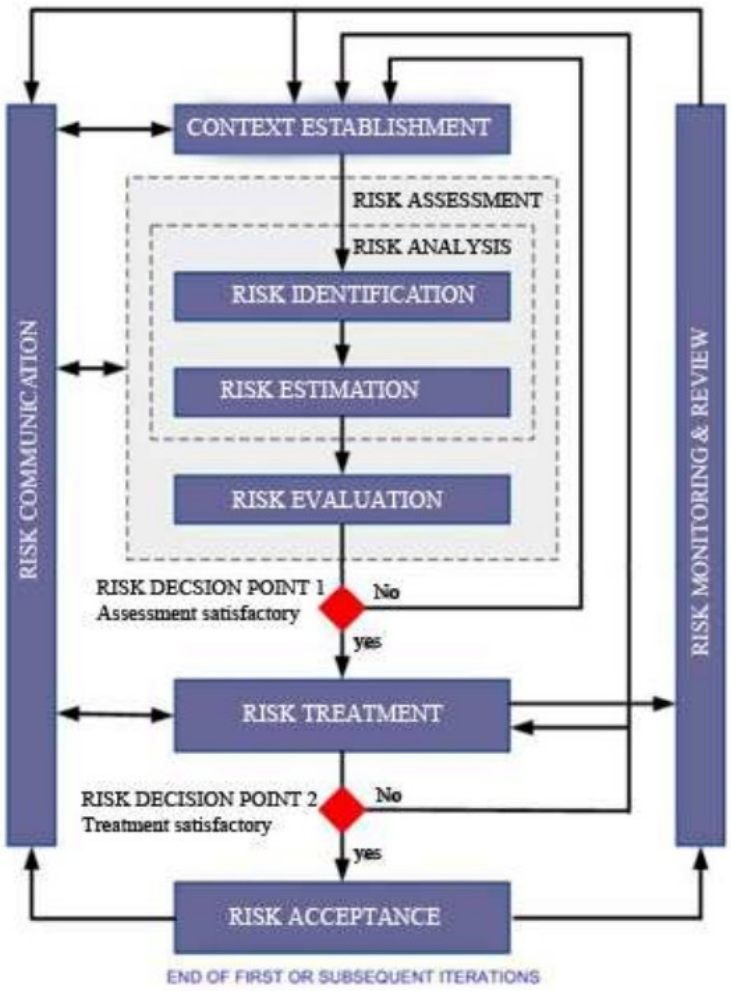
ISO/IEC 27005:2018

https://www.iso.org/standard/80585.html

Το πρότυπο ISO / IEC 27005 συντάχθηκε και δημοσιεύθηκε από το Διεθνή Οργανισμό Τυποποίησης (ISO) και τη Διεθνή Ηλεκτροτεχνική Επιτροπή (IEC).

Το πρότυπο ISO 27005 είναι μία δομημένη, συστηματική και αυστηρή διαδικασία αποτίμησης επικινδυνότητας που λαμβάνει υπόψη όλες τις οργανωτικές πτυχές (ανθρώπους, διαδικασίες και τεχνολογία).

Παρόλα αυτά όμως δεν παρέχει ή συνιστά μια συγκεκριμένη μέθοδο χαμηλού επιπέδου με τις τεχνικές λεπτομέρειες για τη διεξαγωγή αυτής της δραστηριότητας. Δεν περιέχει την ποιοτική ή ποσοτική προσέγγιση, απλά δίνει προτάσεις για εφαρμογή και το πεδίο εφαρμογής της κάθε προσέγγισης. Το πρότυπο είναι προσανατολισμένο σε υψηλού επιπέδου τεχνικές διαχείρισης.



Εικόνα 5. [ISO/IEC. ISO 27005 information technology security techniques information security risk management, 2008]

ISO/IEC. Iso 27005 information technology security techniques information security risk management 2008

ISO 27005:2022

Οι βασικές αλλαγές της νέας έκδοσης είναι οι εξής:

https://www.linkedin.com/pulse/isoiec-270052022-what-new-paul-varela?trk=pulse-article

- όλος ο οδηγός και η ορολογία έχει ευθυγραμμιστεί με το ISO/IEC 27001 και το ISO 31000:2018.
- η δομή των όρων έχει προσαρμοστεί στη διάταξη του ISO/IEC 27001
- (αντίκτυπος → συνέπεια)
- ο ορισμός του σεναρίου κινδύνου και οι σχετικές έννοιες, αντί του σενάριο συμβάντος.
- Η νέα προσέγγιση **βάσει συμβάντων** έρχεται σε αντίθεση με την προσέγγιση που βασίζεται σε περιουσιακά στοιχεία για τον προσδιορισμό του κινδύνου. Είναι ίσως η πιο σημαντική αλλαγή στο πρότυπο.

- Έχει εισαχθεί ένα κριτήριο ενεργοποίησης για να διατηρείται μια ενημερωμένη και δυναμική εκτίμηση.
- Εστιάζει στην παρακολούθηση των σεναρίων κινδύνου (σύνδεση με το ISO 27035 και SOC/SIEM).
- Παρέχουν τεχνικές υλοποίησης σε αυτά που προσαρτώνται.
- Τονίζετε η εκμετάλλευση των τρωτών σημείων στο πλαίσιο της προσέγγισης που βασίζεται σε περιουσιακά στοιχεία. Θα μπορούσε να γίνει αντιστοίχιση με τα CVE σε επιχειρησιακά σενάρια.

- **Τίτλος Προτύπου**

Τεχνολογία πληροφοριών , Τεχνικές ασφάλειας , Διαχείριση κινδύνου ασφάλειας πληροφοριών → Ασφάλεια πληροφοριών, κυβερνοασφάλεια και προστασία της ιδιωτικής ζωής.

- **Incident scenario vs Risk scenario**

Κατά ISO27005:2018 αναφερόταν σε **σενάριο περιστατικού** ενώ στην νέα έκδοση σε **σενάριο κινδύνου**.

Ορίζεται ως μια “ακολουθία ή συνδυασμός γεγονότων που οδηγεί από την αρχική αιτία στην ανεπιθύμητη συνέπεια” που πρέπει να ευθυγραμμιστεί με το ISO 17666:2016.

*Πλεονεκτήματα***:**

• Υποστηρίζεται από μια εκτενή ταξινομία, εννοιολογικό μοντέλο και ένα

πλαίσιο διαχείρισης επικινδυνότητας (ISO 13335, 2700x, 31000).

• Ευελιξία στην επιλογή συμπληρωματικών μεθόδων αποτίμησης

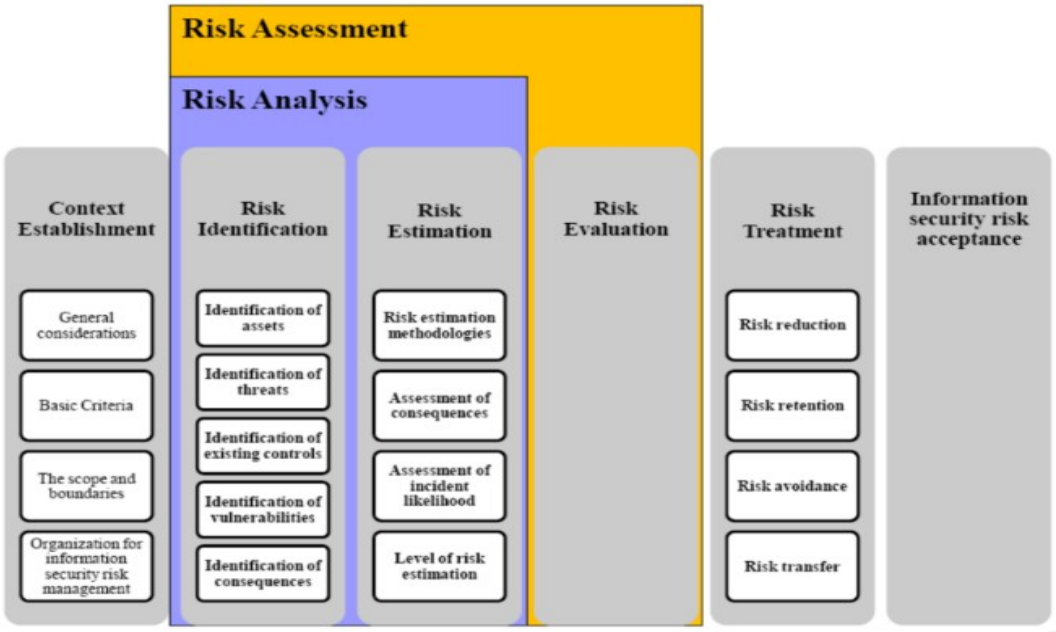
επικινδυνότητας χαμηλού επιπέδου

Μειονεκτήματα:

• Περιγράφει την διαδικασία αποτίμησης της επικινδυνότητας σε αφαιρετικό επίπεδο,

• Χρειάζεται να χρησιμοποιηθεί μαζί με μια εξωτερική μέθοδο αποτίμησης επικινδυνότητας ώστε να γίνουν τα αποτελέσματα της κατανοητά και στη διοίκηση,

• Δεν περιγράφει μια συγκεκριμένη μέθοδο ανάλυσης επικινδυνότητας, αλλά προσφέρει γενικές συμβουλές για την επιλογή και τη χρήση τέτοιων μεθόδων.



Εικόνα 6. Risk Assessment 2013 [Δούσκας Θ. κατά ISO 27005:2018]

Για την Ανάλυση και Διαχείριση Επικινδυνότητας των ΠΣ του Νοσοκομείου χρησιμοποιήθηκε η μέθοδος Magerit.
Μας παραχωρήθηκε ειδική άδεια για την πλήρη χρήση του εργαλείου EAR/PILAR RM, από τον διαχειριστή κ. J. Mañas, μετά την επικοινωνία της επιβλέπουσας κα Καρύδα για ακαδημαϊκούς σκοπούς.

License

2. ΑΝΑΛΥΣΗ Magerit

Η Μέθοδος

https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ramethodsm_magerit.html
(Κάτσικας, 2014)

Η μέθοδος MAGERIT [Crespo .F et al, 2007] είναι μια μεθοδολογία Ανάλυσης και Διαχείρισης Κινδύνου που αναπτύχθηκε το 1997 από το ανώτατο Ισπανικό συμβούλιο για την Ηλεκτρονική διακυβέρνηση (Consejo Superiorde Administración Electrónica).

Ο λόγος επιλογής της μεθόδου είναι ότι σχετίζεται άμεσα με τη γενικευμένη χρήση των ηλεκτρονικών μέσων. Με την χρήση αυτών πρέπει να δημιουργούνται οφέλη, αλλά ταυτόχρονα υπόκεινται σε απειλές και κινδύνους που πρέπει να ελαχιστοποιηθούν με την εφαρμογή αντιμέτρων. Με τον τρόπο αυτό, επιτυγχάνεται η εμπιστοσύνη στη χρήση των μέσων.

Κατά την ορθή εφαρμογή της μεθόδου Magerit επιτυγχάνονται τα παρακάτω:

• Να αντιληφθούν οι υπεύθυνοι την ύπαρξη απειλών, κινδύνων και η ανάγκη έγκαιρης αντιμετώπισής τους.

• Να προσφερθεί μια συστηματική μέθοδο ανάλυσης των κινδύνων.

• Να περιγραφούν και να παρθούν τα κατάλληλα μέτρα ελέγχου της επικινδυνότητας.

• Να προετοιμάσει τον οργανισμού για: διαδικασία αξιολόγησης (evaluation), ελέγχου (audit) και πιστοποίησης (certification).

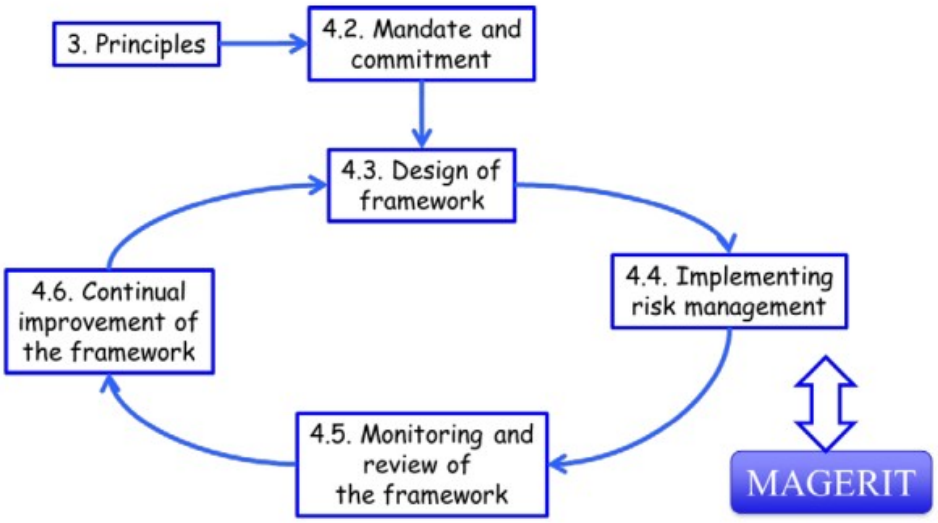
• Τα ευρήματα και τα συμπεράσματα της ανάλυσης και διαχείρισης κινδύνου παρατίθενται σε αναφορές με όμοια δομή.

Το εργαλείο της μεθόδου Magerit είναι το EAR/Pilar. Μέσω αυτού ελέγχετε η ορθή εφαρμογή της μεθόδου βήμα-βήμα, και αποθηκεύονται και ενημερώνονται όλα τα στοιχεία που συλλέγονται κατά την εφαρμογή της. Το εργαλείο παρουσιάστηκε το 2004 και υποστηρίζεται από τον A.L.H.J.Mañas (EAR/Pilar, 2014).

2.1 Περιγραφή Magerit

https://www.sciencedirect.com/science/article/abs/pii/S0950705114000732

Η MAGERIT εφαρμόζει τη Διαδικασία Διαχείρισης Κινδύνων για τη λήψη αποφάσεων από τα διοικητικά όργανα λαμβάνοντας υπόψη τους κινδύνους που προκύπτουν από τη χρήση των τεχνολογιών της πληροφορίας.



Εικόνα 7.Διαδικασία Διαχείρισης Κινδύνου[ISO 31000]

Τα βήματα της μεθόδου περιγράφονται στην βιβλιογραφία (*MAGERIT - Methodology for Information Systems Risk Analysis and Management: Book I – The Method*, (περιλαμβάνει τα βασικά βήματα για την ανάλυση και διαχείριση κινδύνου, την περιγραφή της διαδικασίας και την εφαρμογή της σε πληροφοριακά συστήματα) - *Book II – The Elements, (περιλαμβάνει τα κριτήρια και τις πληροφορίες για την μοντελοποίηση των πληροφοριακών συστημάτων και κινδύνων) - Book III – The Techniques (περιγράφει τις ενέργειες για την ανάλυση και διαχείριση κινδύνων)*. [Κάτσικας, 2014].

Ο Υπολογισμός του Κινδύνου κατά MAGERIT:

Κίνδυνος (Απειλή, Περιουσιακό Στοιχείο) **= Πιθανότητα** (Συμβάντος) **Χ Συνέπειες** (Περιστατικό, Περιουσιακό Στοιχείο)

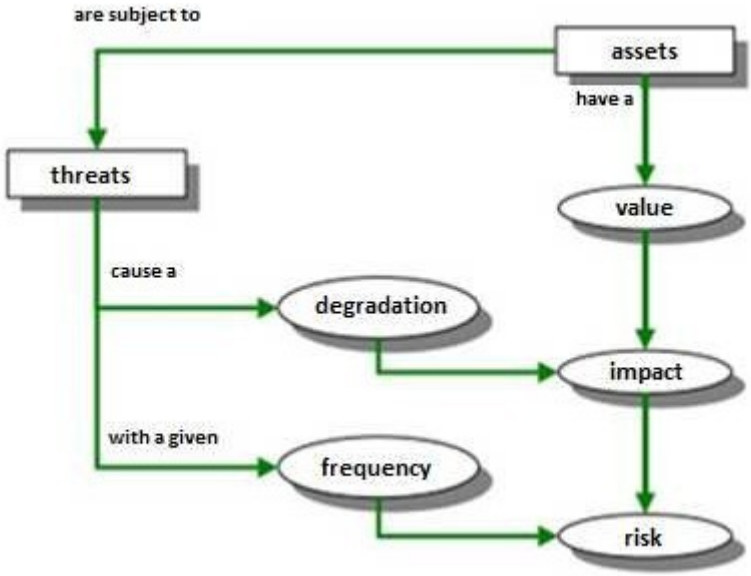
Κατά την έναρξη της μελέτης και κατά την πρώτη συνεδρίαση της ομάδας με τα αρμόδια στελέχη του οργανισμού θα πρέπει:

- Να προσδιοριστούν τα όρια της μελέτης.
- Να προσδιοριστούν οι χρήστες των δεδομένων και τα πρόσωπα που θα συνεργαστούν.
- Να δοθεί εξουσιοδότηση για άντληση στοιχείων και διεξαγωγή των συνεντεύξεων.
- Να προσδιοριστεί το χρονοδιάγραμμα και το σχέδιο διεξαγωγής της μελέτης.

2.2 Ανάλυση Κινδύνου κατά Magerit

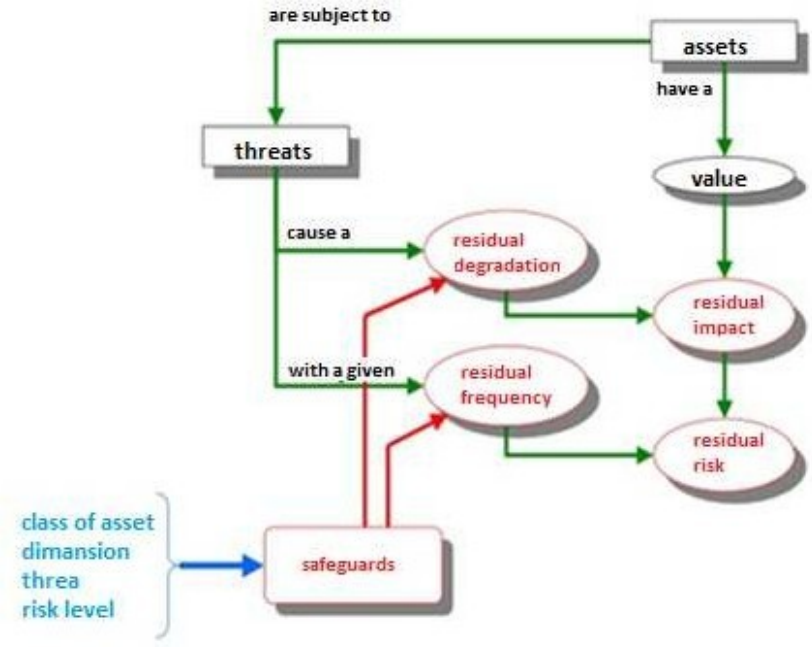
Για την εκτίμηση του κινδύνου, ακολουθούνται τα παρακάτω βήματα:

1. Προσδιορισμός των σχέσεων μεταξύ των αγαθών του οργανισμού και της αξίας τους
2. Προσδιορισμός των απειλών στις οποίες εκτίθενται τα αγαθά.
3. Προσδιορισμός των μέτρων προστασίας (safeguards) που υπάρχουν και πόσο αποτελεσματικά είναι έναντι του κινδύνου.
4. Εκτίμηση της επίπτωσης, (η ζημιά που μπορεί να συμβεί στο αγαθό ως αποτέλεσμα μιας απειλής).
5. Εκτίμηση της επικινδυνότητας, (η βαρύνουσα επίπτωση στο ποσοστό ή την προσδοκία της εμφάνισης της απειλής).



Εικόνα 8. Βήματα Magerit χωρίς safeguards

Αρχικά εκτελούνται τα βήματα 1, 2, 4 και 5, όπου δεν έχουν συνυπολογιστεί τα μέτρα προστασίας και οι εκτιμήσεις των επιπτώσεων και των κινδύνων να είναι δυνητικές.



Εικόνα 9. Βήματα Magerit με safeguards

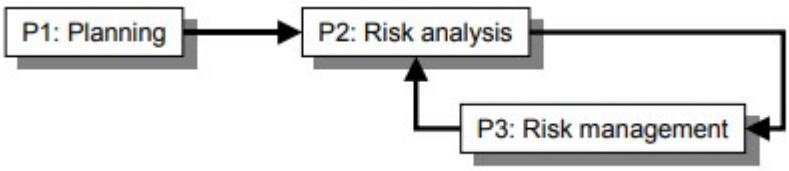
Μόλις ολοκληρωθεί αυτό το θεωρητικό σενάριο, τα μέτρα ασφάλειας λαμβάνονται υπόψη στο βήμα 3 που παρακάμφθηκε, παρέχοντας πλέον μία ρεαλιστική εκτίμηση της επίπτωσης των απειλών και του κίνδυνου. Στη συνέχεια, εκτελούνται εκ νέου τα βήματα 4 και 5.

Οι **τρεις βασικές διαδικασίες**(εικόνα κάτω) του έργου ανάλυσης και διαχείρισης κινδύνου ενσωματώνουν τα πέντε παραπάνω λειτουργικά βήματα:

1. Προετοιμασία και προγραμματισμός έργου *(Preparation & **Planning** of implementation)*.
2. Ανάλυση επικινδυνότητας *(**Risk analysis**)*.
3. Διαχείριση επικινδυνότητας *(**Risk management**)*.

Στη 1η διαδικασία, της προετοιμασίας του έργου, θα πραγματοποιηθεί η ενεργοποίηση του έργου ανάλυσης και διαχείρισης κινδύνου.

Στη 2η και 3η διαδικασία πραγματοποιεί μια συνεχή ανατροφοδότηση όπου η ανάλυση επικινδυνότητας υποστηρίζει τη διαχείριση επικινδυνότητας,



Εικόνα 10.Διαχείριση κινδύνου Magerit[Book III]

Κάθε διαδικασία εκτελείται με συγκεκριμένα βήματα. Τα οποία θα παρουσιαστούν στην ενότητα 2.3 που ακολουθεί.

2.3 Διαδικασίες και βήματα της Magerit και του EAR/Pilar

Διαδικασίες	***Βήματα***
1. Προετοιμασία και προγραμματισμός έργου (Preparation & Planning of implementation)	*Βήμα 1*: Μελέτη σκοπιμότητας *Βήμα 2*: Προσδιορισμός πλαισίου έργου *Βήμα 3*: Προγραμματισμός έργου *Βήμα 4*: Έναρξη έργου
2. Ανάλυση επικινδυνότητας *(Risk analysis)*	*Βήμα 1:* Χαρακτηρισμός Αγαθών *Βήμα 2:* Χαρακτηρισμός και Αποτίμηση Απειλών *Βήμα 3:* Προσδιορισμό Αντιμέτρων *Βήμα 4:* Εκτίμηση Επικινδυνότητας
3. Διαχείριση επικινδυνότητας *(Risk management)*	*Βήμα 1*: Λήψη αποφάσεων *Βήμα 2*: Σχέδιο ασφάλειας *Βήμα 3*: Υλοποίηση σχεδίου ασφάλειας

Πίνακας 1 : Διαδικασίες και βήματα της Magerit και του EAR/Pilar

2.3.1 Διαδικασία 1: Προετοιμασία και Προγραμματισμός Έργου

Στην πρώτη φάση τίθεται ένα πλαίσιο σχετικά με τη συλλογή της απαραίτητης πληροφορίας, την εμπλοκή των της διοίκησης και το σχεδιασμό του έργου.

Βήμα 1: *Μελέτη σκοπιμότητας*.

Περιγράφεται η μελέτη σκοπιμότητας, όπου υπολογίζονται τα προβλήματα και τα πιθανά οφέλη που θα προκύψουν από την υλοποίηση ενός έργου ανάλυσης και διαχείρισης επικινδυνότητας για τον οργανισμό. Προκύπτει μια προκαταρκτική έκθεση, περιλαμβάνοντας τις ενέργειες προετοιμασίας για την διεξαγωγή του έργου.

Βήμα 2: *Προσδιορισμός πλαισίου έργου*.

Ακολουθεί ο καθορισμός του πλαισίου του έργου. Καθορίζονται οι στόχοι του έργου, οι περιορισμοί (π.χ. γεωγραφικοί, χρονικοί, λειτουργικοί κ.ά.) και το κόστος που απαιτείτε.

Βήμα 3: *Προγραμματισμός έργου*.

Έπειτα ακολουθεί ο προγραμματισμός του έργου. Δημιουργείτε το πλάνο των συνεντεύξεων για τη συλλογή πληροφοριών, ποια άτομα θα συμμετέχουν στη διαχείριση και υλοποίηση του έργου και ορίζονται τα καθήκοντά τους. Τέλος, καθορίζεται το χρονοδιάγραμμα του έργου και η διαχείριση των συλεχθέντων πληροφοριών.

Βήμα 4: *Έναρξη έργου*.

Συντάσσονται τα ερωτηματολόγια για τη συλλογή των απαραίτητων πληροφοριών και το πλάνο συνεντεύξεων, δημιουργείται ένας κατάλογος με τα αγαθά που πρέπει να προστατευθούν και προσδιορίζονται τα κριτήρια εκτίμησης τους. Τέλος, γίνεται καθορισμός των πόρων που απαιτούνται για τη υλοποίηση του έργου, και ταυτόχρονα κοινοποιείται σε όλους τους εμπλεκόμενους το πλάνο.

2.3.2 Διαδικασία 2: Ανάλυση Επικινδυνότητας

Αυτή η διαδικασία είναι η κρισιμότερη, καθώς κρίνεται η εγκυρότητα και η αποτελεσματικότητα ολόκληρου του έργου. Περιλαμβάνονται ο εντοπισμός, η εκτίμηση των περιουσιακών στοιχείων και τυχόν απειλών.

Βήμα 1: *Αναγνώριση και Αποτίμηση Αγαθών***.**

Στο βήμα αυτό, τα αγαθά, αναγνωρίζονται, συσχετίζονται και ταξινομούνται σύμφωνα με όσα δεδομένα έχουμε συλλέξει στη προηγούμενη διαδικασία. Τέλος γίνεται αποτίμησή σε αυτά.

Βήμα 2: *Χαρακτηρισμός και Αποτίμηση Απειλών.*

Στο βήμα αυτό αναγνωρίζονται οι απειλές που αφορούν το κάθε αγαθό και κατηγοριοποιούνται με βάση την συχνότητα που μπορεί να εμφανιστούν και το μέγεθος της ζημιάς που μπορούν να προκαλέσουν.

ΚΑΤΗΓΟΡΙΕΣ ΑΠΕΙΛΩΝ	
Φυσικές καταστροφές (Γεγονότα που μπορεί να συμβούν χωρίς να προκαλούνται άμεσα ή έμμεσα από ανθρώπους).	Σεισμοί, Πλημμύρες.
Καταστροφές βιομηχανικής προέλευσης (Γεγονότα που μπορεί να συμβούν από ανθρώπινη δραστηριότητα βιομηχανικού τύπου. Τυχαία ή εσκεμμένα).	Ρύπανση, Μόλυνση, Ηλεκτρικές βλάβες.
Λάθη ή Ακούσιες αποτυχίες (Ακούσιες αστοχίες που προκαλούνται από άτομα).	User errors, Administrator errors.
Ηθελημένες επιθέσεις (Σκόπιμες αστοχίες που προκαλούνται από άτομα).	Manipulation of the configuration, Masquerading of user identity.

Πίνακας 2 : Κατηγοριοποίηση απειλών στη μέθοδο Magerit

Βήμα 3: *Χαρακτηρισμός Αντιμέτρων.*

Στο βήμα αυτό εξετάζονται τα ήδη υπάρχοντα μέτρα και αξιολογούνται με βάση τη αποτελεσματικότητά τους. Αυτό επιτυγχάνεται με την διεξαγωγή συνεντεύξεων και συμπλήρωση ερωτηματολογίων από τα κατάλληλα άτομα.

Βήμα 4: *Εκτίμηση Επικινδυνότητας.*

Στο βήμα αυτό γίνεται εκτίμηση της ενδεχόμενης και εναπομένουσας επίπτωσης για το σύστημα που εξετάζεται. Παράλληλα, ταξινομούνται τα αγαθά, σε βαθμό κρισιμότητας της επίπτωσης ή της επικινδυνότητας. Η μέθοδος, υπολογίζει την εναπομένουσα (residual) επικινδυνότητα συνυπολογίζοντας τη συσσωρευμένη (accumulated) και την αποκλίνουσα (deflected) επικινδυνότητα. Η κλίμακα που χρησιμοποιείται για την αποτίμηση τόσο της επικινδυνότητας όσο και της επίπτωσης παίρνει τιμές από το 0 – 9 και μπορεί να γίνει είτε ποιοτικά είτε ποσοτικά.

2.3.3 Διαδικασία 3: Διαχείριση Επικινδυνότητας

Οι κίνδυνοι αξιολογούνται με βάση: εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα, αυθεντικότητα και υπευθυνότητα.

Για την αντιμετώπιση τους λαμβάνουμε:

- Μέτρα προστασίας
- Πολιτικές
- Διαδικασίες

και αξιολογείται ο εναπομείναντας κίνδυνος.

Η διαχείριση επικινδυνότητας μπορεί να οριστεί ως η διαδικασία μείωσης της πιθανότητας ύπαρξης ανεπιθύμητων συνεπειών σε ένα έργο από το στάδιο του σχεδιασμού μέχρι και την λειτουργία του. (Serpel et al., 2015).

Περιλαμβάνει τον εντοπισμό την ανάλυση την αντιμετώπιση και παρακολούθηση των κινδύνων.

Βήμα 1: *Λήψη Αποφάσεων.*

Προσδιορίζεται η τιμή της επικινδυνότητας σε κλίμακα (κρίσιμη, σοβαρή, αξιόλογη ή αποδεκτή) και αναφέρονται οι επιπτώσεις, περιλαμβάνοντας τις οδηγίες για την αντιμετώπισή τους. Θα οδηγήσει στην λήψη αποφάσεων από τη διοίκηση με σκοπό να αντιμετωπιστούν οι απειλές και να περιοριστούν οι επιπτώσεις τους.

Βήμα 2: *Προετοιμασία σχεδίου ασφάλειας.*

Για τη ανάπτυξη ενός σχεδίου ασφάλειας συνυπολογίζονται τα σενάρια στα οποία οι επιπτώσεις και η επικινδυνότητα βρίσκονται σε κρίσιμο ή σοβαρό επίπεδο. Θα δημιουργηθούν προγράμματα ασφάλειας που θα παρέχουν τρόπους αντιμετώπισής τους. Ο στόχος είναι ο καθορισμός αντιμέτρων τα οποία θα μειώσουν την επίπτωση και την επικινδυνότητα σε επίπεδα αποδεκτά από τη διοίκηση του οργανισμού.

Βήμα 3: *Υλοποίηση του σχεδίου ασφάλειας.*

Εδώ εκτελούνται όλα τα προγράμματα ασφάλειας, με σκοπό την υλοποίηση και εφαρμογή του σχεδίου ασφάλειας που έχει καθοριστεί στο προηγούμενο βήμα. Σαν αποτέλεσμα είναι ο καθορισμός αντιμέτρων, η δημιουργία KPI'S και η δημιουργία ενημερωμένων μοντέλων επικινδυνότητας.

2.4 Το Εργαλείο EAR/Pilar

Το εργαλείο EAR/Pilar [EAR/Pilar, 2014] υποστηρίζει την διαχείριση της επικινδυνότητας, ενώ ταυτόχρονα παρέχει ανάλυση καθώς αυτή υλοποιείται. Το Pilar υποστηρίζει την μεθοδολογία Magerit και ένα φάσμα προτύπων ISO. Τα πρότυπα αυτά είναι:

- 13335: 2004
- 17799: 2005
- 15408: 2005
- 27001: 2005.

Το Pilar παρέχει μια βιβλιοθήκη με περιουσιακά στοιχεία, απειλές και μέτρα προστασίας. Εξάγει μέτρα ασφαλείας κοινά με τα γνωστά πρότυπα ασφαλείας, όπως π.χ ISO/IEC 27002:2013.

Τα εργαλεία μπορούν να εκτιμήσουν τον κίνδυνο για ένα σύστημα εάν μπορέσουμε να υπολογίσουμε την συχνότητα που εμφανίζονται οι απειλές σε αυτό.

Ο αντίκτυπος αφορά το κόστος που προκύπτει αν για κάποιο αγαθό υποβαθμιστεί η αξία του αφού έχει εκτεθεί σε κάποια απειλή.

Σαν αποτέλεσμα με βάση τα παραπάνω, με τον υπολογισμό της συχνότητας και της υποβάθμισης του συστήματος, εκτιμάτε η ευπάθεια του.

Με βάση τα μέτρα ασφαλείας που θα παρθούν για συχνότητα εμφάνισης ή τον αντίκτυπο προκύπτει ο υπολειπόμενος κίνδυνος για το σύστημα μας.

Κατά την αρχική οθόνη του εργαλείου ο αναλυτής καλείται να επιλέξει αν θα ασχοληθεί με μελέτη επικινδυνότητας ή με μελέτη επιχειρησιακής συνέχειας. Επίσης δίνεται η επιλογή ποσοτικής ή ποιοτικής ανάλυσης για καθεμιά από τις προηγούμενες περιπτώσεις μελετών.

2.4.1. Αγαθά

Στο εργαλείο Pilar γίνεται χρήση **layers** για το διαχωρισμό των αγαθών σε κατηγορίες. Με αυτό επιτυγχάνει την εξάρτηση και τις συσχετίσεις μεταξύ των διαφορετικών ομάδων αγαθών. Τα layers ταυτίζονται με τις 9 κατηγορίες αγαθών, που ορίζονται από τη μέθοδο Magerit.

Τα προτεινόμενα **layers** κατά το Pilar είναι τα εξής:

- Essential layer [B]
- Internal services [IS]
- Equipment [E]
- Subcontracted services [SS]
- Facilities [L]
- Personnel [P]

Στην παρούσα μελέτη θα ακολουθηθεί η **κατηγοριοποίηση** των αγαθών κατά Magerit:

Κατηγορίες αγαθών	
1. Υπηρεσίες (Services)	6. Φυσικά Μέσα Αποθήκευσης (Media)
2. Δεδομένα/Πληροφορία (Data/Information)	7. Βοηθητικός Εξοπλισμός (Auxiliary equipment)
3. Εφαρμογές (Applications/Software)	8. Εγκαταστάσεις Εξοπλισμού (Installations)
4. Εξοπλισμός (Computer Equipment/Hardware)	9. Προσωπικό (Personel)
5. Δίκτυα Επικοινωνιών (Communication networks)	

Πίνακας 3 : Κατηγοριοποίηση αγαθών Magerit

Χρησιμοποιείται το “Μοντέλο Εξάρτησης Αγαθών” (Asset Dependency Model). Αυτό μπορεί να γίνει είτε απευθείας μέσω του εργαλείου είτε μέσω της εισαγωγής ειδικού XML αρχείου.

Σημαίνει ότι, ένα αγαθό με μεγαλύτερη αξία, εξαρτάται από ένα χαμηλότερης αξίας, όταν μια απειλή που πλήξει το χαμηλότερο σε αξία αγαθό θα έχει επίπτωση σε αυτό με την υψηλότερη αξία.

Αφού τα αγαθά αναγνωριστούν και κατηγοριοποιηθούν, κατά τη Magerit ακολουθεί η αποτίμηση αυτών.

2.4.2 Αποτίμηση Αγαθών

Κατά την Magerit προσφέρεται, ποιοτική ή ποσοτική ανάλυση και μπορεί να επιλεχθεί ανάλογα από τον υπεύθυνο της μελέτης. Σε κάθε μοντέλο, η επίπτωση υπολογίζεται βάσει της τιμής του αγαθού στις 3 βασικές αρχές της ασφάλειας **C.I.A.** αλλά και με ακόμα 2 την Authenticity και Accountability. (Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα, Απονομή Ευθυνών, Αυθεντικοποίηση).

2.4.3 Εκτίμηση απειλών

Περιέχονται εξειδικευμένα είδη απειλών όπως το malware diffusion αλλά και πιο γενικού περιεχομένου όπως η κοινωνική μηχανική (social engineering). Ορίζετε μια αρχική τιμή της επίπτωσης κάθε απειλής, όπου στην συνέχεια δίνεται η δυνατότητα επεξεργασίας της. Έτσι προσεγγίζει την πιθανότητα ύπαρξης μιας απειλής μέσα από διαφορετικές οπτικές γωνίες (πιθανότητα εμφάνισης, δυνητικότητα, ευκολία, επίπεδο, συχνότητα) και δίνει τη δυνατότητα επέκτασης της βάσης δεδομένων των ευπαθειών με XML αρχεία με τα πρόσφατα CVEs.

2.4.4 Αναγνώριση και Αποτίμηση απειλών

Κατηγορίες Απειλών Magerit και Pilar:

[N] Φυσικές καταστροφές (Natural Disasters)

[I] Καταστροφές βιομηχανικής προέλευσης (Of Industrial Origin)

[E] Λάθη ή ακούσιες αποτυχίες (Errors and unintentional failures)

[A] Ηθελημένες επιθέσεις (Wilful attacks)

[PR] Κίνδυνοι ιδιωτικότητας (Privacy risks)

Στο εργαλείο Pilar η ευπάθεια προσδιορίζεται σε 3-βάθμια κλίμακα "Low", "Medium" ,"High". Επίσης δίνονται κάποιες προκαθορισμένες τιμές αποτίμησης, από τα αρχεία TSV (Threat Standard Values). Αυτά περιέχουν καταλόγους με τις απειλές και τις τιμές τους ανά κατηγορία αγαθού.

Κριτήρια άθροισης επικινδυνότητας.

- Η αποκλίνουσα επικινδυνότητα για διαφορετικά αγαθά μπορεί να αθροιστεί
- Η συσσωρευμένη επικινδυνότητα αγαθών που δεν αλληλεξαρτώνται και δεν έχουν εξάρτηση σε κοινό αγαθό υψηλότερου επιπέδου μπορεί να αθροιστεί.
- Η συσσωρευμένη επικινδυνότητα για τα αγαθά που δεν είναι ανεξάρτητα μεταξύ τους, δεν πρέπει να αθροίζεται καθώς αυτό θα συνεπάγεται την υπερτίμηση της επικινδυνότητας, συμπεριλαμβάνοντας τη συσσωρευμένη αξία των αγαθών υψηλότερου επιπέδου αρκετές φορές.
- Η επικινδυνότητα των διαφόρων απειλών για το ίδιο αγαθό μπορεί να αθροιστεί, αν και είναι χρήσιμο να εξεταστεί σε ποιο βαθμό οι διάφορες απειλές είναι ανεξάρτητες μεταξύ τους ή και παράλληλες.
- Η επικινδυνότητα μιας απειλής σε διαφορετικές διαστάσεις, μπορεί να αθροιστεί.

Οι στόχοι της αποτίμησης των απειλών είναι:

• Εκτίμηση της πιθανότητας να πραγματοποιηθεί μια απειλή ενός αγαθού.

• Εκτίμηση της υποβάθμισης που προκαλεί μια απειλή στο αγαθό.

Επομένως, για να αξιολογηθούν οι απειλές για κάθε αγαθό πρέπει να ληφθούν υπόψη η υποβάθμιση του αγαθού και η πιθανότητα εμφάνισης της απειλής.

2.4.5 Αναγνώριση Ευπαθειών.

Ευπάθεια είναι κάθε αδυναμία που μπορεί να εκμεταλλευτεί μια απειλή ή, πιο συγκεκριμένα, οποιαδήποτε αδυναμία ενός περιουσιακού στοιχείου ή των διασφαλίσεων του που διευκολύνουν την επιτυχία μιας πιθανής απειλής.

Οι ευπάθειες μπορεί να είναι δύο ειδών:

- Τεχνικές ευπάθειες: αδυναμία ενός αγαθού. π.χ. έλλειψη ενημερωμένου λογισμικού
- Οργανωτικές ευπάθειες: αδυναμίες ελέγχου. π.χ. αδυναμία αυθεντικοποίησης του χρήστη.

Και οι δύο τύποι ανακαλύπτονται με ελέγχους, είτε με τη βοήθεια κάποιου εργαλείου σάρωσης ευπάθειας είτε χειροκίνητα.
Οι τεχνικές ευπάθειες συλλέγονται στο PILAR ως αυξημένη πιθανότητα εμφάνισης απειλής.
Τα αναγνωρίστηκαν για τα αγαθά του Νοσοκομείου εμπλουτίζοντας την βάση δεδομένων από το πιο πρόσφατο πρότυπο του NIST.[https://cve.mitre.org/]

[E] Equipment	
[SW] Applications	
[A_OS_PCs] OS Windows	
CVE-2023-21558	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVE-2023-21746	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVE-2023-21752	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H
CVE-2023-21757	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVE-2023-21758	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVE-2023-21759	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N
CVE-2023-21760	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H
CVE-2023-21765	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVE-2023-21766	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N
CVE-2023-21767	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVE-2023-21771	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

Εικόνα 11. Vulnerabilities Win 10

2.4.6 Χαρακτηρισμός αντιμέτρων Magerit.

Πραγματοποιείται εντοπισμός των ήδη υπαρχόντων αντιμέτρων, που προκύπτουν καθ' όλη τη διάρκεια της μελέτης ενώ εκτιμάται η αποτελεσματικότητα τους.

Κατά την αναγνώριση των υπαρχόντων αντιμέτρων, το εργαλείο προτείνει μια λίστα με αντίμετρα, από τα οποία θα επιλεχθούν ποία ισχύουν ή όχι, ενώ δίνεται η δυνατότητα το ίδιο το εργαλείο να προτείνει αυτόματα.

Τα αντίμετρα κατηγοριοποιούνται βάση της αποτελεσματικότητας τους και αξιολογούνται σε maturity levels(επίπεδο ωριμότητας), όπου ορίζεται η κατάσταση εφαρμογής των υπαρχόντων αντιμέτρων στις διάφορες φάσεις του έργου. Η κλίμακα αξιολόγησης που χρησιμοποιείται είναι από 0% (L0) μέχρι 100% (L5).

effectiveness	level	meaning	administrative
0%	L0	non existent	does not exist
10%	L1	initial / ad hoc	started
50%	L2	repeatable, but intuitive	partly done
90%	L3	defined process	working
95%	L4	managed and measurable	monitored
100%	L5	optimised	continuous improvement

Εικόνα 12. Maturity Level[Book II the elements]

Επίσης γίνεται διαχωρισμός των αντιμέτρων βάση 4 κατηγοριών:

ΚΑΤΗΓΟΡΙΕΣ ΑΝΤΙΜΕΤΡΩΝ
[PR] : Διαδικασίες (procedures)
[PER] : Πολιτική Προσωπικού (personnel policy)

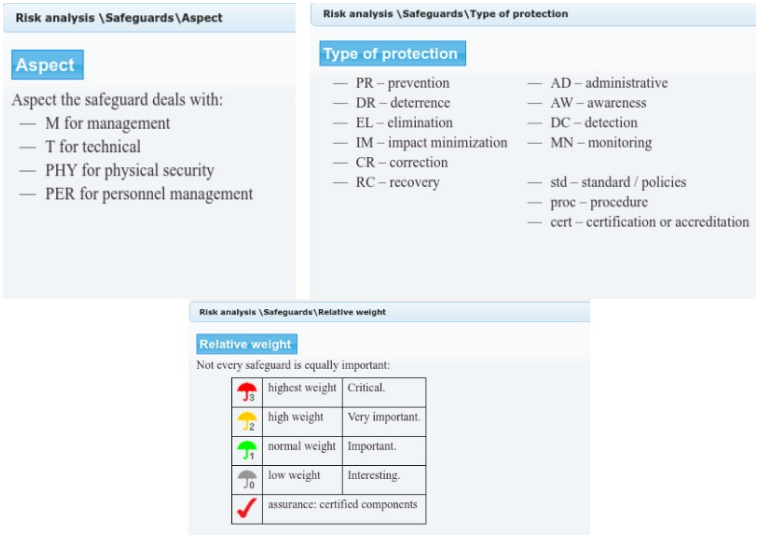
[T] : Τεχνικές Λύσεις (Technical solutions) : • [SW] : Λογισμικό (applications (software) • [HW] : Φυσικές Συσκευές (physical devices) • [COM] : Προστασία Τηλεπικοινωνιών (protection of communications)
[PHY] : Φυσική Ασφάλεια(Physical Security)

Πίνακας 4. Κατηγορίες Αντιμέτρων

Τα αντίμετρα αποτιμώνται λαμβάνοντας υπόψη:

1. Την καταλληλότητα τους για το σκοπό που υλοποιήθηκαν.
2. Την ποιότητα της υλοποίησης τους.
3. Την εκπαίδευση των υπευθύνων για τη διαμόρφωση και τη λειτουργιά τους.
4. Την εκπαίδευση των χρηστών, εφόσον αυτοί έχουν κάποιο ενεργό ρολό.
5. Την ύπαρξη μέτρων ελέγχου για τη μέτρηση της αποτελεσματικότητας τους.
6. Την ύπαρξη διαδικασιών για τακτικές αναθεωρήσεις των αντιμέτρων αυτών.

Χρησιμοποιείται διαχωρισμός των αντιμέτρων βάσει 4 κατηγοριών και ορίζεται ο τύπος προστασίας για κάθε αντίμετρο. Οι 10 τύποι προστασίας.



Εικόνα 13.Διαχωρισμός Αντιμέτρων [EAR/PILAR]

3. ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ ΓΕΝΙΚΟΥ ΝΟΣΟΚΟΜΕΙΟΥ

Το Πληροφοριακό Σύστημα του Γενικού Νοσοκομείου (ΠΣΓΝ), αφορά το σύνολο των εφαρμογών πληροφορικής έχοντας αλληλεξαρτήσεις μεταξύ τους και καλύπτοντας τις επιχειρησιακές απαιτήσεις του.

Το Νοσοκομείο διαθέτει ολοκληρωμένο πληροφοριακό σύστημα με υποσυστήματα ιατρικού και εργαστηριακού, νοσηλευτικού, διοικητικού-οικονομικού και τεχνικού.

Έχουν αναπτυχθεί μέσα σε αυτό διάφορα υποσυστήματα που το καθένα καλύπτει διαφορετικές λειτουργικές διαδικασίες μέσω ενός ενιαίου περιβάλλοντος που έχει αναπτυχθεί από τον οργανισμό εσωτερικά.

Οι περιοχές που συμπεριλαμβάνει ένα ΠΣΓΝ μπορεί να κατηγοριοποιηθούν γενικά στις παρακάτω:

– Ιατρικά Πληροφοριακά Συστήματα

– Διαχειριστικά Συστήματα ασθενών

– Διοικητικό - οικονομικά Συστήματα

Ιατρικό Υποσύστημα:

Εκτελούνται οι βασικές κεντρικές λειτουργίες διαχείρισης όπως (υποδοχή ασθενών, προγραμματισμό ασθενών), τήρηση του κατάλογου ασθενών και τον ιατρικό τους φάκελο. Επίσης διαχειρίζονται οι εργαστηριακές εξετάσεις, διαγνώσεις, κλινικών πρωτοκόλλων, ιατρικών πορισμάτων, επειγόντων περιστατικών, χειρουργείων, εξωτερικών ιατρείων, προγραμματισμένων εξετάσεων (ραντεβού), αποτελεσμάτων εξετάσεων – γνωματεύσεων, φαρμάκων. Τέλος μπορεί να γίνει επεξεργασία των στοιχείων των ασθενών, και με κατάλληλη επεξεργασία να εξαχθούν διάφοροι δείκτες.

Νοσηλευτικό Υποσύστημα:

Αφορά τη διαχείριση και την ανάπτυξη των διεργασιών των νοσηλευτικών δεδομένων, των πληροφοριών και την υποστήριξη της νοσηλευτικής πρακτικής και της νοσηλευτικής φροντίδας. Βοηθά στη διοίκηση της νοσηλευτικής υπηρεσίας, στη διαχείριση ατομικών πληροφοριών για την φροντίδα του ασθενή, στη διαχείριση πληροφοριών και την λήψη αποφάσεων για την νοσηλευτική θεραπεία που θα ακολουθηθεί.

Νοσηλευτική Υπηρεσία
– Ιατρικές Πράξεις– Ηλεκτρονικές Παραγγελίες (OrderEntry) – Διαιτολογικό
– Ιατρικά Πορίσματα

– Εξειδικευμένες εφαρμογές:

Τηλεϊατρική - Υποστήριξη σταθμών διακομιδής ασθενών

Κατ' οίκον. περίθαλψη

Εξειδικευμένες μέθοδοι θεραπείας

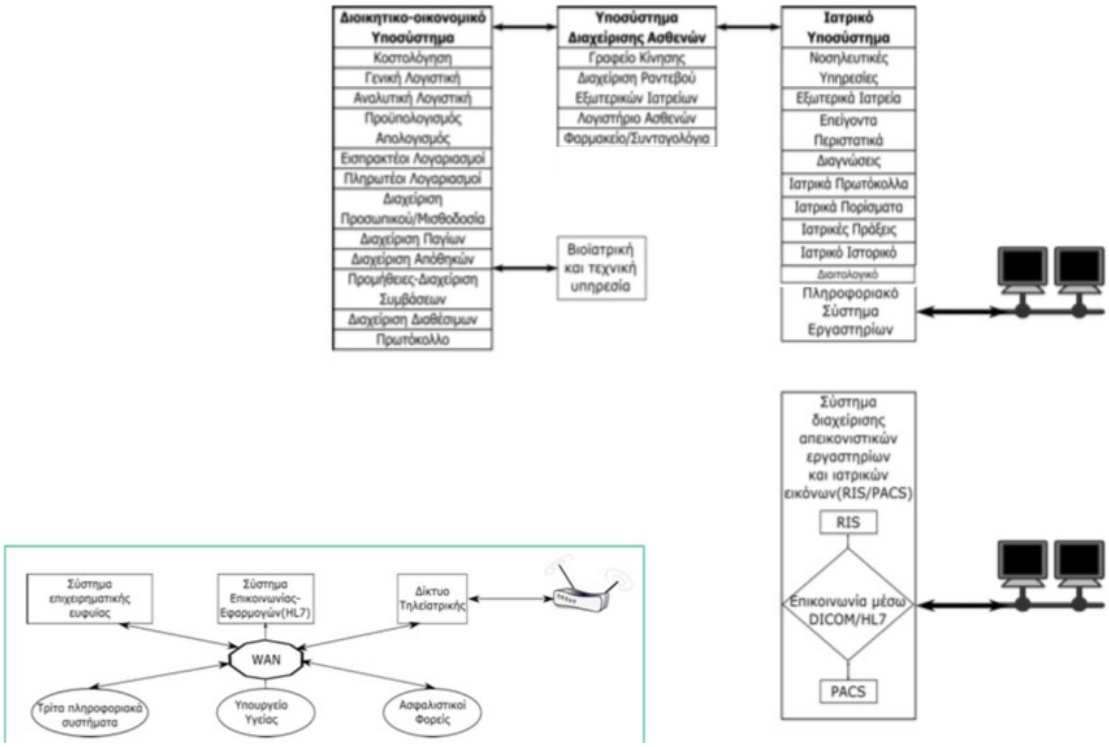
Η Πληροφορική στην Ιατρική - eHealth: Βασικές Αρχές και Εφαρμογές, Venot et all, 2019. Ηλεκτρονική Υγειά, Π. Αγγελίδης, 2015. Διαφάνειες, Συστήματα υγείας και πληροφορική, Η. Βαρλάμης

Διοικητικό - οικονομικό Υποσύστημα

- Γραφείο κίνησης - Λογιστήριο ασθενών - Διοικητική υποστήριξη , γραμματεία - Διαχείριση ανθρωπίνων πόρων - Μισθοδοσία - Λογιστήριο - Πρωτόκολλο - Διαχείριση υλικού - Προμήθειες - Αποθήκες - Τμήμα διατροφής

Υποσύστημα Διαχείρισης Ασθενών

– Γραφείο κίνησης – εξυπηρέτησης εσωτερικών ασθενών
– Διαχείριση ραντεβού – εξωτερικών απογευματινών ιατρειών – Λογιστήριο ασθενών– τιμολόγηση ιατρικών υπηρεσιών – Φαρμακείο – Συνταγολόγια.



Εικόνα 14. ΠΣ Νοσοκομείου

https://drdollah.com/hospital-information-system-his/

3.1 Χαρακτηρισμός Αγαθών

ASSET INVENTORY

Τα περιουσιακά Στοιχεία του υπό εξέταση οργανισμού (ΠΣΓΝ) θα τα κατατάξουμε στις παρακάτω βασικές κατηγορίες:

Εικόνα 15. Assets

• Essential Assets - **Data:**

Είναι τα δεδομένα που αφορούν στα μη-προσωπικά, στα προσωπικά και στα ευαίσθητα προσωπικά δεδομένα των:

Υπαλλήλων, αφορούν προσωπικά και οικονομικά στοιχειά (αμοιβές, εισφορές, κτλ).

Ασθενών, αφορούν τούς ασθενείς του ΓΝ και είναι ευαίσθητα δεδομένα(επισκέψεις και αρχείο ασθενών, χρήση φαρμάκων, ιατρικές και εργαστηριακών εξετάσεων, και δεδομένα της αιμοδοσίας).

Λογιστικά, αφορούν τα οικονομικά στοιχειά των συναλλασσόμενων με το ΓΝ, (προμηθευτές, τις οικονομικές συναλλαγές, και στοιχειά ισολογισμών)

• **Services:**

Είναι όλες εκείνες οι υπηρεσίες που παρέχονται στους χρήστες.

• 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

Εφαρμογές Προσωπικού

Εφαρμογές Ασθενών

• **Equipment:**

- Hardware

Είναι όλα εκείνα τα υλικά μέρη του ΠΣ που επεξεργάζονται τα δεδομένα.

Server με Windows 2012 Server, για τα οικονομικά του Νοσοκομείου.

Server με Windows 2012 Server για τις εφαρμογές ΓΝ**,** τις οποίες έχει αναπτύξει το ΗΔΙΚΑ και χρησιμοποιούνται από το Τμήμα Εισαγωγών Ασθενών, το Φαρμακείο, το Γραφείο Υλικού, το Λογιστήριο, το Τμήμα Διατροφής, τη Γραμματεία Εξωτερικών Ιατρειών, τα Γραφεία Νοσηλίων, Ιματισμού και Υγειονομικού Υλικού.

Server με Windows 2012, για τις εφαρμογές του Τμήματος Αιμοδοσίας.

Personal Computer με λειτουργικό σύστημα Windows 10 για την εφαρμογή της Μισθοδοσίας.

Lan Printer ethernet, για τον κεντρικό εξυπηρετητή.

Δικτυακός εξοπλισμός (routers, switches ,hubs). Περιλαμβάνει τις συσκευές του δικτύου, όπως δρομολογητές, τερματικές συσκευές κλπ., που χρησιμοποιούνται για τη επικοινωνία του Πληροφοριακού Συστήματος του ΓΝ**.** Οι δικτυακές και τηλεπικοινωνιακές υπηρεσίες των παρόχων, καθώς και ο εξοπλισμός τους, δεν περιλαμβάνονται. Λαμβάνονται, όμως, υπόψη στην παρούσα μελέτη ασφάλειας ως πιθανές πήγες απειλών και κίνδυνων. Εξοπλισμός δικτύου.

Work Stations, οι 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 Ιατρειών, το Γραφείο Υγειονομικού και το Τμήμα Ιματισμού.

Για χρήση των τοπικών εφαρμογών στο Σταθμό Αιμοδοσίας, στη Γραμματεία – Πρωτόκολλο, στο Γραφείο Μισθοδοσίας, στο γραφείο Προσωπικού και στο Γραφείο Προμηθειών.

Personal Computer, για χρήση του προσωπικού του σε όλα τα τμήματα του νοσοκομείου.

- **Software:**

Είναι τα λογισμικά προγράμματα στο ΠΣ-ΓΝ (λειτουργικό λογισμικό, λογισμικά εφαρμογών, λογισμικά υποστήριξης).

Λογισμικό συστημάτων και ανάπτυξης εφαρμογών. αποτελούνται από τα λειτουργικά συστήματα των εξυπηρετητών και των σταθμών εργασίας. Επίσης, περιλαμβάνουν βοηθητικό λογισμικό (π.χ. MS Office), λογισμικό βάσεων δεδομένων (Oracle, MySQL), λογισμικό διαχείρισης ηλεκτρονικού ταχυδρομείου (e-mail) και λογισμικό για την ασφάλεια των Πληροφορικών Συστημάτων.

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, firewall.

• **Facilities:**

Είναι οι κτιριακές εγκαταστάσεις στις οποίες βρίσκεται ο υλικός εξοπλισμός του ΠΣΓΝ.

• **Personel:**

Χρήστες (common users, administrative staff, IT Enginner, operators, medical staff), που εισάγουν στοιχεία, υποστηρικτές, προγραμματιστές, εκπαιδευτές, αναλυτές, ειδικοί δικτύων. Στο Πληροφοριακό Σύστημα Νοσοκομείου εμπλέκονται διοικητικοί υπάλληλοι, ιατροί, επιστήμονες πληροφορικής, νοσηλευτές, ασθενείς.

Εξαρτήσεις μεταξύ Αγαθών

Οι πληροφορίες και οι υπηρεσίες πρέπει να βρίσκονται πάντα στην κορυφή. Η αξία των πληροφοριών πρέπει να γίνεται αποδεκτή από τις υπηρεσίες που τις διαχειρίζονται. Επομένως, οι πληροφορίες βρίσκονται στην κορυφή και οι υπηρεσίες ακριβώς από κάτω.

Θα πρέπει ο υπεύθυνος να αναζητήσει πού μπορεί να αποτύχει το σύστημα ή, πιο σωστά, πού θα μπορούσε να διακυβευτεί η ασφάλεια των περιουσιακών στοιχείων.

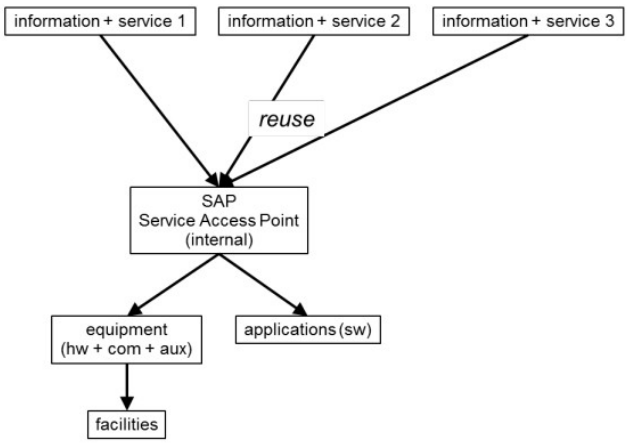
• Εάν υπάρχουν δεδομένα που είναι σημαντικά λόγω της εμπιστευτικότητας τους, είναι απαραίτητο να γνωρίζουμε που θα αποθηκευτούν και από που θα επανακτηθούν. Που θα μπορούσαν να αποκαλυφθούν;

• Εάν υπάρχουν δεδομένα που είναι σημαντικά λόγω της ακεραιότητάς τους, είναι απαραίτητο να γνωρίζουμε που θα αποθηκευτούν και από που θα επανακτηθούν. Που θα μπορούσαν να τροποποιηθούν;

• Εάν μια υπηρεσία είναι σημαντική λόγω της διαθεσιμότητάς της, είναι απαραίτητο να γνωρίζετε ποια αγαθά χρησιμοποιούνται για την παροχή της: η αποτυχία αυτών θα σταματούσε την υπηρεσία.

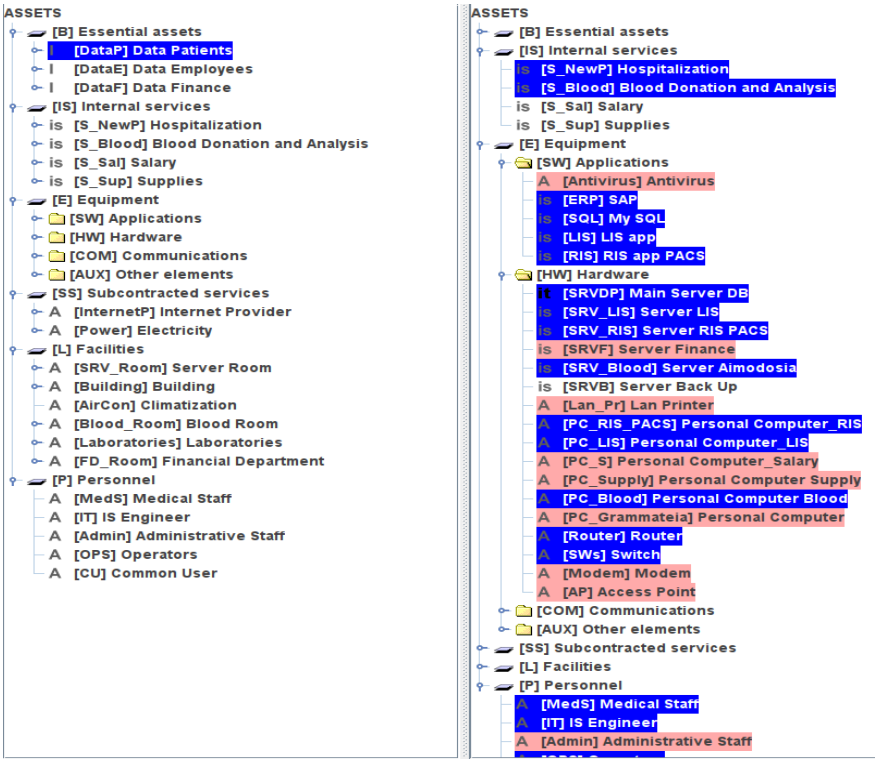
Ένα αγαθό μπορεί να δεχθεί επίθεση άμεσα ή έμμεσα μέσω ενός άλλου αγαθού από το οποίο εξαρτάται. Σαν αποτέλεσμα, οι **υπηρεσίες** εξαρτώνται από τον **εξοπλισμό** που με τη σειρά του εξαρτάται από τις **εγκαταστάσεις** στις οποίες βρίσκεται, χωρίς να χρειάζεται να δηλωθεί ότι οι υπηρεσίες εξαρτώνται από τις εγκαταστάσεις.

(The "Guide of techniques" contains the algorithmic model for calculating the total dependencies between assets on the basis of the direct dependencies).



Εικόνα 16. Εξαρτήσεις Αγαθών

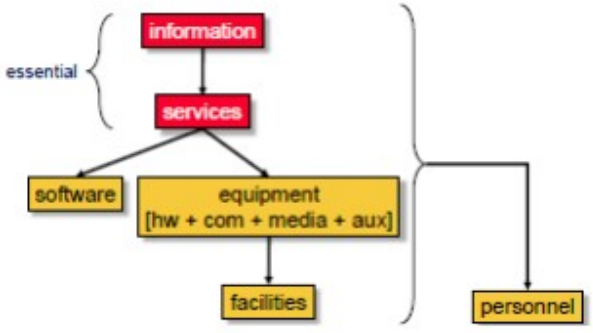
Τα **δεδομένα** εξαρτώνται από την **εφαρμογή**. Η εφαρμογή δεν έχει αξία χωρίς δεδομένα. Η πρόσβαση στα δεδομένα γίνεται μέσω της εφαρμογής, οπότε η εφαρμογή είναι το μέσο για να επιτεθεί κάποιος στα δεδομένα.



Εικόνα 17. Δεδομένα ασθενών εξαρτήσεις

Μοντελοποιημένες Εξαρτήσεις.

Για ένα μοντέλο εξαρτήσεων είναι απαραίτητο να ανιχνευθούν για κάθε αγαθό όλα τα στοιχεία από τα οποία εξαρτάται άμεσα ή έμμεσα. Από την λίστα εξαρτήσεων προκύπτει η συσσωρευμένη αξία, έτσι ώστε εάν βρεθεί ένα αγαθό χωρίς συσσωρευμένη αξία, αυτό σημαίνει ότι οι εξαρτήσεις έχουν διαμορφωθεί λάθος.



Εικόνα 18. Μοντέλο εξαρτήσεων

Εικόνα 19. Assets above - below

Αποτίμηση Αξίας Αγαθών.

Τα αγαθά συλλέχθηκαν, αποτιμήθηκαν και προσδιορίστηκε η αξία τους(ΠΑΡΑΡΤΗΜΑ Β), μέσω των συνεντεύξεων που πραγματοποιήθηκαν με τους υπευθύνους του κάθε τομέα, συμπληρώνοντας τα αντίστοιχα ερωτηματολόγια του ΠΑΡΑΡΤΗΜΑΤΟΣ Α.

[GH] A.1. Assets > A.1.6. valuation of assets

Edit Export Import

asset	[A]	[I]	[C]	[Auth]	[Acc]	[V]
ASSETS						
[B] Essential assets						
I [DataP] Data Patients	[7]	[6]	[9]	[6]	[7]	[6]
I [DataE] Data Employees	[9]	[7]	[7]	[5]	[5]	[7]
I [DataF] Data Finance	[7]	[9]	[7]	[5]	[7]	[6]
[IS] Internal services						
is [S_NewP] Hospitalization						
is [S_Blood] Blood Donation and Analysis						
is [S_Sal] Salary						
is [S_Sup] Supplies						
[E] Equipment						
[SW] Applications						
A [Antivirus] Antivirus	[3]	[4]	[4]	[3]	[4]	
is [ERP] SAP	[7]	[5]	[5]	[5]	[6]	
is [SQL] My SQL	[6]	[6]	[5]	[4]	[8]	
is [LIS] LIS app	[5]	[4]	[3]	[4]	[5]	
is [RIS] RIS app PACS	[5]	[4]	[3]	[4]	[5]	
[HW] Hardware						
it [SRVDP] Main Server DB	[6]	[6]	[5]	[4]	[5]	
is [SRV_LIS] Server LIS	[5]	[5]	[4]	[3]	[4]	
is [SRV_RIS] Server RIS PACS	[5]	[5]	[4]	[3]	[4]	
is [SRVF] Server Finance	[5]	[5]	[4]	[3]	[4]	
is [SRV_Blood] Server Aimodosia	[5]	[5]	[5]	[3]	[4]	
is [SRVB] Server Back Up	[5]	[5]	[4]	[3]	[4]	
A [Lan_Pr] Lan Printer	[5]	[3]	[4]	[3]	[4]	
A [PC_RIS_PACS] Personal Computer_RIS	[5]	[3]	[4]	[4]	[5]	
A [PC_LIS] Personal Computer_LIS	[5]	[3]	[4]	[4]	[5]	
A [PC_S] Personal Computer_Salary	[5]	[3]	[4]	[4]	[5]	
A [PC_Supply] Personal Computer Supply	[5]	[3]	[4]	[4]	[5]	
A [PC_Blood] Personal Computer Blood	[5]	[3]	[4]	[4]	[5]	
A [PC_Grammateia] Personal Computer	[5]	[3]	[4]	[4]	[5]	
A [Router] Router	[5]	[4]	[4]	[3]	[5]	
A [SWs] Switch	[5]	[4]	[4]	[3]	[5]	
A [Modem] Modem	[5]	[4]	[4]	[3]	[5]	
A [AP] Access Point	[5]	[4]	[4]	[3]	[5]	
[COM] Communications						
[Firewall] Firewall	[6]					
A [LAN] Local Area Nettwork	[4]	[3]	[4]	[4]	[5]	
A [WiFi] WiFi	[3]	[4]	[3]	[4]	[6]	
[AUX] Other elements						
A [Generator] Generator	[5]	[3]	[4]	[4]	[5]	
[SS] Subcontracted services						
A [InternetP] Internet Provider	[3]	[3]	[3]	[2]	[4]	
A [Power] Electricity	[6]	[3]	[4]	[4]	[4]	
[L] Facilities						
A [SRV_Room] Server Room	[7]	[3]	[4]	[7]	[7]	
A [Building] Building	[3]	[3]	[4]	[4]	[5]	
A [AirCon] Climatization	[5]	[3]	[4]	[4]	[5]	
A [Blood_Room] Blood Room	[4]	[3]	[4]	[4]	[5]	
A [Laboratories] Laboratories	[4]	[3]	[4]	[4]	[5]	
A [FD_Room] Financial Department	[4]	[3]	[4]	[4]	[5]	
[P] Personnel						
A [MedS] Medical Staff	[4]	[5]	[8]	[5]	[6]	
A [IT] IS Engineer	[4]	[3]	[3]	[3]	[6]	
A [Admin] Administrative Staff	[4]	[5]	[8]	[5]	[6]	
A [OPS] Operators	[4]	[3]	[6]	[4]	[6]	
A [CU] Common User	[4]	[5]	[6]	[4]	[6]	

Εικόνα 20.Αποτίμηση αξίας αγαθών

- **Εκτίμηση επικινδυνότητας με χρήση του εργαλείου PILAR.**

Η ανάλυση του κινδύνου περιλαμβάνει τρία στάδια:

1. Αναγνώριση κινδύνου (Risk Identification)

Τι μπορεί να πάει λάθος; → Η απάντηση στην πρώτη ερώτηση απαρτίζεται από ένα σύνολο σεναρίων συμβάντων/ατυχημάτων

2. Εκτίμηση κινδύνου (Risk Estimation)

Πόσο πιθανό είναι να συμβεί; → Η δεύτερη ερώτηση απαιτεί την εκτίμηση της πιθανότητας των σεναρίων αυτών

3. Αποτίμηση κινδύνου (Risk Evaluation)

Ποιες είναι οι συνέπειες; → Η τρίτη ερώτηση εκτιμά τις συνέπειες των σεναρίων συμβάντων/ατυχημάτων

Μέσα από τις απαντήσεις των παραπάνω ερωτήσεων μπορούν να εντοπισθούν οι κίνδυνοι, να ποσοτικοποιηθούν και να αξιολογηθούν με σκοπό να μειωθούν οι αρνητικές επιπτώσεις. Η διαδικασία αξιολόγησης είναι ένα γεγονός ή γεγονότα σε συνέχεια (σενάρια) που μπορούν να οδηγήσουν σε συνέπειες όπως, αύξηση του κόστους των επισκευών, μείωση της κινητικότητας του δικτύου ή καθυστέρηση στο χρόνο μεταφοράς των δεδομένων.

Η αποτίμηση των αγαθών του Οργανισμού οδηγεί στον έναν από τους δύο παράγοντες που συνθέτουν την επικινδυνότητα των ΠΣ, την επίπτωση (impact). Ο δεύτερος παράγοντας, η πιθανότητα (probability), συντίθεται από την απειλή και την ευπάθεια (αδυναμία), ως εξής:

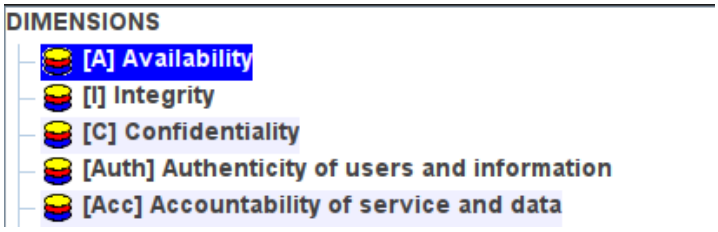
Απειλή x Ευπάθεια (Αδυναμία) = Πιθανότητα

Πιθανότητα x Επίπτωση = Επικινδυνότητα.

Η MAGERIT κατά τον υπολογισμό της επικινδυνότητας μελετά τα αγαθά και υπολογίζεται η τιμής τους κατά τις 5 αρχές ασφαλείας:

Confidentiality Integrity Availability Authenticity και **Accountability.**

(Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα, Απονομή Ευθυνών, Αυθεντικότητα).



Εικόνα 21. 5 Βασικές Αρχές Ασφάλειας

Αρχικά γίνεται:

- **εκτίμηση της αξίας των αγαθών**

- εκτίμηση των επιπτώσεων

- υπολογισμός επικινδυνότητας

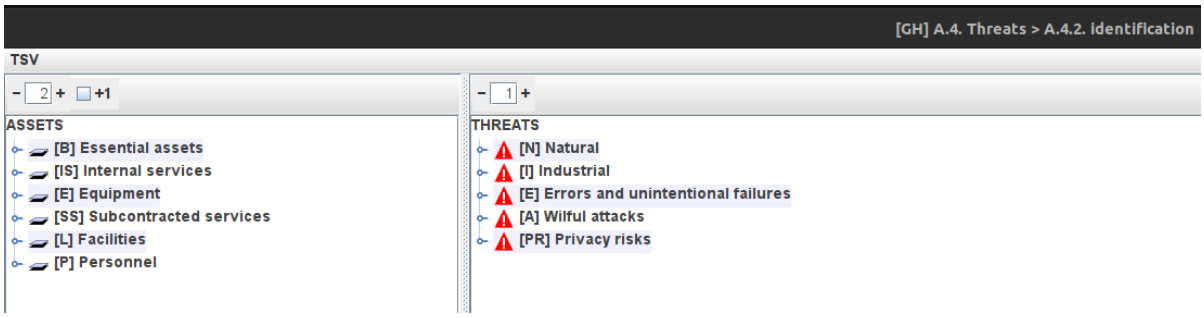
προκύπτει η επικινδυνότητα για κάθε απειλή σε κάθε αγαθό.

Στην συνέχεια παρουσιάζονται και αποτιμώνται οι απειλές που αντιμετωπίζουν τα ΠΣ και οι εγκαταστάσεις του ΠΓΝΣ.

3.2 Χαρακτηρισμός και Αποτίμηση Απειλών

Σε αυτό το στάδιο της εκτίμησης επικινδυνότητας θα γίνει εκτίμηση των απειλών (threats). Το εργαλείο Pilar έχει δημιουργηθεί σύμφωνα με τη μέθοδο Magerit. Σύμφωνα με τη μέθοδο, οι απειλές κατατάσσονται σε πέντε κατηγορίες:

- [Φ] Φυσικές Καταστροφές
- [Β] Βιομηχανικής προέλευσης
- [Α] Ακούσιες βλάβες και λάθη
- [Ε] Εκούσιες επιθέσεις
- [Α] Κίνδυνοι ιδιωτικότητας



Εικόνα 22. Κατηγορίες Απειλών

Σκοπός είναι να γίνει χαρακτηρισμός του περιβάλλοντος στο οποίο μια απειλή μπορεί να συμβεί, και οι συνέπειες που είναι πιθανό να επηρεάσουν ακόμα και τα άτομα.

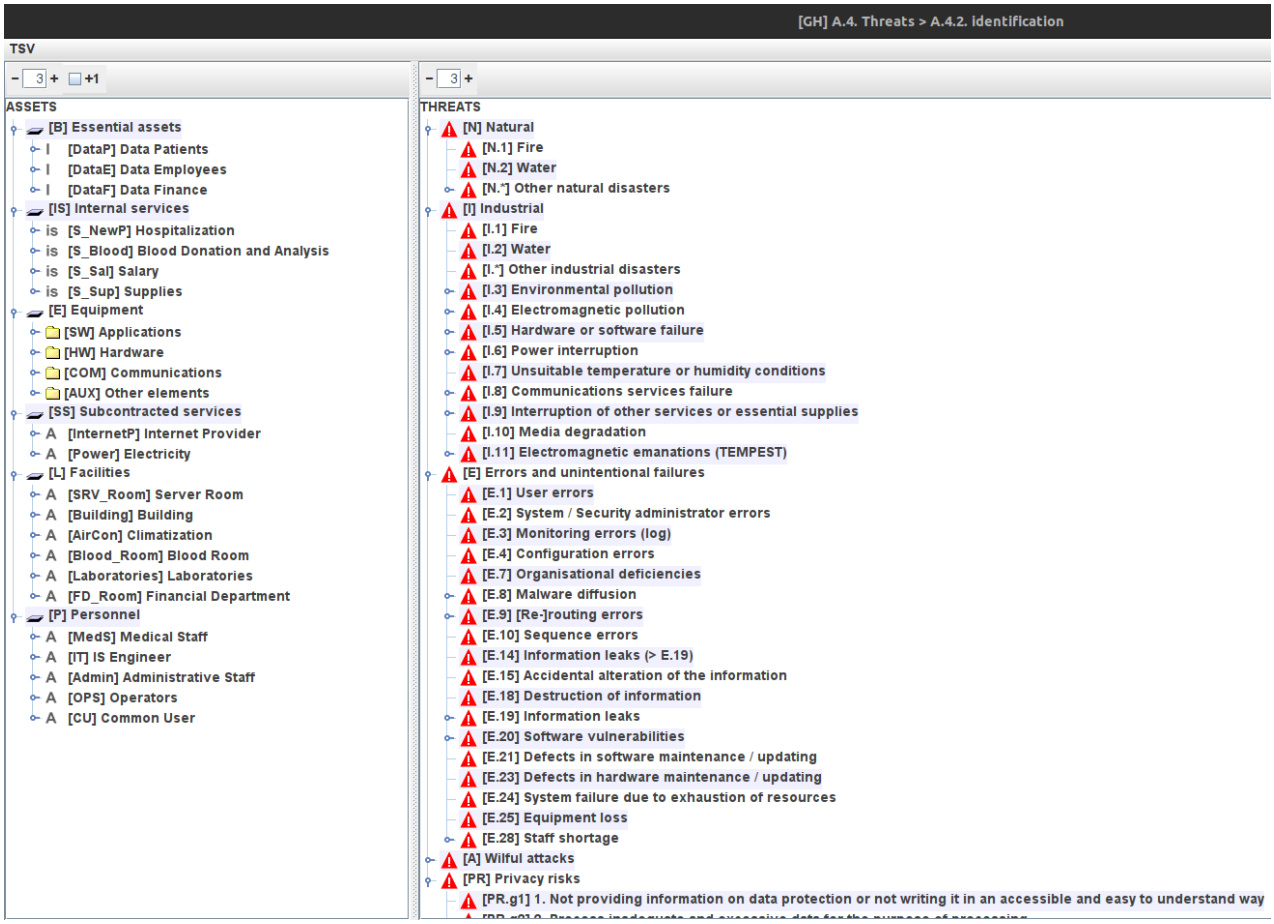
Ο χαρακτηρισμός των απειλών αποτελείται από τις δύο επιμέρους ενέργειες:

- Αναγνώριση των απειλών
- Αποτίμηση των απειλών

Με βάση την κατηγοριοποίηση των αγαθών στο προηγούμενο στάδιο το εργαλείο προτείνει απειλές για κάθε αγαθό. Για κάθε απειλή υπολογίζεται αυτόματα η πιθανότητα εμφάνισης της από το εργαλείο PILAR και εκτιμά την υποβάθμιση / υποτίμηση της αξίας του αγαθού λόγω της απειλής που υφίσταται.

Αναγνώριση Απειλών

Ο πίνακας που ακολουθεί παρουσιάζει τις κυριότερες απειλές που αντιμετωπίζουν τα ΠΣ και οι βασικές κτιριακές εγκαταστάσεις του ΠΣΓΝ.



Εικόνα 23. Αναγνώριση Απειλών

Αποτίμηση Απειλών

Στο Pilar η τρωτότητα προσδιορίζεται με κλίμακα που αποτιμάται: “Πολύ χαμηλή, Χαμηλή, “Μεσαία” ή Υψηλή, Πολύ υψηλή” .

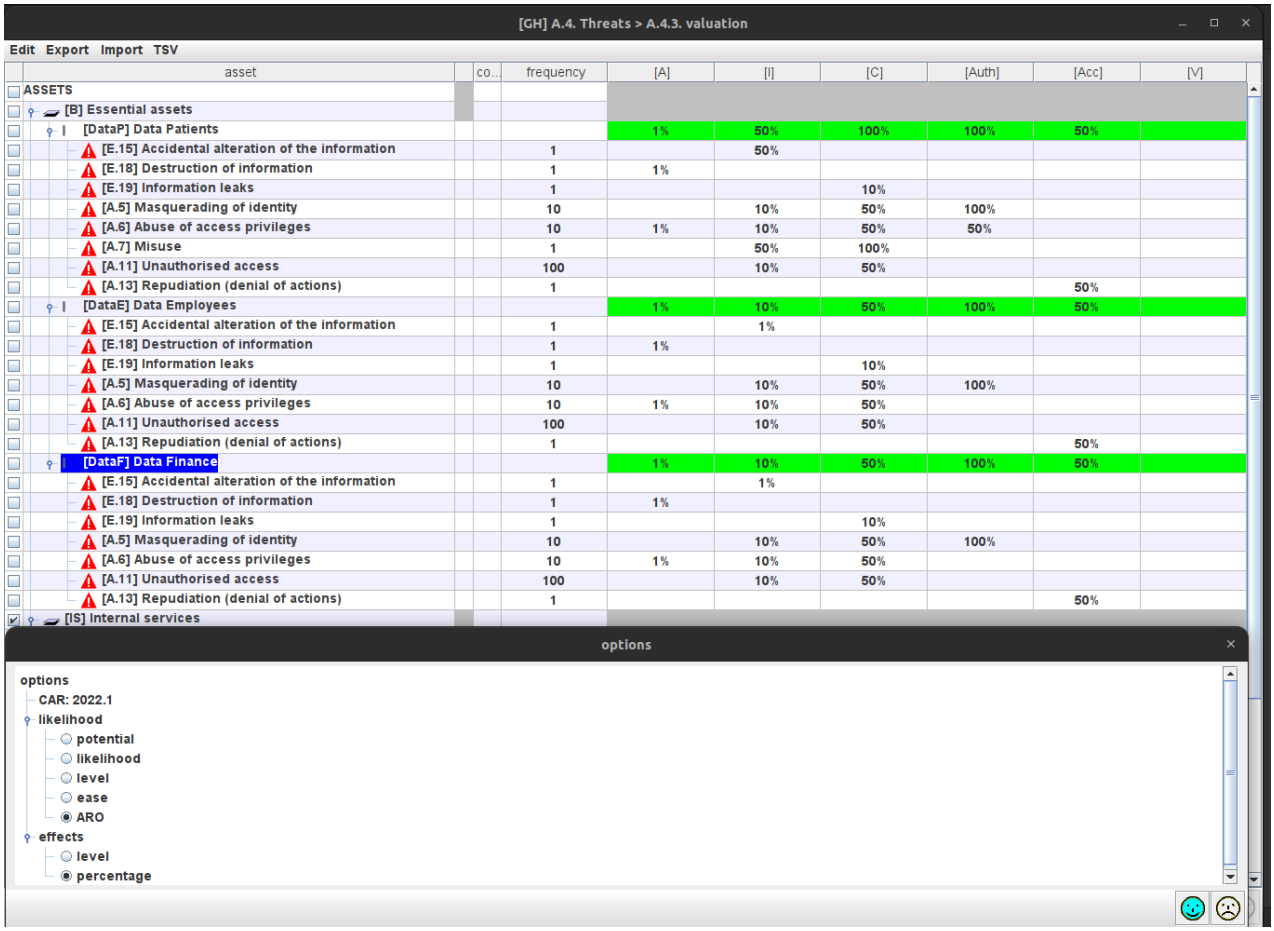
Η πιθανότητα μπορεί να μοντελοποιηθεί αριθμητικά ως ρυθμός εμφάνισης. Χρησιμοποιείται ως σημείο αναφοράς το ένα έτος, με αποτέλεσμα να χρησιμοποιείται ο ετήσιος ρυθμός εμφάνισης ως μέτρο της πιθανότητας να συμβεί κάτι.

potential	likelihood	level	ease	ARO
XL extra large	AC almost certain	VH very high	E easy	100
L large	VH very high	H high	M medium	10
M medium	P possible	M medium	D difficult	1
S small	U unlikely	L low	VD very difficult	0.1
XS extra small	VR very rare	VL very low	ED extremely difficult	0.01

ARO – Annual Rate of Occurrence

Εικόνα 24. ARO(annual rate of occurrence)[Magerit Book III the elements]

Στο ΠΑΡΑΡΤΗΜΑ Γ παρουσιάζονται για κάθε αγαθό οι απειλές που κινδυνεύει, η συχνότητα εμφάνισης τους και η συνέπεια από την υποβάθμιση της αξίας τους (σε ποσοστό επί %) ως προς **C.I.A. Authenticity** και **Accountability**.
Ορίζονται κάποιες προκαθορισμένες τιμές, σε αρχεία TSV (Threat Standard Values). Τα TSV είναι κατάλογοι με τις απειλές και τις τιμές τους για κάθε κατηγορία αγαθού.



Εικόνα 25.Valuation of threats

Likelihood: Πόσο συχνά εμφανίζεται μια απειλή (frequency).

100	very frequent	daily
10	frequent	monthly
1	normal	annually
1/10	infrequent	every few years

Εικόνα 26. Likelihood- frequency

3.3 Εκτίμηση Επιπτώσεων

Κατά την εκτίμηση των επιπτώσεων (impact), εκτιμάται η ζημία που έχει προκληθεί σε κάποιο αγαθό από την εμφάνιση μιας απειλής σε αυτό.

Impact estimation

Impact can be calculated from simple, double-entry tables:

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

Εικόνα 27. Impact= degradation / value

Επίσης υπολογίζεται:

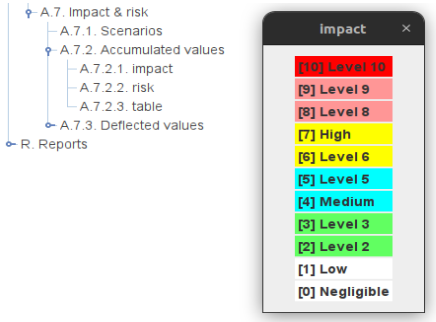
- Η δυνητική (**potential**) επίπτωση στην οποία υποβάλλεται το σύστημα.
- Η εναπομένουσα (**residual**) επίπτωση. (**safeguards**)

Για τον υπολογισμό της δυνητικής επίπτωσης (potential impact) λαμβάνεται υπόψη η αξία των κρίσιμων αγαθών και τα αποτελέσματα της αποτίμησης απειλών, χωρίς την εφαρμογή αντιμέτρων.

Η εναπομένουσα επίπτωση (residual impact) υπολογίζεται λαμβάνοντας υπόψη και τα υπάρχοντα αντίμετρα (κεφάλαιο 3.4).

Οι επιπτώσεις παρουσιάζονται με την ακόλουθη κλίμακα ανάλογα με την αξία τους:

[10]: Κρίσιμη, [9-8]: Πολύ Υψηλή, [7-6]: Υψηλή, [5-4]: Μέτρια, [3-2]: Χαμηλή, [1-0]: Αμελητέα



Δυνητική Επίπτωση (Potential impact)

Η δυνητική επικινδυνότητα υπολογίζεται λαμβάνοντας υπόψη την αξία των αγαθών και την αποτίμηση των απειλών. Πρόκειται για την έκταση της ζημιάς που προκαλείται από την πραγματοποίηση μιας απειλής.

[GH] A.7.2. Accumulated values > A.7.2.1. Impact

View Export

potential | current | target | PILAR

asset	[A]	[I]	[C]	[Auth]	[Acc]	[V]
ASSETS	[9]	[9]	[9]	[9]	[8]	
[B] Essential assets	[3]	[6]	[9]	[6]	[6]	
[DataP] Data Patients	[1]	[5]	[9]	[6]	[6]	
[DataE] Data Employees	[3]	[4]	[6]	[5]	[4]	
[DataF] Data Finance	[1]	[6]	[6]	[5]	[6]	
[IS] Internal services	[9]	[9]	[9]	[7]	[7]	
is [S_NewP] Hospitalization	[6]	[5]	[8]	[6]	[7]	
is [S_Blood] Blood Donation and Analysis	[7]	[6]	[9]	[6]	[7]	
is [S_Sal] Salary	[9]	[9]	[7]	[5]	[7]	
is [S_Sup] Supplies	[8]	[6]	[6]	[7]	[5]	
[E] Equipment	[9]	[9]	[9]	[9]	[8]	
[SW] Applications	[9]	[9]	[9]	[9]	[7]	
A [Antivirus] Antivirus	[7]	[6]	[9]			
is [ERP] SAP	[9]	[9]	[9]	[9]	[7]	
is [SQL] My SQL	[9]	[9]	[9]		[7]	
is [LIS] LIS app	[7]	[9]	[9]	[9]	[7]	
is [RIS] RIS app PACS	[7]	[9]	[9]	[9]	[7]	
[HW] Hardware	[9]	[9]	[9]	[9]	[8]	
[COM] Communications	[8]	[7]	[8]	[9]		
[Firewall] Firewall						
A [LAN] Local Area Nettwork	[8]	[7]	[8]	[9]		
A [WiFi] WiFi	[8]	[7]	[8]	[9]		
[AUX] Other elements	[9]	[9]	[9]	[9]	[8]	
A [Generator] Generator	[5]	[3]	[4]	[4]	[5]	
A [Cabling] Cabling	[9]	[6]	[8]			
A [Surveillans] Camera	[9]	[7]	[8]	[9]		
A [UPS] UPS	[9]	[9]	[9]	[9]	[8]	
A [Antena] Antena	[2]	[0]	[0]	[2]		
A [RFID] RFID reader	[9]	[6]	[8]			
A [UHF] UHF						
[SS] Subcontracted services	[9]	[9]	[9]	[9]	[8]	
A [InternetP] Internet Provider	[9]	[9]	[9]	[9]	[8]	
A [Power] Electricity	[6]	[3]	[4]	[4]	[4]	
[L] Facilities	[9]	[9]	[9]	[9]	[8]	
[P] Personnel	[8]	[9]	[9]			
A [MedS] Medical Staff	[8]	[8]	[7]			
A [IT] IS Engineer	[8]	[9]	[9]			
A [Admin] Administrative Staff	[8]	[8]	[8]			
A [OPS] Operators	[8]	[8]	[8]			
A [CU] Common User	[8]	[8]	[7]			

Εικόνα 28. Potential Impact

Γνωρίζοντας την αξία των αγαθών και την υποβάθμιση που προκαλείται σε αυτά από τις απειλές, η δυνητική επίπτωση ορίζεται ως η άμεση επίπτωση της πραγμάτωσης των απειλών στο ΠΣ και αποτιμάται ως προς την:

[Δ] Διαθεσιμότητα **[Ακ]** Ακεραιότητα **[Ε]** Εμπιστευτικότητα **[Αυθ]** Αυθεντικότητα πληροφορίας (authenticity) **[ΑΕ]** Απονομή Ευθυνών (accountability).

asset	[A]	[I]	[C]	[Auth]	[Acc]
ASSETS	[9]	[9]	[9]	[9]	[8]
[B] Essential assets	[3]	[6]	[9]	[6]	[6]
I [DataP] Data Patients	[1]	[5]	[9]	[6]	[6]
[E.15] Accidental alteration of the information		[5]			
[E.18] Destruction of information	[1]				
[E.19] Information leaks			[6]		
[A.5] Masquerading of identity		[3]	[8]	[6]	
[A.6] Abuse of access privileges	[1]	[3]	[8]	[5]	
[A.7] Misuse		[5]	[9]		
[A.11] Unauthorised access		[3]	[8]		
[A.13] Repudiation (denial of actions)					[6]
I [DataE] Data Employees	[3]	[4]	[6]	[5]	[4]
[E.15] Accidental alteration of the information		[1]			
[E.18] Destruction of information	[3]				
[E.19] Information leaks			[4]		
[A.5] Masquerading of identity		[4]	[6]	[5]	
[A.6] Abuse of access privileges	[3]	[4]	[6]		
[A.11] Unauthorised access		[4]	[6]		
[A.13] Repudiation (denial of actions)					[4]
I [DataF] Data Finance	[1]	[6]	[6]	[5]	[6]
[E.15] Accidental alteration of the information		[3]			
[E.18] Destruction of information	[1]				
[E.19] Information leaks			[4]		
[A.5] Masquerading of identity		[6]	[6]	[5]	
[A.6] Abuse of access privileges	[1]	[6]	[6]		
[A.11] Unauthorised access		[6]	[6]		
[A.13] Repudiation (denial of actions)					[6]
[IS] Internal services	[9]	[9]	[9]	[7]	[7]
is [S_NewP] Hospitalization	[6]	[5]	[8]	[6]	[7]
is [S_Blood] Blood Donation and Analysis	[7]	[6]	[9]	[6]	[7]
is [S_Sal] Salary	[9]	[9]	[7]	[5]	[7]
is [S_Sup] Supplies	[8]	[6]	[6]	[7]	[5]
[E] Equipment	[9]	[9]	[9]	[9]	[8]
[SW] Applications	[9]	[9]	[9]	[9]	[7]
A [Antivirus] Antivirus	[7]	[6]	[9]		
is [ERP] SAP	[9]	[9]	[9]	[9]	[7]
is [SQL] My SQL	[9]	[9]	[9]		[7]
is [LIS] LIS app	[7]	[9]	[9]	[9]	[7]
is [RIS] RIS app PACS	[7]	[9]	[9]	[9]	[7]
[HW] Hardware	[9]	[9]	[9]	[9]	[8]
is [LIS] LIS app	[7]	[9]	[9]	[9]	[7]
[I.5.1] Software failure	[6]				
[I.9] Interruption of other services or essential supplies	[6]				
[E.1] User errors	[4]	[6]	[6]		
[E.2] System / Security administrator errors	[5]	[7]	[7]		
[E.8] Malware diffusion	[4]	[6]	[6]		
[E.15] Accidental alteration of the information		[6]			
[E.18] Destruction of information	[4]				
[E.19] Information leaks			[6]		
[E.20] Software vulnerabilities	[1]	[7]	[7]		
[E.21] Defects in software maintenance / updating	[1]	[6]	[8]		
[E.24] System failure due to exhaustion of resources	[6]				
[A.5] Masquerading of identity		[9]	[9]	[9]	
[A.6] Abuse of access privileges	[1]	[6]	[8]	[9]	
[A.7] Misuse	[4]	[6]	[8]		
[A.8] Malware diffusion	[7]	[9]	[9]		
[A.11] Unauthorised access		[6]	[8]	[9]	
[A.13] Repudiation (denial of actions)					[7]
[A.15] Deliberate alteration of information		[8]			
[A.18] Destruction of information	[6]				
[A.19] Disclosure of information			[8]		
[A.22] Software manipulation	[6]	[9]	[9]		
[A.24] Denial of service	[6]				
is [RIS] RIS app PACS	[7]	[9]	[9]	[9]	[7]
[HW] Hardware	[9]	[9]	[9]	[9]	[8]
[COM] Communications	[8]	[7]	[8]	[9]	
[Firewall] Firewall					
A [LAN] Local Area Nettwork	[8]	[7]	[8]	[9]	
A [WiFi] WiFi	[8]	[7]	[8]	[9]	
[AUX] Other elements	[9]	[9]	[9]	[9]	[8]
[SS] Subcontracted services	[9]	[9]	[9]	[9]	[8]
[L] Facilities	[9]	[9]	[9]	[9]	[8]
[P] Personnel	[8]	[9]	[9]		
A [MedS] Medical Staff	[8]	[8]	[7]		
A [IT] IS Engineer	[8]	[9]	[9]		
A [Admin] Administrative Staff	[8]	[8]	[8]		

Εικόνα 29. Impact - CIA-Auth-Acc

Συνολική Επίπτωση **(Accumulated impact).**

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

Για ένα περιουσιακό στοιχείο μετριέται η συνολική του αξία (η δική του και επιπλέον των περιουσιακών στοιχείων που εξαρτώνται από αυτό).
Υπολογίζεται ως, η υψηλότερη αξία των τιμών μεταξύ του περιουσιακού στοιχείου που αποτιμάται και αυτών που εξαρτώνται από αυτό και τις συνολικές απειλές που εκτίθεται.

Η συνολική επίπτωση της απειλής για ένα περιουσιακό στοιχείο ορίζεται ως 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:

Επίπτωση **= V_{round}(x x d).**

Όσο μεγαλύτερη, η συνολική αποτίμηση ενός περιουσιακού στοιχείου και η ζημία (degradation) του επιτιθέμενου περιουσιακού στοιχείου τόσο μεγαλύτερη η επίπτωση.

Η αξία του ΠΣ ορίζεται στις υπηρεσίες που παρέχει και στα δεδομένα που χειρίζεται ενώ οι απειλές εμφανίζονται στα αλληλεξαρτώμενα περιουσιακά στοιχεία του οργανισμού.

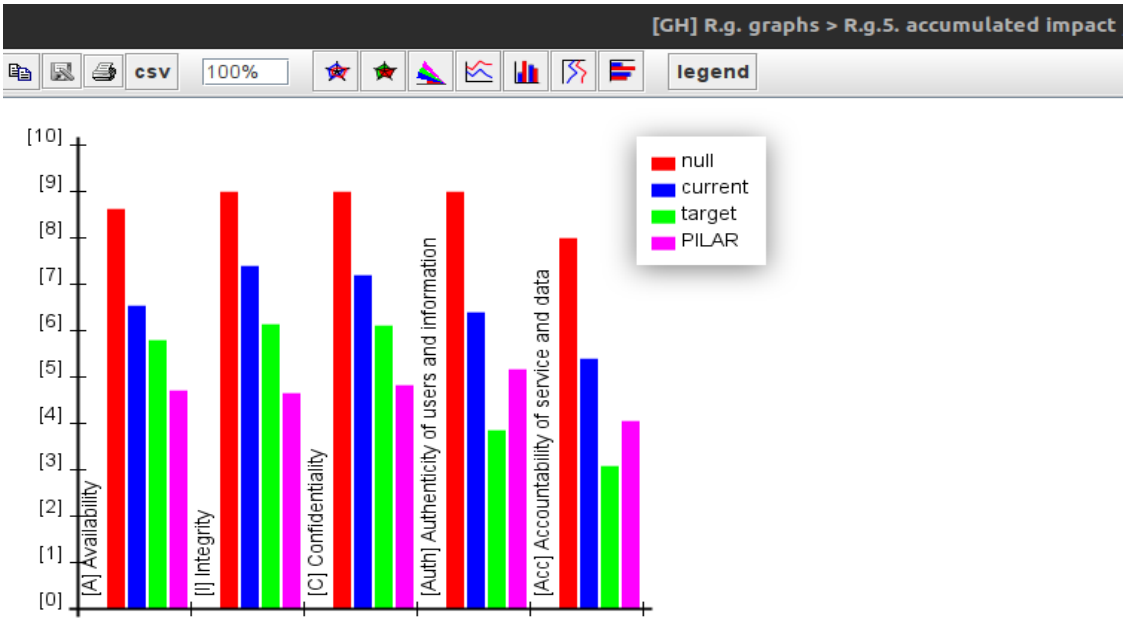
[GH] A.7.2. Accumulated values > A.7.2.1. impact

View Export

potential | current | target | PILAR

asset	[A]	[I]	[C]	[Auth]	[Acc]
ASSETS	[9]	[9]	[9]	[9]	[8]
[B] Essential assets	[3]	[6]	[9]	[6]	[6]
[DataP] Data Patients	[1]	[5]	[9]	[6]	[6]
[E.15] Accidental alteration of the information		[5]			
[E.18] Destruction of information	[1]				
[E.19] Information leaks			[6]		
[A.5] Masquerading of identity		[3]	[8]	[6]	
[A.6] Abuse of access privileges	[1]	[3]	[8]	[5]	
[A.7] Misuse		[5]	[9]		
[A.11] Unauthorised access		[3]	[8]		
[A.13] Repudiation (denial of actions)					[6]
[DataE] Data Employees	[3]	[4]	[6]	[5]	[4]
[E.15] Accidental alteration of the information		[1]			
[E.18] Destruction of information	[3]				
[E.19] Information leaks			[4]		
[A.5] Masquerading of identity		[4]	[6]	[5]	
[A.6] Abuse of access privileges	[3]	[4]	[6]		
[A.11] Unauthorised access		[4]	[6]		
[A.13] Repudiation (denial of actions)					[4]
[DataF] Data Finance	[1]	[6]	[6]	[5]	[6]
[E.15] Accidental alteration of the information		[3]			
[E.18] Destruction of information	[1]				
[E.19] Information leaks			[4]		
[A.5] Masquerading of identity		[6]	[6]	[5]	
[A.6] Abuse of access privileges	[1]	[6]	[6]		
[A.11] Unauthorised access		[6]	[6]		
[A.13] Repudiation (denial of actions)					[6]
[IS] Internal services	[9]	[9]	[9]	[7]	[7]
[E] Equipment	[9]	[9]	[9]	[9]	[8]
[SW] Applications	[9]	[9]	[9]	[9]	[7]
[HW] Hardware	[9]	[9]	[9]	[9]	[8]
[COM] Communications	[8]	[7]	[8]	[9]	
[AUX] Other elements	[9]	[9]	[9]	[9]	[8]
[SS] Subcontracted services	[9]	[9]	[9]	[9]	[8]
[L] Facilities	[9]	[9]	[9]	[9]	[8]
[P] Personnel	[8]	[9]	[9]		

Εικόνα 30. Accumulated Impact



Εικόνα 31. Accumulated graph

Ανακλώμενη επίπτωση (**Deflected Impact**)

Η ανακλώμενη επίπτωση υπολογίζεται **για κάθε περιουσιακό στοιχείο**, **για κάθε απειλή** και **για κάθε απαίτηση ασφαλείας,** ως συνάρτηση της εγγενούς αξίας και της υποβάθμισης που προκαλείται.

i. Όσο μεγαλύτερη είναι η εγγενής αξία ενός αγαθού, τόσο μεγαλύτερη είναι η επίδραση.

ii. Όσο μεγαλύτερη είναι η υποβάθμιση του αγαθού που δέχεται επίθεση, τόσο μεγαλύτερος είναι ο αντίκτυπος.

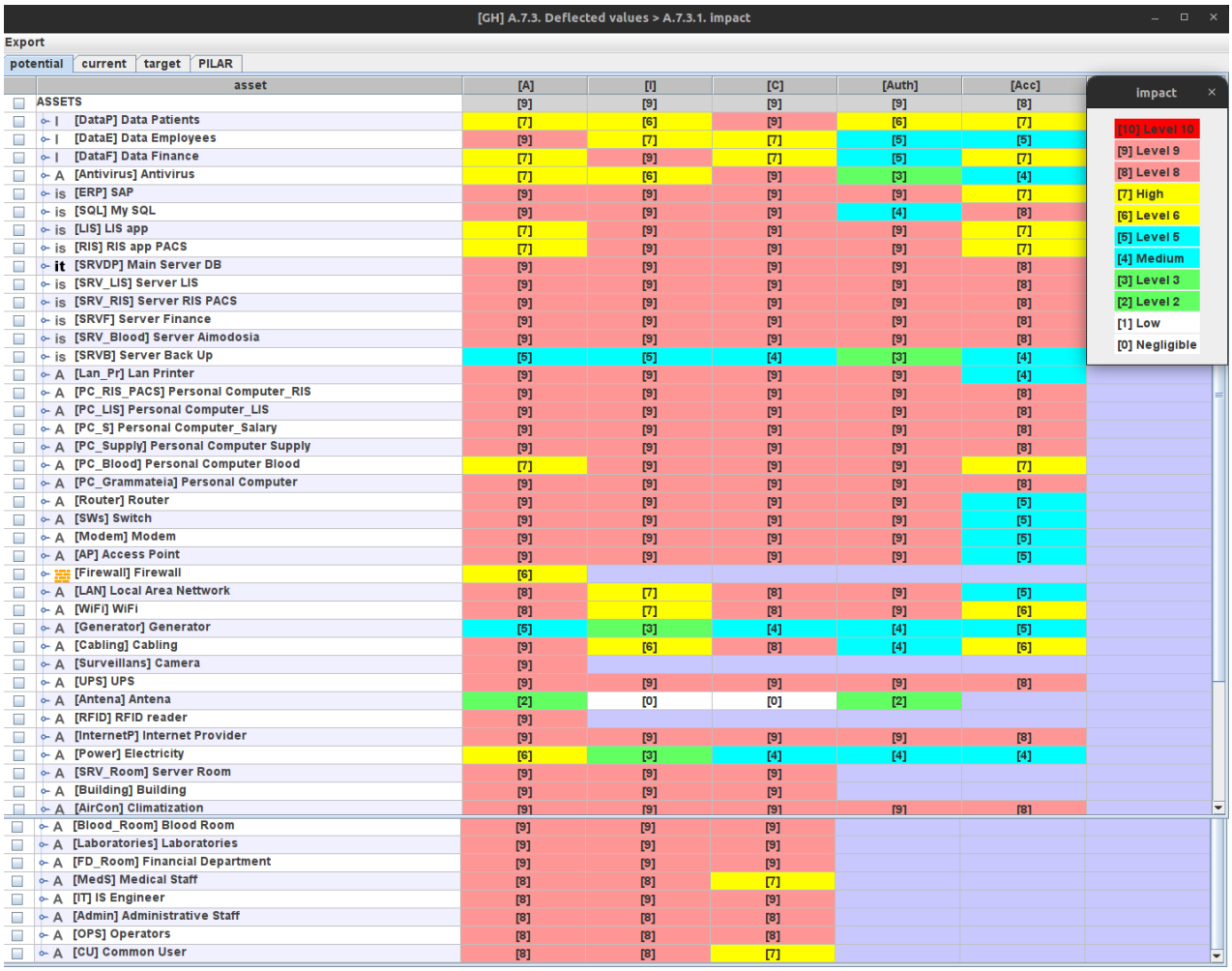
iii. Όσο μεγαλύτερη είναι η εξάρτηση από το αγαθό που δέχεται επίθεση, τόσο μεγαλύτερος είναι ο αντίκτυπος.

Επειδή η ανακλώμενη επίπτωση υπολογίζεται σε αγαθά που έχουν τη δική τους αξία, επιτρέπει τον προσδιορισμό των συνεπειών των τεχνικών συμβάντων στην λειτουργία του πληροφοριακού συστήματος. Είναι μια διαχείριση για την αποδοχή ενός συγκεκριμένου επιπέδου κινδύνου.

Αν το αγαθό Α εξαρτάται από το Β, οι απειλές του Β θα επηρεάσουν και το αγαθό Α. Αν το Β έχει μείωση "**D**", αυτή θα μεταφερθεί και στο "**A**" και η επίπτωση στο Α θα είναι, η απώλεια της βασικής του αξίας. Αν η τιμή του Α είναι «**V**» τότε η τιμή της επίπτωσης είναι:

Επίπτωση **= V x D x degree(AB)**

Η ανακλώμενη επίπτωση υπολογίζεται για κάθε αγαθό:



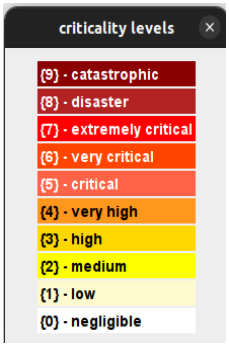
asset	[A]	[I]	[C]	[Auth]	[Acc]
ASSETS	[9]	[9]	[9]	[9]	[8]
[DataP] Data Patients	[7]	[6]	[9]	[6]	[7]
[DataE] Data Employees	[9]	[7]	[7]	[5]	[5]
[DataF] Data Finance	[7]	[9]	[7]	[5]	[7]
[Antivirus] Antivirus	[7]	[6]	[9]	[3]	[4]
[ERP] SAP	[9]	[9]	[9]	[9]	[7]
[SQL] My SQL	[9]	[9]	[9]	[4]	[8]
[LIS] LIS app	[7]	[9]	[9]	[9]	[7]
[RIS] RIS app PACS	[7]	[9]	[9]	[9]	[7]
[SRVDP] Main Server DB	[9]	[9]	[9]	[9]	[8]
[SRV_LIS] Server LIS	[9]	[9]	[9]	[9]	[8]
[SRV_RIS] Server RIS PACS	[9]	[9]	[9]	[9]	[8]
[SRVF] Server Finance	[9]	[9]	[9]	[9]	[8]
[SRV_Blood] Server Aimodosia	[9]	[9]	[9]	[9]	[8]
[SRVB] Server Back Up	[5]	[5]	[4]	[3]	[4]
[Lan_Pr] Lan Printer	[9]	[9]	[9]	[9]	[4]
[PC_RIS_PACS] Personal Computer_RIS	[9]	[9]	[9]	[9]	[8]
[PC_LIS] Personal Computer_LIS	[9]	[9]	[9]	[9]	[8]
[PC_S] Personal Computer_Salary	[9]	[9]	[9]	[9]	[8]
[PC_Supply] Personal Computer Supply	[9]	[9]	[9]	[9]	[8]
[PC_Blood] Personal Computer Blood	[7]	[9]	[9]	[9]	[7]
[PC_Grammateia] Personal Computer	[9]	[9]	[9]	[9]	[8]
[Router] Router	[9]	[9]	[9]	[9]	[5]
[SWs] Switch	[9]	[9]	[9]	[9]	[5]
[Modem] Modem	[9]	[9]	[9]	[9]	[5]
[AP] Access Point	[9]	[9]	[9]	[9]	[5]
[Firewall] Firewall	[6]				
[LAN] Local Area Nettwork	[8]	[7]	[8]	[9]	[5]
[WiFi] WiFi	[8]	[7]	[8]	[9]	[6]
[Generator] Generator	[5]	[3]	[4]	[4]	[5]
[Cabling] Cabling	[9]	[6]	[8]	[4]	[6]
[Surveillans] Camera	[9]				
[UPS] UPS	[9]	[9]	[9]	[9]	[8]
[Antena] Antena	[2]	[0]	[0]	[2]	
[RFID] RFID reader	[9]				
[InternetP] Internet Provider	[9]	[9]	[9]	[9]	[8]
[Power] Electricity	[6]	[3]	[4]	[4]	[4]
[SRV_Room] Server Room	[9]	[9]	[9]		
[Building] Building	[9]	[9]	[9]		
[AirCon] Climatization	[9]	[9]	[9]	[9]	[8]
[Blood_Room] Blood Room	[9]	[9]	[9]		
[Laboratories] Laboratories	[9]	[9]	[9]		
[FD_Room] Financial Department	[9]	[9]	[9]		
[MedS] Medical Staff	[8]	[8]	[7]		
[IT] IS Engineer	[8]	[9]	[9]		
[Admin] Administrative Staff	[8]	[8]	[8]		
[OPS] Operators	[8]	[8]	[8]		
[CU] Common User	[8]	[8]	[7]		

Εικόνα 32. Deflected Impact

Τα αναλυτικά αποτελέσματα παρατίθενται στο ΠΑΡΑΡΤΗΜΑ Δ.

3.3.1 Εκτίμηση Επικινδυνότητας

Ολοκληρώνοντας την ανάλυση επικινδυνότητας στο στάδιο αυτό υπολογίζεται ο κίνδυνος. Με τον κίνδυνο εκτιμάται η βλάβη που μπορεί να υποστεί το κάθε αγαθό από κάθε απειλή. Υπολογίζεται με βάση **την επίπτωση και την συχνότητα εμφάνισης**.
Η κλίμακα επικινδυνότητας μετριέται σε κλίμακα από (0 – 9). Στην συνέχεια παρατίθεται ένα μέρος του συνολικού πίνακα επικινδυνότητας για όλα τα αγαθά και στους 5 άξονες ασφάλειας και για κάθε μια από τις 5 κατηγορίες απειλών.



Export

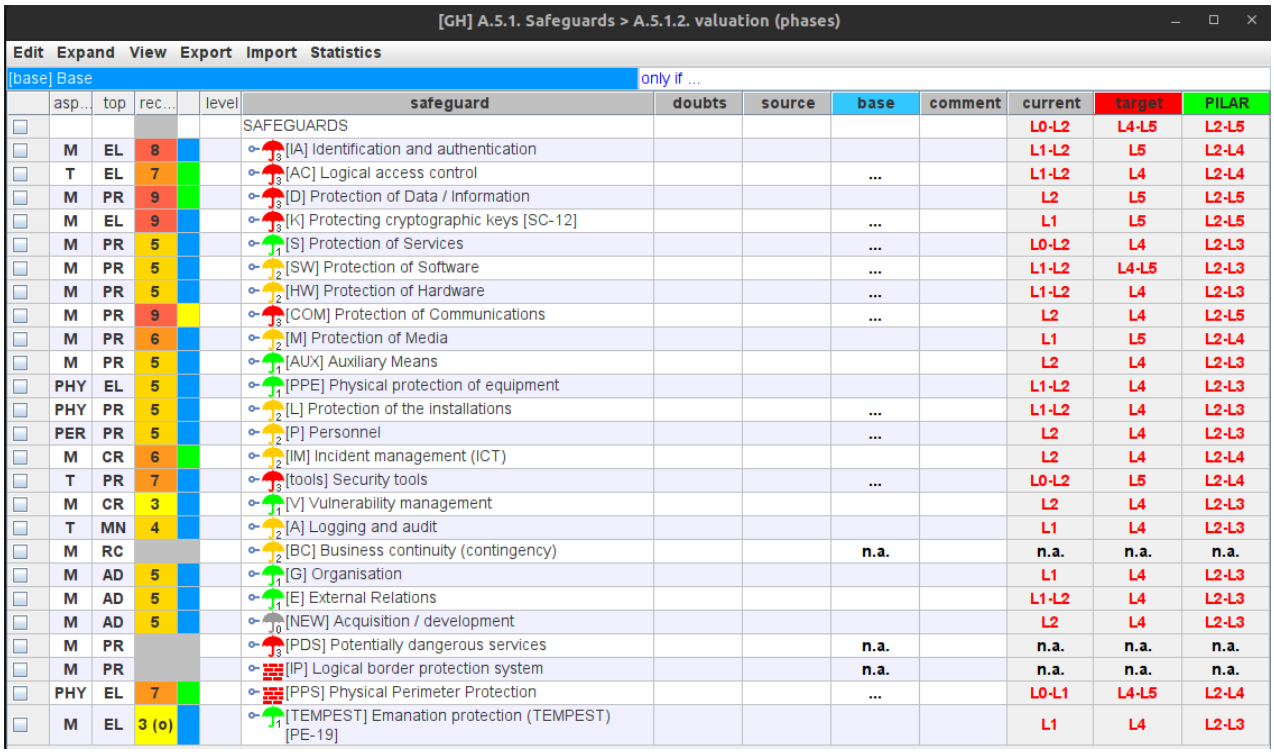
potential | current | target | PILAR | summary (impact) | summary (risk)

asset	threat	D	V	AV	D	I	F	R
[SRVDP] Main Server DB	[A.11] Unauthorised access	[I]	[6]	[9]	100%	[9]	100	{8.0}
[SRV_LIS] Server LIS	[A.11] Unauthorised access	[I]	[5]	[9]	100%	[9]	100	{8.0}
[SRV_RIS] Server RIS PACS	[A.11] Unauthorised access	[I]	[5]	[9]	100%	[9]	100	{8.0}
[SRVF] Server Finance	[A.11] Unauthorised access	[I]	[5]	[9]	100%	[9]	100	{8.0}
[SRV_Blood] Server Aimodosia	[A.11] Unauthorised access	[I]	[5]	[9]	100%	[9]	100	{8.0}
[SRVDP] Main Server DB	[A.11] Unauthorised access	[C]	[5]	[9]	100%	[9]	100	{8.0}
[SRV_LIS] Server LIS	[A.11] Unauthorised access	[C]	[4]	[9]	100%	[9]	100	{8.0}
[SRV_RIS] Server RIS PACS	[A.11] Unauthorised access	[C]	[4]	[9]	100%	[9]	100	{8.0}
[SRVF] Server Finance	[A.11] Unauthorised access	[C]	[4]	[9]	100%	[9]	100	{8.0}
[SRV_Blood] Server Aimodosia	[A.11] Unauthorised access	[C]	[5]	[9]	100%	[9]	100	{8.0}
[ERP] SAP	[A.11] Unauthorised access	[Auth]	[5]	[9]	100%	[9]	100	{8.0}
[LIS] LIS app	[A.11] Unauthorised access	[Auth]	[4]	[9]	100%	[9]	100	{8.0}
[RIS] RIS app PACS	[A.11] Unauthorised access	[Auth]	[4]	[9]	100%	[9]	100	{8.0}
[SRVDP] Main Server DB	[A.11] Unauthorised access	[Auth]	[4]	[9]	100%	[9]	100	{8.0}
[SRV_LIS] Server LIS	[A.11] Unauthorised access	[Auth]	[3]	[9]	100%	[9]	100	{8.0}
[SRV_RIS] Server RIS PACS	[A.11] Unauthorised access	[Auth]	[3]	[9]	100%	[9]	100	{8.0}
[SRVF] Server Finance	[A.11] Unauthorised access	[Auth]	[3]	[9]	100%	[9]	100	{8.0}
[SRV_Blood] Server Aimodosia	[A.11] Unauthorised access	[Auth]	[3]	[9]	100%	[9]	100	{8.0}
[PC_RIS_PACS] Personal Computer_RIS	[A.11] Unauthorised access	[Auth]	[4]	[9]	100%	[9]	100	{8.0}
[PC_LIS] Personal Computer_LIS	[A.11] Unauthorised access	[Auth]	[4]	[9]	100%	[9]	100	{8.0}
[PC_S] Personal Computer_Salary	[A.11] Unauthorised access	[Auth]	[4]	[9]	100%	[9]	100	{8.0}
[PC_Supply] Personal Computer Supply	[A.11] Unauthorised access	[Auth]	[4]	[9]	100%	[9]	100	{8.0}
[PC_Blood] Personal Computer Blood	[A.11] Unauthorised access	[Auth]	[4]	[9]	100%	[9]	100	{8.0}
[PC_Grammateia] Personal Computer	[A.11] Unauthorised access	[Auth]	[4]	[9]	100%	[9]	100	{8.0}
[ERP] SAP	[A.3] Manipulation of activity r...	[I]	[5]	[9]	50%	[8]	100	{7.5}
[SRVDP] Main Server DB	[A.3] Manipulation of activity r...	[I]	[6]	[9]	50%	[8]	100	{7.5}
[SRV_RIS] Server RIS PACS	[A.3] Manipulation of activity r...	[I]	[5]	[9]	50%	[8]	100	{7.5}
[SRVF] Server Finance	[A.3] Manipulation of activity r...	[I]	[5]	[9]	50%	[8]	100	{7.5}
[SRV_Blood] Server Aimodosia	[A.3] Manipulation of activity r...	[I]	[5]	[9]	50%	[8]	100	{7.5}
[DataP] Data Patients	[A.11] Unauthorised access	[C]	[9]	[9]	50%	[8]	100	{7.5}
[S_NewP] Hospitalization	[A.11] Unauthorised access	[C]		[9]	50%	[8]	100	{7.5}
[S_Blood] Blood Donation and Analysis	[A.11] Unauthorised access	[C]		[9]	50%	[8]	100	{7.5}
[ERP] SAP	[A.11] Unauthorised access	[C]	[5]	[9]	50%	[8]	100	{7.5}
[LIS] LIS app	[A.11] Unauthorised access	[C]	[3]	[9]	50%	[8]	100	{7.5}
[RIS] RIS app PACS	[A.11] Unauthorised access	[C]	[3]	[9]	50%	[8]	100	{7.5}
[PC_RIS_PACS] Personal Computer_RIS	[A.11] Unauthorised access	[C]	[4]	[9]	50%	[8]	100	{7.5}
[PC_LIS] Personal Computer_LIS	[A.11] Unauthorised access	[C]	[4]	[9]	50%	[8]	100	{7.5}
[PC_S] Personal Computer_Salary	[A.11] Unauthorised access	[C]	[4]	[9]	50%	[8]	100	{7.5}
[PC_Supply] Personal Computer Supply	[A.11] Unauthorised access	[C]	[4]	[9]	50%	[8]	100	{7.5}
[PC_Blood] Personal Computer Blood	[A.11] Unauthorised access	[C]	[4]	[9]	50%	[8]	100	{7.5}
[PC_Grammateia] Personal Computer	[A.11] Unauthorised access	[Auth]	[4]	[9]	100%	[9]	100	{8.0}
[ERP] SAP	[A.3] Manipulation of activity r...	[I]	[5]	[9]	50%	[8]	100	{7.5}
[SRVDP] Main Server DB	[A.3] Manipulation of activity r...	[I]	[6]	[9]	50%	[8]	100	{7.5}
[SRV_RIS] Server RIS PACS	[A.3] Manipulation of activity r...	[I]	[5]	[9]	50%	[8]	100	{7.5}
[SRVF] Server Finance	[A.3] Manipulation of activity r...	[I]	[5]	[9]	50%	[8]	100	{7.5}
[SRV_Blood] Server Aimodosia	[A.3] Manipulation of activity r...	[I]	[5]	[9]	50%	[8]	100	{7.5}
[DataP] Data Patients	[A.11] Unauthorised access	[C]	[9]	[9]	50%	[8]	100	{7.5}
[S_NewP] Hospitalization	[A.11] Unauthorised access	[C]		[9]	50%	[8]	100	{7.5}
[S_Blood] Blood Donation and Analysis	[A.11] Unauthorised access	[C]		[9]	50%	[8]	100	{7.5}
[ERP] SAP	[A.11] Unauthorised access	[C]	[5]	[9]	50%	[8]	100	{7.5}
[LIS] LIS app	[A.11] Unauthorised access	[C]	[3]	[9]	50%	[8]	100	{7.5}
[RIS] RIS app PACS	[A.11] Unauthorised access	[C]	[3]	[9]	50%	[8]	100	{7.5}
[PC_RIS_PACS] Personal Computer_RIS	[A.11] Unauthorised access	[C]	[4]	[9]	50%	[8]	100	{7.5}
[PC_LIS] Personal Computer_LIS	[A.11] Unauthorised access	[C]	[4]	[9]	50%	[8]	100	{7.5}
[PC_S] Personal Computer_Salary	[A.11] Unauthorised access	[C]	[4]	[9]	50%	[8]	100	{7.5}
[PC_Supply] Personal Computer Supply	[A.11] Unauthorised access	[C]	[4]	[9]	50%	[8]	100	{7.5}
[PC_Blood] Personal Computer Blood	[A.11] Unauthorised access	[C]	[4]	[9]	50%	[8]	100	{7.5}
[PC_Grammateia] Personal Computer	[A.11] Unauthorised access	[C]	[4]	[9]	50%	[8]	100	{7.5}
[LIS] LIS app	[A.5] Masquerading of identity	[I]	[4]	[9]	100%	[9]	10	{7.1}
[RIS] RIS app PACS	[A.5] Masquerading of identity	[I]	[4]	[9]	100%	[9]	10	{7.1}
[SRV_LIS] Server LIS	[A.5] Masquerading of identity	[I]	[5]	[9]	100%	[9]	10	{7.1}
[SRV_RIS] Server RIS PACS	[A.5] Masquerading of identity	[I]	[5]	[9]	100%	[9]	10	{7.1}

Εικόνα 33. Potential RISK

3.4 Προσδιορισμός Αντιμέτρων

Αντίμετρο είναι το μετρό που λαμβάνεται για την προστασία του πληροφοριακού συστήματος και την αντιμετώπιση των απειλών. Το μετρό μπορεί να ενεργεί ανιχνεύοντας, προλαμβάνοντας ή μειώνοντας την απώλεια που σχετίζεται με την εμφάνιση μιας απειλής ή κατηγορίας απειλών



[GH] A.5.1. Safeguards > A.5.1.2. valuation (phases)

Edit Expand View Export Import Statistics

[base] Base — only if ...

	asp...	top	rec...		level	safeguard	doubts	source	base	comment	current	target	PILAR
						SAFEGUARDS					L0-L2	L4-L5	L2-L5
	M	EL	8			[IA] Identification and authentication					L1-L2	L5	L2-L4
	T	EL	7			[AC] Logical access control			...		L1-L2	L4	L2-L4
	M	PR	9			[D] Protection of Data / Information					L2	L5	L2-L5
	M	EL	9			[K] Protecting cryptographic keys [SC-12]			...		L1	L5	L2-L5
	M	PR	5			[S] Protection of Services			...		L0-L2	L4	L2-L3
	M	PR	5			[SW] Protection of Software			...		L1-L2	L4-L5	L2-L3
	M	PR	5			[HW] Protection of Hardware			...		L1-L2	L4	L2-L3
	M	PR	9			[COM] Protection of Communications			...		L2	L4	L2-L5
	M	PR	6			[M] Protection of Media					L1	L5	L2-L4
	M	PR	5			[AUX] Auxiliary Means					L2	L4	L2-L3
	PHY	EL	5			[PPE] Physical protection of equipment					L1-L2	L4	L2-L3
	PHY	PR	5			[L] Protection of the installations			...		L1-L2	L4	L2-L3
	PER	PR	5			[P] Personnel			...		L2	L4	L2-L3
	M	CR	6			[IM] Incident management (ICT)					L2	L4	L2-L4
	T	PR	7			[tools] Security tools			...		L0-L2	L5	L2-L4
	M	CR	3			[V] Vulnerability management					L2	L4	L2-L3
	T	MN	4			[A] Logging and audit					L1	L4	L2-L3
	M	RC				[BC] Business continuity (contingency)			n.a.		n.a.	n.a.	n.a.
	M	AD	5			[G] Organisation					L1	L4	L2-L3
	M	AD	5			[E] External Relations					L1-L2	L4	L2-L3
	M	AD	5			[NEW] Acquisition / development					L2	L4	L2-L3
	M	PR				[PDS] Potentially dangerous services			n.a.		n.a.	n.a.	n.a.
	M	PR				[IP] Logical border protection system			n.a.		n.a.	n.a.	n.a.
	PHY	EL	7			[PPS] Physical Perimeter Protection			...		L0-L1	L4-L5	L2-L4
	M	EL	3 (o)			[TEMPEST] Emanation protection (TEMPEST) [PE-19]					L1	L4	L2-L3

Εικόνα 34. Safeguards μελέτη Νοσοκομείου

Από κάθε συνέντευξη, καταγράφεται μια εκτίμηση της αποτελεσματικότητας κάθε αντιμέτρου σχετικά με τις απειλές για τις οποίες υλοποιήθηκε. Τέλος, τα αντίμετρα αυτά παρουσιάζονται υπό μορφή αναφοράς σύμφωνα με το βαθμό αποτελεσματικότητα τους.

Προσδιορισμός των αντιμέτρων:

Απαίτηση για έγκριση/εξουσιοδότηση:

Το αντίμετρο μπορεί να εφαρμοστεί στις παρακάτω κατηγορίες περιουσιακών στοιχείων του ΠΣ: Στοιχεία/πληροφορίες, υπηρεσίες, εφαρμογές (λογισμικό), εξοπλισμό πληροφορικής (hardware), δίκτυα επικοινωνιών. Προστατεύει τις ακόλουθες ιδιότητες ασφάλειας: Ακεραιότητα, εμπιστευτικότητα και αυθεντικότητα.

Απειλές που οφείλονται σε πρόσωπα:

Λάθη των χρηστών, λάθη του διαχειριστή συστήματος ασφάλειας, διάδοση ιομορφικού λογισμικού, αλλοίωση πληροφοριών, διαρροή πληροφοριών, ευπάθεια λογισμικού, λάθη στη συντήρηση/επικαιροποίηση προγραμμάτων (software), πλαστογράφηση της ταυτότητας του χρήστη, κατάχρηση στα προνόμια πρόσβασης, μη εξουσιοδοτημένη πρόσβαση.

Εργαλείο προστασίας από ιομορφικό λογισμικό:

Η εταιρεία προσφέρει εργαλεία προστασίας από ιομορφικό λογισμικό, αλλά δεν είναι πάντα ενημερωμένα, τα ακόλουθα αντίμετρα επιλέχθηκαν:

• Το πρόγραψα πρέπει να ενημερώνεται τακτικά.

• Η βάση δεδομένων του προγράμματος πρέπει να ενημερώνεται τακτικά

• Τα αντίμετρα αυτά εφαρμόζονται στο επίπεδο των εφαρμογών και του λογισμικού.

Προστασία των εφαρμογών της πληροφορικής: Τα αντίμετρα επιλέχθηκαν με

βάση ότι δεν υπάρχουν τα εξής:

• Κανονισμοί για την επιτρεπόμενη χρήση των εφαρμογών.

• Κανόνες για την εγκατάσταση μη εξουσιοδοτημένου λογισμικού και προϊόντων

με συγκεκριμένη άδεια.

• Διαδικασίες για τη δημιουργία αντιγράφων ασφάλειας.

• Τα αρχεία δεδομένων της εφαρμογής πρέπει να προστατεύονται εξασφαλίζοντας

εμπιστευτικότητα και ακεραιότητα.

• Έλεγχος έκδοσης όλων των προγραμμάτων λογισμικού.

Προστασία του εξοπλισμού:

• Κανονισμοί για τη σωστή χρήση του εξοπλισμού.

• Διαδικασίες που είναι εξουσιοδοτημένες να χρησιμοποιήσουν τον εξοπλισμό.

• Προφίλ ασφαλείας.

Διασφαλίζονται οι διαστάσεις όπως η ακεραιότητα και η εμπιστευτικότητα.

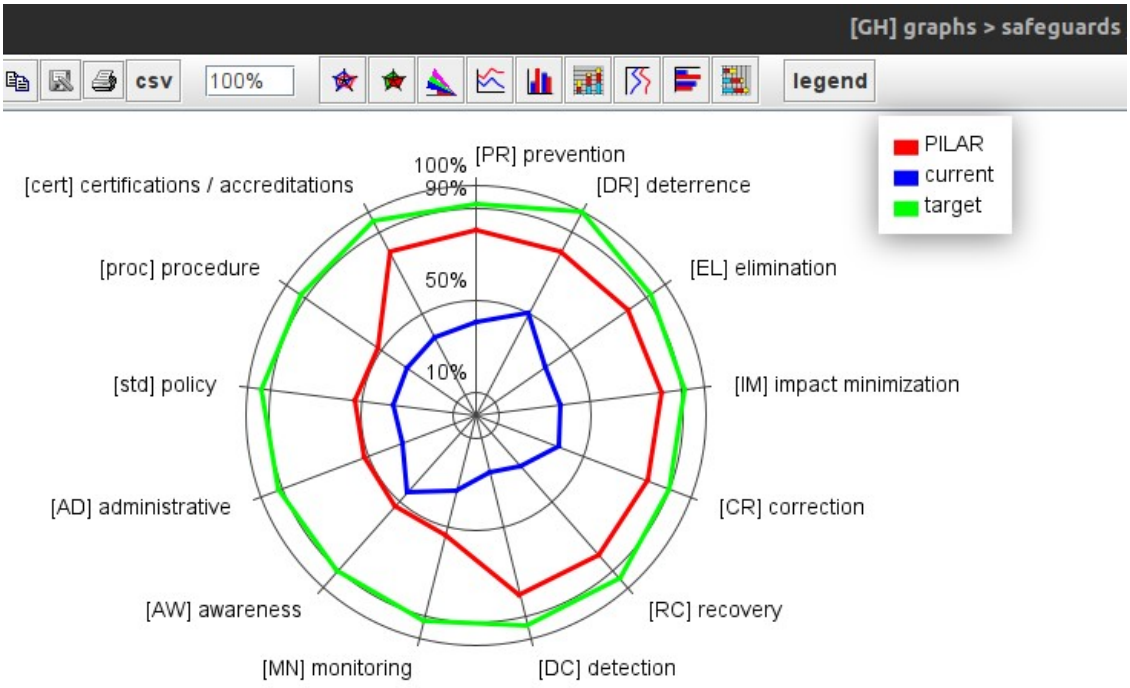
Διασφάλιση Επικοινωνιών:

• Προφίλ ασφάλειας: Αποφυγή απειλών όπως λάθη χρηστών, σφάλματα ακολουθίας, απρόβλεπτη χρήση, προώθηση μηνυμάτων, μη εξουσιοδοτημένη πρόσβαση.

Προστατεύονται οι: Ακεραιότητα, εμπιστευτικότητα και αυθεντικότητα.

• Έλεγχος της προέλευσης και του προορισμού των μηνυμάτων (φίλτρο).

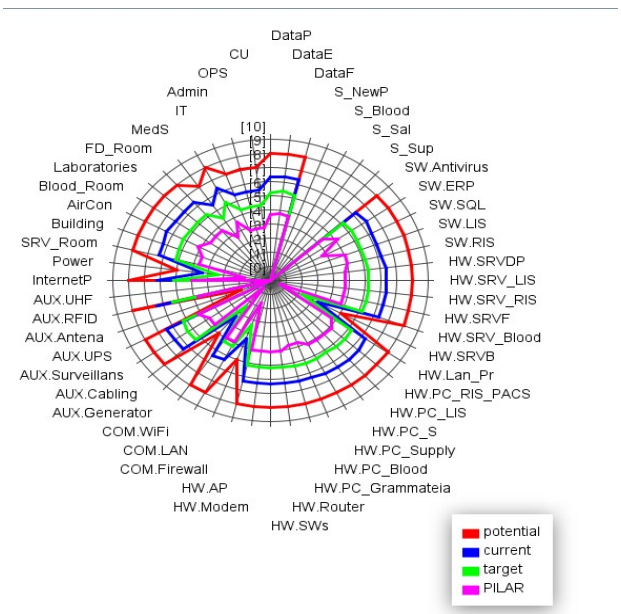
Αντιμετώπιση της μη εξουσιοδοτημένης πρόσβασης.



Εικόνα 35. Safeguards graph

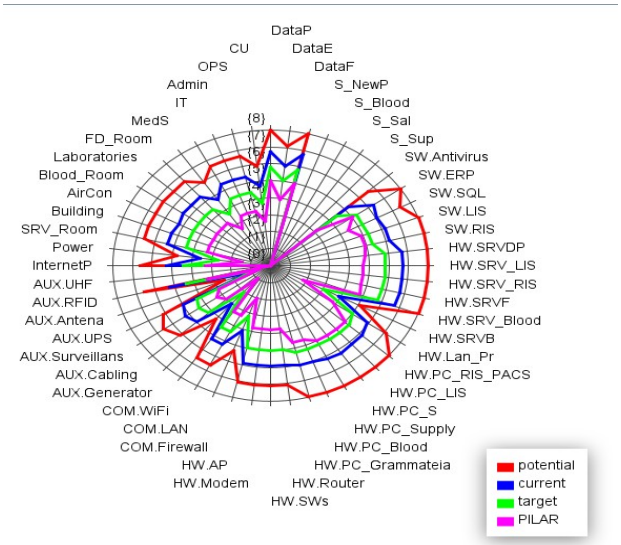
Εναπομένουσα Αθροιστική Επίπτωση (residual)

Μετά την εφαρμογή των προτεινόμενων αντιμέτρων σε κάθε αγαθό η εναπομένουσα επίπτωση συναθροίζεται στον παρακάτω πίνακα:



Εκτίμηση Εναπομένουσας Επικινδυνότητας (residual)

Η συσσωρευμένη εναπομένουσα επικινδυνότητα δείχνει τη διάχυση της επικινδυνότητας ανάμεσα σε εξαρτώμενα αγαθά. Όσα αγαθά παρουσιάζουν τιμή > 3, αποτελούν σημείο προσοχής με υψηλή επικινδυνότητα.



Εικόνα 36. RESIDUAL IMPACT - RISK

3.5 Συνολικά αποτελέσματα εκτίμησης επικινδυνότητας

Risk estimation

The frequency is also modelled from a simple scale:

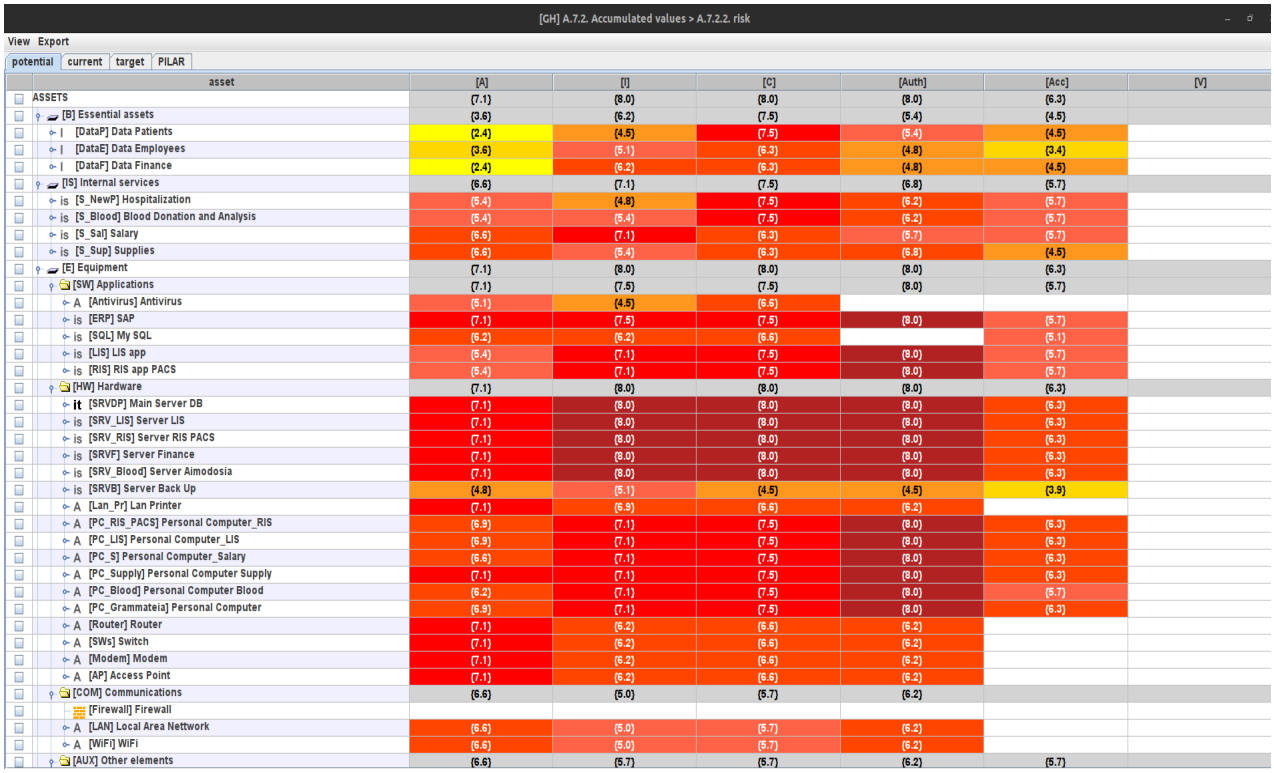
- **VF:** very frequent (daily)
- **F:** frequent (monthly)
- **NF:** normal frequency (yearly)
- **I:** infrequent (every few years)

The impact and the frequency can be combined into a table to calculate the risk:

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

Η εκτίμηση προκύπτει προσδιορίζοντας την ενδεχομένη και εναπομένουσα επίπτωση του υπό μελέτη συστήματος. Ταυτόχρονα, ταξινομούνται κατά προτεραιότητα τα αγαθά ή οι ομάδες αγαθών, με σειρά επίπτωσης ή επικινδυνότητας. Σκοπός είναι ο υπολογισμός της επίπτωσης της επικινδυνότητας και η κατανόηση των αποτελεσμάτων.

Κατά τη Magerit και το Pilar, υπολογίζετε η απομένουσα (residual) συνολική επικινδυνότητα συνυπολογίζοντας την συσσωρευμένη (accumulated) και την ανακλώμενη (deflected) επικινδυνότητα.
Η επικινδυνότητα που υπολογίζεται για κάθε αγαθό αθροίζεται (aggregated) όταν υπάρχουν συγκεκριμένα κριτήρια. Για τον υπολογισμό της επικινδυνότητας χρησιμοποιούνται προκαθορισμένοι πίνακες ή αλγοριθμική ανάλυση όπως βλέπουμε στον πίνακα παρακάτω.



[GH] A.7.2. Accumulated values > A.7.2.2. risk

View Export

potential | current | target | PILAR

asset	[A]	[I]	[C]	[Auth]	[Acc]	[V]
ASSETS	(7.1)	(8.0)	(8.0)	(8.0)	(6.3)	
[B] Essential assets	(3.6)	(6.2)	(7.5)	(5.4)	(4.5)	
[DataP] Data Patients	(2.4)	(4.5)	(7.5)	(5.4)	(4.5)	
[DataE] Data Employees	(3.6)	(5.1)	(6.3)	(4.8)	(3.4)	
[DataF] Data Finance	(2.4)	(6.2)	(6.3)	(4.8)	(4.5)	
[IS] Internal services	(6.6)	(7.1)	(7.5)	(6.8)	(5.7)	
[S_NewP] Hospitalization	(5.4)	(4.8)	(7.5)	(6.2)	(5.7)	
[S_Blood] Blood Donation and Analysis	(5.4)	(5.4)	(7.5)	(6.2)	(5.7)	
[S_Sal] Salary	(6.6)	(7.1)	(6.3)	(5.7)	(5.7)	
[S_Sup] Supplies	(6.6)	(5.4)	(6.3)	(6.8)	(4.5)	
[E] Equipment	(7.1)	(8.0)	(8.0)	(8.0)	(6.3)	
[SW] Applications	(7.1)	(7.5)	(7.5)	(8.0)	(5.7)	
[Antivirus] Antivirus	(5.1)	(4.5)	(6.6)			
[ERP] SAP	(7.1)	(7.5)	(7.5)	(8.0)	(5.7)	
[SQL] My SQL	(6.2)	(6.2)	(6.6)		(5.1)	
[LIS] LIS app	(5.4)	(7.1)	(7.5)	(8.0)	(5.7)	
[RIS] RIS app PACS	(5.4)	(7.1)	(7.5)	(8.0)	(5.7)	
[HW] Hardware	(7.1)	(8.0)	(8.0)	(8.0)	(6.3)	
[SRVDP] Main Server DB	(7.1)	(8.0)	(8.0)	(8.0)	(6.3)	
[SRV_LIS] Server LIS	(7.1)	(8.0)	(8.0)	(8.0)	(6.3)	
[SRV_RIS] Server RIS PACS	(7.1)	(8.0)	(8.0)	(8.0)	(6.3)	
[SRVF] Server Finance	(7.1)	(8.0)	(8.0)	(8.0)	(6.3)	
[SRV_Blood] Server Aimodosia	(7.1)	(8.0)	(8.0)	(8.0)	(6.3)	
[SRVB] Server Back Up	(4.8)	(5.1)	(4.5)	(4.5)	(3.9)	
[Lan_Pr] Lan Printer	(7.1)	(6.9)	(6.6)	(6.2)		
[PC_RIS_PACS] Personal Computer_RIS	(6.9)	(7.1)	(7.5)	(8.0)	(6.3)	
[PC_LIS] Personal Computer_LIS	(6.9)	(7.1)	(7.5)	(8.0)	(6.3)	
[PC_S] Personal Computer_Salary	(6.6)	(7.1)	(7.5)	(8.0)	(6.3)	
[PC_Supply] Personal Computer Supply	(7.1)	(7.1)	(7.5)	(8.0)	(6.3)	
[PC_Blood] Personal Computer Blood	(6.2)	(7.1)	(7.5)	(8.0)	(5.7)	
[PC_Grammateia] Personal Computer	(6.9)	(7.1)	(7.5)	(8.0)	(6.3)	
[Router] Router	(7.1)	(6.2)	(6.6)	(6.2)		
[SWs] Switch	(7.1)	(6.2)	(6.6)	(6.2)		
[Modem] Modem	(7.1)	(6.2)	(6.6)	(6.2)		
[AP] Access Point	(7.1)	(6.2)	(6.6)	(6.2)		
[COM] Communications	(6.6)	(5.0)	(5.7)	(6.2)		
[Firewall] Firewall						
[LAN] Local Area Nettwork	(6.6)	(5.0)	(5.7)	(6.2)		
[WiFi] WiFi	(6.6)	(5.0)	(5.7)	(6.2)		
[AUX] Other elements	(6.6)	(5.7)	(5.7)	(6.2)	(5.7)	

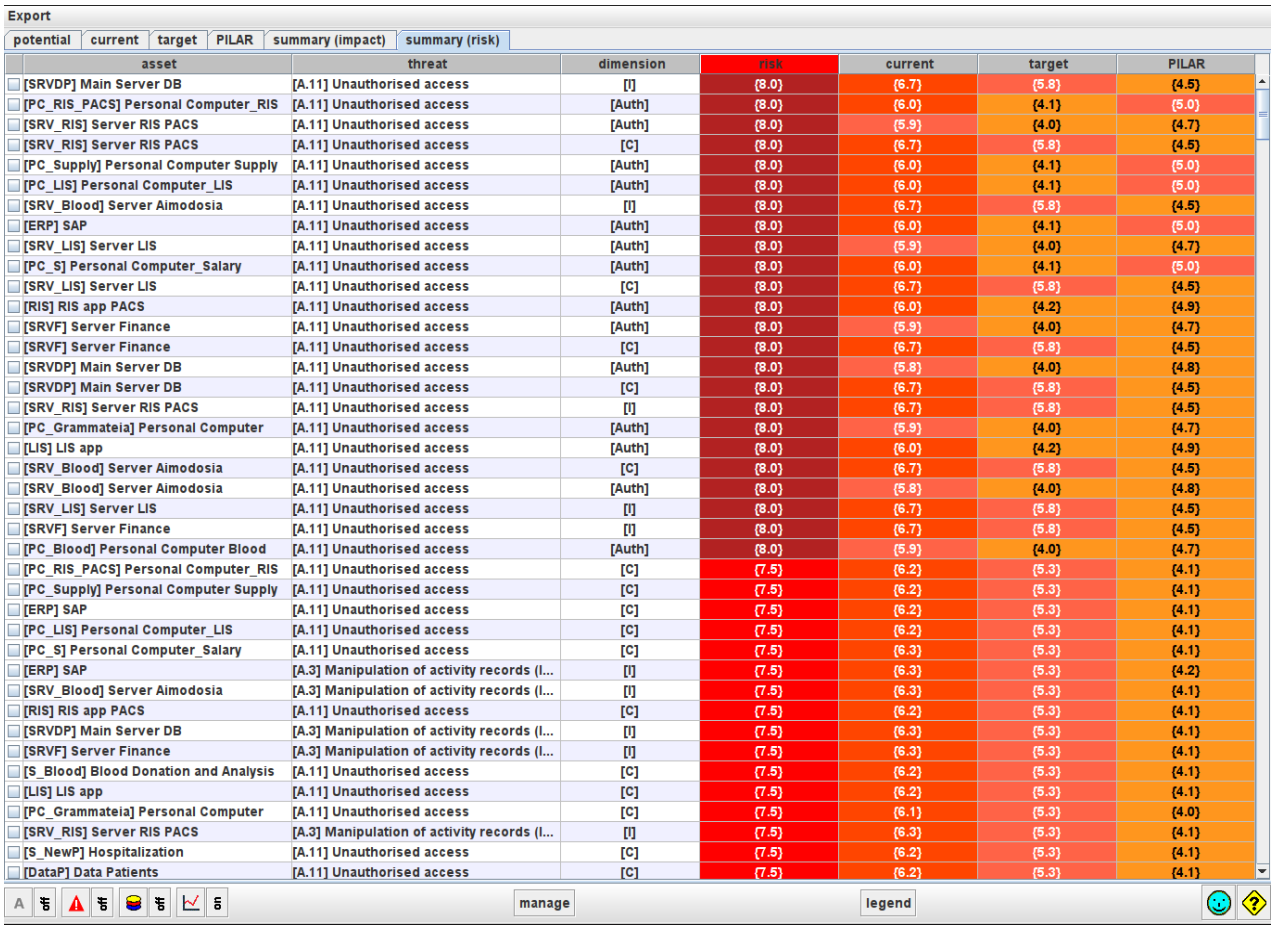
Εικόνα 37. RESIDUAL (ACCUMULATED-DEFLECTED) RISK

Κυριότερα σημεία επικινδυνότητας που χρήζουν αντιμετώπιση.

Ο **server** της αιμοδοσίας, είναι εγκατεστημένος σε σημείο με τα ελάχιστα πρότυπα ασφάλειας. Εκεί βρίσκεται και ο δρομολογητής και πάνω τους περνούν σωληνώσεις αποχέτευσης. Επίσης όλος ο εξοπλισμός βρίσκεται σε εμφανές σημείο, είναι τοποθετημένος δίπλα στο τζάμι της γραμματείας του τμήματος αιμοδοσίας.

Οι **κωδικοί πρόσβασης** είναι σχετικά γνωστοί ανάμεσα σε εργαζόμενους του Νοσοκομείου, κάτι που κάνει το σύστημα ευπαθές σε επιθέσεις social engineering. Ο κωδικός πρόσβασης πρέπει να αλλάζει ανά τακτά χρονικά διαστήματα και να κρατείτε μυστικός.

Το μη ενημερωμένο **antivirus**, σε κάποιους υπολογιστές που δεν έχουν πρόσβαση στο διαδίκτυο, με αποτέλεσμα να είναι επιρρεπείς σε επιθέσεις κακόβουλων χρηστών. Πρέπει να υπάρχει συχνή ενημέρωση του Antivirus.



asset	threat	dimension	risk	current	target	PILAR
[SRVDP] Main Server DB	[A.11] Unauthorised access	[I]	(8.0)	(6.7)	(5.8)	(4.5)
[PC_RIS_PACS] Personal Computer_RIS	[A.11] Unauthorised access	[Auth]	(8.0)	(6.0)	(4.1)	(5.0)
[SRV_RIS] Server RIS PACS	[A.11] Unauthorised access	[Auth]	(8.0)	(5.9)	(4.0)	(4.7)
[SRV_RIS] Server RIS PACS	[A.11] Unauthorised access	[C]	(8.0)	(6.7)	(5.8)	(4.5)
[PC_Supply] Personal Computer Supply	[A.11] Unauthorised access	[Auth]	(8.0)	(6.0)	(4.1)	(5.0)
[PC_LIS] Personal Computer_LIS	[A.11] Unauthorised access	[Auth]	(8.0)	(6.0)	(4.1)	(5.0)
[SRV_Blood] Server Aimodosia	[A.11] Unauthorised access	[I]	(8.0)	(6.7)	(5.8)	(4.5)
[ERP] SAP	[A.11] Unauthorised access	[Auth]	(8.0)	(6.0)	(4.1)	(5.0)
[SRV_LIS] Server LIS	[A.11] Unauthorised access	[Auth]	(8.0)	(5.9)	(4.0)	(4.7)
[PC_S] Personal Computer_Salary	[A.11] Unauthorised access	[Auth]	(8.0)	(6.0)	(4.1)	(5.0)
[SRV_LIS] Server LIS	[A.11] Unauthorised access	[C]	(8.0)	(6.7)	(5.8)	(4.5)
[RIS] RIS app PACS	[A.11] Unauthorised access	[Auth]	(8.0)	(6.0)	(4.2)	(4.9)
[SRVF] Server Finance	[A.11] Unauthorised access	[Auth]	(8.0)	(5.9)	(4.0)	(4.7)
[SRVF] Server Finance	[A.11] Unauthorised access	[C]	(8.0)	(6.7)	(5.8)	(4.5)
[SRVDP] Main Server DB	[A.11] Unauthorised access	[Auth]	(8.0)	(5.8)	(4.0)	(4.8)
[SRVDP] Main Server DB	[A.11] Unauthorised access	[C]	(8.0)	(6.7)	(5.8)	(4.5)
[SRV_RIS] Server RIS PACS	[A.11] Unauthorised access	[I]	(8.0)	(6.7)	(5.8)	(4.5)
[PC_Grammateia] Personal Computer	[A.11] Unauthorised access	[Auth]	(8.0)	(5.9)	(4.0)	(4.7)
[LIS] LIS app	[A.11] Unauthorised access	[Auth]	(8.0)	(6.0)	(4.2)	(4.9)
[SRV_Blood] Server Aimodosia	[A.11] Unauthorised access	[C]	(8.0)	(6.7)	(5.8)	(4.5)
[SRV_Blood] Server Aimodosia	[A.11] Unauthorised access	[Auth]	(8.0)	(5.8)	(4.0)	(4.8)
[SRV_LIS] Server LIS	[A.11] Unauthorised access	[I]	(8.0)	(6.7)	(5.8)	(4.5)
[SRVF] Server Finance	[A.11] Unauthorised access	[I]	(8.0)	(6.7)	(5.8)	(4.5)
[PC_Blood] Personal Computer Blood	[A.11] Unauthorised access	[Auth]	(8.0)	(5.9)	(4.0)	(4.7)
[PC_RIS_PACS] Personal Computer_RIS	[A.11] Unauthorised access	[C]	(7.5)	(6.2)	(5.3)	(4.1)
[PC_Supply] Personal Computer Supply	[A.11] Unauthorised access	[C]	(7.5)	(6.2)	(5.3)	(4.1)
[ERP] SAP	[A.11] Unauthorised access	[C]	(7.5)	(6.2)	(5.3)	(4.1)
[PC_LIS] Personal Computer_LIS	[A.11] Unauthorised access	[C]	(7.5)	(6.2)	(5.3)	(4.1)
[PC_S] Personal Computer_Salary	[A.11] Unauthorised access	[C]	(7.5)	(6.3)	(5.3)	(4.1)
[ERP] SAP	[A.3] Manipulation of activity records (I...	[I]	(7.5)	(6.3)	(5.3)	(4.2)
[SRV_Blood] Server Aimodosia	[A.3] Manipulation of activity records (I...	[I]	(7.5)	(6.3)	(5.3)	(4.1)
[RIS] RIS app PACS	[A.11] Unauthorised access	[C]	(7.5)	(6.2)	(5.3)	(4.1)
[SRVDP] Main Server DB	[A.3] Manipulation of activity records (I...	[I]	(7.5)	(6.3)	(5.3)	(4.1)
[SRVF] Server Finance	[A.3] Manipulation of activity records (I...	[I]	(7.5)	(6.3)	(5.3)	(4.1)
[S_Blood] Blood Donation and Analysis	[A.11] Unauthorised access	[C]	(7.5)	(6.2)	(5.3)	(4.1)
[LIS] LIS app	[A.11] Unauthorised access	[C]	(7.5)	(6.2)	(5.3)	(4.1)
[PC_Grammateia] Personal Computer	[A.11] Unauthorised access	[C]	(7.5)	(6.1)	(5.3)	(4.0)
[SRV_RIS] Server RIS PACS	[A.3] Manipulation of activity records (I...	[I]	(7.5)	(6.3)	(5.3)	(4.1)
[S_NewP] Hospitalization	[A.11] Unauthorised access	[C]	(7.5)	(6.2)	(5.3)	(4.1)
[DataP] Data Patients	[A.11] Unauthorised access	[C]	(7.5)	(6.2)	(5.3)	(4.1)

Εικόνα 38. Συνολική Επικινδυνότητα

Η απομένουσα_επικινδυνότητα (residual risk) υποδεικνύει ποια περιουσιακά στοιχεία πρέπει να προστατευθούν λαμβάνοντας υπόψη τα υφιστάμενα μέτρα (safeguards) στο πληροφοριακό σύστημα.
Ο ανακλώμενος κίνδυνος έχει λάβει υπόψη του τις αλληλεξαρτήσεις μεταξύ του κάθε κρίσιμου αγαθού και τις εξαρτήσεις με αυτό. Αν κάποιο αγαθό παραμένει με υψηλό βαθμό επικινδυνότητας σημαίνει ότι δεν αντιμετωπίζεται ικανοποιητικά από τα υφιστάμενα μέτρα προστασίας.
Η βαθμολογία του κινδύνου έχει υπολογιστεί με υποκειμενικό τρόπο αλλά δίνει μια σαφή εικόνα για το ποιες προτεραιότητες θα πρέπει να δοθούν στην αντιμετώπιση των κινδύνων. Η αποτίμηση περιλαμβάνει την συνολική αποτίμηση όλων των περιουσιακών στοιχείων που αλληλοεξαρτώνται, και τα υπάρχοντα μέτρα ασφαλείας.

4. ΔΙΑΧΕΙΡΗΣΗ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ

Η διαχείριση της επικινδυνότητας (**Risk Management**) ορίζεται ως μια συστηματική και συνεχή διαδικασία: *προσδιορισμού (identification), εκτίμησης (Assessment), μετριασμού (mitigate) και ελέγχου, των τεχνικών, λειτουργικών και άλλων ειδών κινδύνου (risks), καθώς και την εφαρμογή των ενδεδειγμένων μέτρων ασφαλείας και ελέγχων για την σωστή εφαρμογή τους* [Κάτσικας et al, 2004].

Η αξιολόγηση επικινδυνότητας, αναφέρεται σε μια αντικειμενική, επαναληπτική μέθοδο η οποία συλλέγει στοιχεία που αφορούν κινδύνους, απειλές, τρωτότητες και ελέγχους, υπολογίζοντας το μέγεθος της επικινδυνότητας για έναν οργανισμό και προτείνοντας μέτρα για τη μείωση του [Richard E. Mackey, 2011].

Στην διαχείριση κινδύνων, ο τελικός στόχος είναι να βρεθούν τα κατάλληλα μέτρα ασφάλειας έτσι ώστε είτε να μειωθεί είτε να διατηρηθεί ο κίνδυνος και να διαμορφωθεί ένα σχέδιο διαχείρισης του [Κάτσικας, 2014].

Σε περίπτωση παράβλεψης των κινδύνων υπάρχουν συνέπειες όπως[Chapman & Ward, 2009]:

- Στην υγεία και ασφάλεια των εμπλεκόμενων
- Στην φήμη - αξιοπιστία
- Στην εμπιστοσύνη των πελατών
- Στην οικονομική κατάσταση
- Στις υποδομές και περιβάλλον του οργανισμού,

Ακολουθεί μία αξιολόγηση των περιοχών με το μεγαλύτερο βαθμό επικινδυνότητας

Διαδίκτυο:(Sub. Services) Πραγματοποίηση της απειλής ενδέχεται να προκαλέσει συνέπειες όπως τη διακοπή της κανονικής ροής εργασιών του Οργανισμού και των καθημερινών δραστηριοτήτων.

Μέτρα μείωσης ενδεχόμενου πραγματοποίησης :

- Περιορισμός χρήσης του διαδικτύου, ώστε αυτό να χρησιμοποιείται μόνο για δραστηριότητες του Οργανισμού και όχι για την προσωπική χρήση των εργαζομένων.
- Εγκατάσταση (firewalls, proxy servers) για την υποστήριξη όσο το δυνατόν περισσότερο φορτίο στο δίκτυο.

Λογισμικό ERP:(Software) Πρόκειται για το κυρίως λογισμικό το οποίο χρησιμοποιεί το Νοσοκομείο για τη διεξαγωγή των λειτουργιών του. Η απειλή προέρχεται από την έλλειψη προσωπικού κωδικού πρόσβασης στο σύστημα που βρίσκεται εγκατεστημένη η εφαρμογή.

Μέτρα για την αντιμετώπιση:

- Είναι αναγκαίοι οι εμπιστευτικοί κωδικοί πρόσβασης για το σύστημα
- Προσαρμογή των κατάλληλων δικαιωμάτων πρόσβασης, ανάλογα με τη θέση εργασίας, την περιγραφή τής και το είδος των δεδομένων που απαιτούνται.

Antivirus:(Software) Η έλλειψη ενημερωμένου antivirus ενδέχεται να προκαλέσει τη διάδοση κακόβουλου λογισμικού στα συστήματα του Νοσοκομείου με αποτέλεσμα να προκαλέσει σοβαρές συνέπειες στην ακεραιότητα των δεδομένων και την εμπιστευτικότητα. Ο λόγος από τον οποίο απειλείται το σύστημα είναι η συχνή χρήση USB Stick για τη μεταφορά αρχείων.

Μέτρα για την αντιμετώπιση:

- Εγκατάσταση πλήρους ενημερωμένης εφαρμογής Antivirus.
- Ενημέρωση της βάσης δεδομένων της εφαρμογής κατά ελάχιστον 2 φορές το μήνα.
- Κατάργηση των θυρών εξωτερικών συνδέσεων USB από όλους τους υπολογιστές.

Λειτουργικό Σύστημα Υπολογιστών:(Software) Οι απειλές που αφορούν τη διάδοση κακόβουλου λογισμικού. Οφείλεται στην έλλειψη ενημερωμένου ιομορφικού λογισμικού. Ακόμα η μη ύπαρξη ενημερωμένων εφαρμογών ενδέχεται να προκαλέσει συνέπειες στην ακεραιότητα και στην εμπιστευτικότητα.

Μέτρα για την αντιμετώπιση:

- Απόκτηση λογισμικού με άδεια.
- Εγκατάσταση ενημερώσεων για το λογισμικό και το λειτουργικό σύστημα
- Άδεια εισόδου στο λειτουργικό σύστημα με ξεχωριστό κωδικό ανά υπάλληλο.

Εξυπηρετητής Αιμοδοσίας:(Hardware). Η πραγμάτωση απειλής που δίνει υψηλό βαθμό επικινδυνότητας είναι ο κακός χειρισμός εξοπλισμού ο οποίος ενδέχεται να επηρεάσει την εμπιστευτικότητα. Λόγω της κακής τοποθέτησης του εξοπλισμού σε ανασφαλές περιβάλλον. Ο εξοπλισμός των βάσεων δεδομένων βρίσκεται σε ένα κοινό δωμάτιο χωρίς έλεγχο πρόσβασης σε αυτό. Αυτό μπορεί να προκαλέσει την εσκεμμένη απώλεια ή υποκλοπή πληροφορίας.

Μέτρα για την αντιμετώπιση:

- Μεταφορά του server σε δωμάτιο με όλα τα προβλεπόμενα μέτρα ασφάλειας.
- Το δωμάτιο (server room) που θα μεταφερθεί ο server, θα πρέπει να προφυλάσσεται και από τις φυσικές καταστροφές.

Προσωπικοί υπολογιστές:(Hardware) Η απειλή με το μεγαλύτερο βαθμό επικινδυνότητας είναι η χρήση του εξοπλισμού αυτού για σκοπούς πέρα των επιτρεπόμενων. Οι υπάλληλοι ενδέχεται να εγκαταστήσουν προγράμματα που δεν σχετίζονται με την εργασία τους.

Μέτρα για την αντιμετώπιση:

- Κατάργηση δικαιώματος εγκατάστασης από τους κοινούς χρήστες, παρά μόνο από την ομάδα ων τεχνικών.

LAN:(Communication) Απειλές εντοπίστηκαν στην δρομολόγηση πακέτων. Δεν υπάρχουν κανόνες δρομολόγησης, ούτε μηχανισμοί αποτροπής μη εξουσιοδοτημένης πρόσβασης.

Μέτρα για την αντιμετώπιση:

- Κρυπτογράφηση των δεδομένων (εμπιστευτικότητα).
- Ψηφιακά πιστοποιητικά στις υπηρεσίες όπου ανταλλάσσονται δεδομένα, καθώς και η συχνή συντήρηση του τοπικού δικτύου.

Καλωδίωση εγκαταστάσεων:(Auxiliary). Η κακή ποιότητα της εγκατάστασης των καλωδιώσεων και της σύνδεσης του εξοπλισμού που βρίσκονται εκτεθειμένα. Προκαλείτε θόρυβος στην επικοινωνία μεταξύ των υπολογιστικών πόρων του Νοσοκομείου.

Μέτρα για την αντιμετώπιση:

- Σχεδιασμός εκ νέου όλων των συστατικών της καλωδίωσης.
- Αποφυγή διαδρομών της καλωδίωσης μέσα από κοινόχρηστους χώρους Προστασία από τη φθορά ή μη εξουσιοδοτημένης παρακολούθησης (χρήση θωρακισμένου αγωγού, κουτιά ή πέρασμα καλωδίωσης μέσα από κλειστούς χώρους)
- Διαχωρισμός ηλεκτρικής καλωδίωσης από δικτυακής, για αποφυγή παρεμβολών.

Κεντρικό Κτίριο:(Facilities). Το μοναδικό μέτρο προστασίας είναι η ύπαρξη ενός φρουρού στην κεντρική είσοδο.

Μέτρα για την αντιμετώπιση:

- Ενίσχυση του αριθμού των security, καθώς και τα συστήματα έκτακτης ανάγκης και προστασίας (συναγερμοί).
- Ενίσχυση καμερών ασφαλείας σε όλο το κτίριο (και όχι μόνο στο δωμάτιο των εξυπηρετητών).

Προσωπικό: Απειλές που αφορούν το προσωπικό. Η πρώτη απειλή εντοπίζεται στο social engineering. Κάποιοι εργαζόμενοι χρησιμοποιούν τους κωδικούς για την πρόσβαση στους υπολογιστές άλλων συναδέλφων τους, έχοντας πρόσβαση σε πληροφορίες που δεν θα έπρεπε να έχουν. Η δεύτερη απειλή εντοπίζεται στον εκβιασμό ή κακή χρήση της πληροφορίας που μπορεί να αποκτήσει κάποιος εις βάρος άλλου.

Μέτρα αντιμετώπισης:

- Πολιτική σχετική με τη διαχείριση του προσωπικού (ασφάλεια).
- Δημιουργία διαδικασιών ασφάλειας (περιστατικών έκτακτης ανάγκης).
- Αντίδραση για την πρόληψη του εκβιασμού. Πρόληψη και αντιμετώπιση των επιθέσεων social engineering.

Προτεινόμενα Μέτρα Ασφάλειας

Μη εξουσιοδοτημένη χρήση των εφαρμογών:

Να απαγορευθεί η εγκατάσταση προγραμμάτων (software) από μη εξουσιοδοτημένους χρήστες.

Αποφυγή χρήσης μη εγκεκριμένου λογισμικού.

Οι εργαζόμενοι να επαληθεύουν ότι το αποθηκευτικό μέσο που πρόκειται να χρησιμοποιήσουν δεν περιέχει κάποιας μορφής κακόβουλο λογισμικό. Ενδείκνυται η χρήση antivirus.

Ορθή χρήση Hardware:

Απαγόρευση μετακίνησης των υπολογιστών ή εγκατάσταση/απεγκατάσταση συσκευών.

Απαγ'ορευση τοποθέτησης αντικειμένων πάνω στον εξοπλισμό ή την κάλυψη των οπών εξαερισμού αυτού.

Συντήρηση εξοπλισμού η επισκευ'η μόνο από το αρμόδιο τμήμα.

Ευθύνη του εργαζομένου, και υποχρέωση να καλύψει την αξία της επισκευής ή την αντικατάσταση του επηρεαζόμενου εξοπλισμού.

Αντίγραφα ασφαλείας:

Χρήση των οπτικών μέσων μόνο για δημιουργία αντιγράφου ασφάλειας πληροφοριών.

Συχνή δημιουργία αντίγραφων ασφάλειας της ευαίσθητης και κρίσιμης πληροφορίας που υπάρχει στους υπολογιστές τους.

Χρήση των υπηρεσιών διαδικτύου:

Χρήση αποκλειστικών λογαριασμών.

Απαγορεύεται η οποιαδήποτε τροποποίηση της ταυτότητας των χρηστών από την ηλεκτρονική εφαρμογή.

Χρήση του διαδικτύου σχετικά με τις δραστηριοτήτες του τμήματος

Προστασία εγκαταστάσεων:

Πολιτικές πρόσβασης στους servers και τους σταθμούς εργασίας.

Διαχείριση του προσωπικού:

Πρέπει να υπάρχουν ρήτρες εμπιστευτικότητας για τη διασφάλιση των πληροφοριών τoy οργανισμού.

Οι χρήστες, οφείλουν να τηρούν της εμπιστευτικότητα της πληροφορίας.

Πολιτική καθαρού γραφείου.

Τα μέτρα και οι πολιτικές ασφαλείας του ΓΝ απαρτίζουν το σχέδιο ασφαλείας το οποίο πρέπει να εφαρμοστεί σωστά ώστε να επιτύχει το στόχο του.

5. ΣΥΜΠΕΡΑΣΜΑΤΑ

Στην παρούσα μελέτη ανάλυσης κινδύνων στο ΠΣ ΓΝ διερευνήθηκε ο βαθμός επικινδυνότητας των κρίσιμων περιουσιακών στοιχείων του ΠΣ του ΓΝ και προτάθηκαν μέτρα ασφαλείας για την αντιμετώπιση τους στα πλαίσια της διαχείρισης της επικινδυνότητας.
Σκοπός της μελέτης ήταν η ανάλυση και αποτίμηση των απειλών του ΠΣ του ΓΝ ώστε να υπολογιστεί με ποσοτικούς και ποιοτικούς όρους ο βαθμός επικινδυνότητας για κάθε συνδυασμό ανά απειλή - αγαθό.

Η συλλογή των δεδομένων για το ΠΣ του ΓΝ στηρίχθηκε στις απόψεις του προσωπικού του ΓΝ και θεωρείται υποκειμενική. Με βάση των απαντήσεων που δόθηκαν από το προσωπικό θα επηρεαστεί και η ακρίβεια των αποτελεσμάτων της ανάλυσης επικινδυνότητας.

Αναδείχθηκαν σημαντικά προβλήματα και ελλείψεις ασφαλείας και σημεία που πρέπει να μελετηθούν περαιτέρω. Σε συνάρτηση με το κόστος υλοποίησης που απαιτείται καταλήγουμε στο ότι τα περισσότερα μπορούν να επιλυθούν μέσα από το ίδιο τον οργανισμό. Η υλοποίηση των μέτρων ασφαλείας θα πρέπει να γίνεται σταδιακά καθώς και να πραγματοποιείτε η ανάλυση κινδύνων συνεχώς ως μια δυναμική διαδικασία.
Λόγω του ότι η ανάλυση και διαχείριση κινδύνων είναι δυναμική διαδικασία θα πρέπει να υπάρχει συνεχώς ανανέωση των ευπαθειών από την βάση του NIST καθώς επίσης και από τα μέτρα που έχουν εφαρμοστεί.

Θα πρέπει να γνωστοποιηθούν τα προβλήματα που σχετίζονται με την ασφάλεια του ΠΣ του ΓΝ:

• Συχνά περιστατικά ασφάλειας.
• Μελέτη των λειτουργιών του Νοσοκομείου που σχετίζονται με την εκπλήρωση της αποστολής και των εργασιών του ΓΝ.
• Αναβάθμιση των Υλικών και των Υπηρεσιών που απαιτούνται.
• Τεχνολογικές αλλαγές
• Ανάπτυξη νέων συστημάτων.
Συλλογή και αξιολόγηση μελετών ασφαλείας για τα ΠΣ του ΓΝ οργανογράμματα, απαιτήσεις, τεχνικές προδιαγραφές, πληροφορίες που να υποδεικνύουν τις κρίσιμες περιοχές από αποτελέσματα από προηγούμενες αναλύσεις επικινδυνότητας.

ΠΑΡΑΡΤΗΜΑ Α. Συλλογή Αγαθών - Ερωτηματολόγια

Α. ΕΡΩΤΗΜΑΤΟΛΟΓΙΑ

Ομάδα Ερωτήσεων		Καταγραφή/συλλογή πληροφοριών
Α	Γενικές Πληροφορίες Νοσοκομείου	Συλλογή δεδομένων που αφορούν α) την δομή του Νοσοκομείου β) τον αριθμό των τμημάτων του Νοσοκομείου.
Β	Γενικές Πληροφορίες Συνεντευξιαζόμενου	Συλλογή δεδομένων που αφορούν τον συνεντευξιαζόμενο.
Γ	Πληροφορίες διαχείρισης της ασφάλειας ψηφιακών υποδομών νοσοκομείου	Καταγραφή πληροφοριών.
		Καταγραφή των τύπων των συστημάτων και της IT υποδομής που χρησιμοποιούνται.
Δ	Πληροφορίες για την εφαρμογή των μέτρων ασφάλειας	Συλλογή δεδομένων σχετικά με τους παράγοντες που επηρεάζουν τη διαχείριση των ψηφιακών υποδομών.
Ε	Σχόλια	Γενικά σχόλια.

Α. Γενικές Πληροφορίες για το Νοσοκομείο

1: Αριθμός εργαζομένων;

2: Τμήματα;

3: Κάτοικοι εξυπηρέτησης του νοσοκομείου.

Β. Γενικές Πληροφορίες Συνεντευξιαζόμενου

1: Όνομα/επώνυμο και στοιχειά επικοινωνίας.

2: Ηλικία.

3: Φύλο.

4: Θέση εργασίας.

Γ. Πληροφορίες της Ασφάλειας Ψηφιακών Υποδομών Νοσοκομείου.

1: Ποιος είναι ο κύριός παράγοντας της διαχείρισης ασφάλειας των ψηφιακών υποδομών;

2: Η ασφάλεια είναι Διοικητικό θέμα, Τεχνικό θέμα ή και τα δύο;

3: Τι συμβάντα πρέπει να αντιμετωπίσει ένα νοσοκομείο έτσι ώστε να θεωρηθεί πως διαχειρίζεται αποτελεσματικά την ασφάλεια των ψηφιακών υποδομών;

4: Τι πρέπει να κάνει το ΓΝ για την διαχείριση της ασφάλειας των ψηφιακών υποδομών;

5: Πληροφορίες σχετικά με τον τύπο των συστημάτων που χρησιμοποιούνται στα πλαίσια της διαχείρισης της ασφάλειας των ψηφιακών υποδομών;

Δ. Πληροφορίες για την εφαρμογή των Μέτρων Ασφάλειας, των πολίτικων και του σχεδίου ασφάλειας.

1: Υπάρχει μελέτη για την διαχείριση της ασφάλειας;

2: Υπάρχουν γεγονότα σχετίζονται με την διαχείριση της ασφάλειας;

3: Χρειάζεται CISO;

4: Υπάρχει πολιτική καθαρού γραφείου;

5: Υπάρχει πολιτική ασύρματης επικοινωνίας;

6: Τι είναι το Σχέδιο Ανάκαμψης από Καταστροφή;

Ε. Σχόλια

Το εργαλείο EAR/PILAR συσχετίζει τα αγαθά σε υποκατηγορίες, που μπορούν να χρησιμοποιηθούν σαν **ερωτηματολόγια** προς τους αρμόδιους του οργανισμού για την καλύτερη κατηγοριοποίηση τους.

[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 organization 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	

Valuation (if applicable)		
dimension	***value***	***reason***

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

asset:	**degree:**
why?:	

asset:	**degree:**
why?:	

[HW] Hardware

[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	

Valuation (if applicable)		
dimension	***value***	***reason***

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

asset:	**degree:**
why?:	

asset:	**degree:**
why?:	

[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	

Valuation (if applicable)		
dimension	***value***	***reason***

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

asset:	**degree:**
why?:	

asset:	**degree:**
why?:	

[SI] Media

[SI] Media	
code:	**name:**
description:	
responsible:	
location:	
number:	
type (tick on all those that apply): ( ) [electronic] electronic ( ) [disk] disk ( ) [disquette] diskettes ( ) [cd] (CD-ROM) ( ) [usb] USB devices ( ) [dvd] DVD ( ) [tape] magnetic tape ( ) [mc] memory card ( ) [ic] intelligent cards ( ) [non_electronic] non-electronic ( ) [printed] printed paper ( ) [tape] paper tape ( ) [film] microfilm ( ) [cards] punched cards	

Valuation (if applicable)		
dimension	***value***	***reason***

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

asset:	**degree:**
why?:	

asset:	**degree:**
why?:	

[AUX] Auxiliary equipment

[AUX] Auxiliary equipment	
code:	**name:**
description:	
responsible:	
location:	
number:	
type (tick on all those that apply): ( ) [power] power supplies ( ) [ups] uninterruptible power supplies ( ) [gen] electrical generators ( ) [ac] air conditioning ( ) [cabling] cabling ( ) [robot] robots ( ) [tape] ... tapes ( ) [disk] ... disks ( ) [supply] essential supplies ( ) [destroy] media destruction equipment ( ) [furniture] furniture: cupboards, , etc ( ) [safe] safe	

Valuation (if applicable)		
dimension	***value***	***reason***

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

asset:	**asset:**
why?:	

asset:	**asset:**
why?:	

[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	

Valuation (if applicable)		
dimension	***value***	***reason***

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

asset:	**asset:**
why?:	

asset:	**asset:**
why?:	

[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	

Valuation (if applicable)		
dimension	***value***	***reason***

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

asset:	**asset:**
why?:	

asset:	**asset:**
why?:	

ΠΑΡΑΡΤΗΜΑ Β. Αποτίμηση Αγαθών

Value model

project: [GH] General Hospital

1. Project data

GH	General Hospital
organisation	Health Care
description	General Hospital in Athens
version	1
date	02/01/2023
system owner	Ioannis Skopelitis
library	[std] INFOSEC library (1.2.2022)

roles

is likely to result in high risk? (Art. 35.1; see WP 248)

- Evaluation or scoring
- Automated-decision making with legal or similar significant effect
- Systematic monitoring
- Sensitive data or data of a highly personal nature
- Data processes on a large scale
- Matching or combining datasets
- Data concerning vulnerable data subjects
- Innovative use or applying new technological or organisational solutions
- Prevents data subjects from exercising a right or using a service or a contract

data

controls

License

[edu] Information & Communication Systems Security

Dept. of Information & Communication Systems Eng.
Univ. of the Aegean
[... 1.3.2023]

2. Dimensions

[A] Availability
[I] Integrity
[C] Confidentiality
[Auth] Authenticity of users and information
[Acc] Accountability of service and data
[V] Value (eg. human lives, corporate assets, etc.)

3. Security domains

[base] Base

4. Assets

4.1. Domain: [base] Base

Layer: [B] Essential assets

[DataP] Data Patients
[DataE] Data Employees
[DataF] Data Finance

Layer: [IS] Internal services

[S_NewP] Hospitalization
[S_Blood] Blood Donation and Analysis
[S_Sal] Salary
[S_Sup] Supplies

Layer: [E] Equipment

[SW] Applications
- [Antivirus] Antivirus
- [ERP] SAP
- [SQL] My SQL
- [LIS] LIS app
- [RIS] RIS app PACS

[HW] Hardware
- [SRVDP] Main Server DB
- [SRV_LIS] Server LIS
- [SRV_RIS] Server RIS PACS
- [SRVF] Server Finance
- [SRV_Blood] Server Aimodosia
- [SRVB] Server Back Up
- [Lan_Pr] Lan Printer
- [PC_RIS_PACS] Personal Computer_RIS
- [PC_LIS] Personal Computer_LIS

[PC_S] Personal Computer_Salary
[PC_Supply] Personal Computer Supply
[PC_Blood] Personal Computer Blood
[PC_Grammateia] Personal Computer
[Router] Router
[SWs] Switch
[Modem] Modem
[AP] Access Point
[COM] Communications
[Firewall] Firewall
[LAN] Local Area Nettwork
[WiFi] WiFi
[AUX] Other elements
[Generator] Generator
[Cabling] Cabling
[Surveillans] Camera
[UPS] UPS
[Antena] Antena
[RFID] RFID reader
[UHF] UHF

Layer: [SS] Subcontracted services

[InternetP] Internet Provider
[Power] Electricity

Layer: [L] Facilities

[SRV_Room] Server Room
[Building] Building
[AirCon] Climatization
[Blood_Room] Blood Room
[Laboratories] Laboratories
[FD_Room] Financial Department

Layer: [P] Personnel

[MedS] Medical Staff
[IT] IS Engineer
[Admin] Administrative Staff
[OPS] Operators
[CU] Common User

4.2. valuation of assets

domain: [base] Base

layer: [B] Essential assets

asset	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[DataP] Data Patients	[7](1)	[6](2)	[9](3)	[6](4)	[7](5)	[6](6)
[DataE] Data Employees	[9](7)	[7](8)	[7](9)	[5](10)	[5](11)	[7](9)
[DataF] Data Finance	[7](12)	[9](13)	[7](14)	[5](15)	[7](12)	[6](16)

(1) Personal Information:
Classic
[5] is likely to cause significant distress to an individual
Legal and Regulatory Obligations:
[7] is likely to lead to a major breach of a legal or regulatory obligation
Disruption of Activities:
[7] Is likely to cause major disruption to activities within an organisation and with major impact on other organisations
[4] 4 hours < RTO < 1 day

(2) Personal Information:
Classic
[6] is likely to cause significant distress to a group of individuals
[5] is likely to cause significant distress to an individual

(3) Personal Information:
Classic
[6] is likely to cause significant distress to a group of individuals
Loss of Goodwill:
[9] Is likely to result in widespread adverse publicity for exceptionally seriously adversely affecting relations ...

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

(5) Legal and Regulatory Obligations:
[7] is likely to lead to a major breach of a legal or regulatory obligation

(6) Personal Information:
[6] is likely to cause a significant breach of a legal regulatory requirement for personal information
Legal and Regulatory Obligations:
[5] is likely to lead to a breach of a legal or regulatory obligation

(7) [5] is likely to cause significant distress to an individual
Legal and Regulatory Obligations:
[9] is likely to lead to an exceptionally serious breach of a legal or regulatory obligation
[5] is likely to lead to a breach of a legal or regulatory obligation
Disruption of Activities:
[5] Is likely to cause disruption to activities within an organisation and with some impact on other organisations

(8) [7] is likely to lead to a major breach of a legal or regulatory obligation
Disruption of Activities:
[5] Is likely to cause disruption to activities within an organisation and with some impact on other organisations

(9) [6] is likely to cause a significant breach of a legal regulatory requirement for personal information
[7] is likely to lead to a major breach of a legal or regulatory obligation

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

(11) Personal Information:
[5] is likely to cause significant distress to an individual
(12) [7] is likely to lead to a major breach of a legal or regulatory obligation
(13) [6] is likely to cause a significant breach of a legal regulatory requirement for personal information
[9] is likely to lead to an exceptionally serious breach of a legal or regulatory obligation
(14) [6] is likely to cause significant distress to a group of individuals
[7] is likely to lead to a major breach of a legal or regulatory obligation
(15) Legal and Regulatory Obligations:
(16) [6] is likely to cause a significant breach of a legal regulatory requirement for personal information
Legal and Regulatory Obligations:

layer: [E] Equipment

asset	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[Antivirus] Antivirus	[3]	[4]	[4]	[3]	[4]	
[ERP] SAP	[7]	[5]	[5]	[5]	[6]	
[SQL] My SQL	[6]	[6]	[5]	[4]	[8]	
[LIS] LIS app	[5]	[4]	[3]	[4]	[5]	
[RIS] RIS app PACS	[5]	[4]	[3]	[4]	[5]	
[SRVDP] Main Server DB	[6]	[6]	[5]	[4]	[5]	
[SRV_LIS] Server LIS	[5]	[5]	[4]	[3]	[4]	
[SRV_RIS] Server RIS PACS	[5]	[5]	[4]	[3]	[4]	
[SRVF] Server Finance	[5]	[5]	[4]	[3]	[4]	
[SRV_Blood] Server Aimodosia	[5]	[5]	[5]	[3]	[4]	
[SRVB] Server Back Up	[5]	[5]	[4]	[3]	[4]	
[Lan_Pr] Lan Printer	[5]	[3]	[4]	[3]	[4]	
[PC_RIS_PACS] Personal Computer_RIS	[5]	[3]	[4]	[4]	[5]	
[PC_LIS] Personal Computer_LIS	[5]	[3]	[4]	[4]	[5]	
[PC_S] Personal Computer_Salary	[5]	[3]	[4]	[4]	[5]	
[PC_Supply] Personal Computer Supply	[5]	[3]	[4]	[4]	[5]	
[PC_Blood] Personal Computer Blood	[5]	[3]	[4]	[4]	[5]	
[PC_Grammateia] Personal Computer	[5]	[3]	[4]	[4]	[5]	

[Router] Router	[5]	[4]	[4]	[3]	[5]	
[SWs] Switch	[5]	[4]	[4]	[3]	[5]	
[Modem] Modem	[5]	[4]	[4]	[3]	[5]	
[AP] Access Point	[5]	[4]	[4]	[3]	[5]	
[Firewall] Firewall	[6]					
[LAN] Local Area Nettwork	[4]	[3]	[4]	[4]	[5]	
[WiFi] WiFi	[3]	[4]	[3]	[4]	[6]	
[Generator] Generator	[5]	[3]	[4]	[4]	[5]	
[Cabling] Cabling	[5]	[3]	[4]	[4]	[6]	
[Surveillans] Camera	[4]					
[UPS] UPS	[5]	[3]	[4]	[4]	[5]	
[Antena] Antena	[2]	[1]	[1]	[2]	[1]	
[RFID] RFID reader	[4]					

layer: [SS] Subcontracted services

asset	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[InternetP] Internet Provider	[3]	[3]	[3]	[2]	[4]	
[Power] Electricity	[6]	[3]	[4]	[4]	[4]	

layer: [L] Facilities

asset	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[SRV_Room] Server Room	[7]	[3]	[4]	[7]	[7]	
[Building] Building	[3]	[3]	[4]	[4]	[5]	
[AirCon] Climatization	[5]	[3]	[4]	[4]	[5]	
[Blood_Room] Blood Room	[4]	[3]	[4]	[4]	[5]	
[Laboratories] Laboratories	[4]	[3]	[4]	[4]	[5]	
[FD_Room] Financial Department	[4]	[3]	[4]	[4]	[5]	

layer: [P] Personnel

asset	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[MedS] Medical Staff	[4]	[5]	[8]	[5]	[6]	
[IT] IS Engineer	[4]	[3]	[3]	[3]	[6]	
[Admin] Administrative Staff	[4]	[5]	[8]	[5]	[6]	
[OPS] Operators	[4]	[3]	[6]	[4]	[6]	
[CU] Common User	[4]	[5]	[6]	[4]	[6]	

ΠΑΡΑΡΤΗΜΑ Γ. Πίνακας Απειλών/Αγαθό

project: [GH] General Hospital

Project data

GH	General Hospital
organisation	Health Care
description	General Hospital in Athens
version	1
date	02/01/2023
system owner	Ioannis Skopelitis
library	[std] INFOSEC library (1.2.2022)

roles

is likely to result in high risk? (Art. 35.1; see WP 248)

Evaluation or scoring

Automated-decision making with legal or similar significant effect

Systematic monitoring

Sensitive data or data of a highly personal nature

Data processes on a large scale

Matching or combining datasets

Data concerning vulnerable data subjects

Innovative use or applying new technological or organisational solutions

Prevents data subjects from exercising a right or using a service or a contract

data

controls

License

Dimensions

[A] Availability
[I] Integrity
[C] Confidentiality
[Auth] Authenticity of users and information
[Acc] Accountability of service and data
[V] Value (eg. human lives, corporate assets, etc.)

Security domains

[base] Base

threats / asset

[DataP] Data Patients

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[E.15] Accidental alteration of the information	1	-	50 %	-	-	-	-
[E.18] Destruction of information	1	1%	-	-	-	-	-
[E.19] Information leaks	1	-	-	10%	-	-	-
[A.5] Masquerading of identity	10	-	10 %	50%	100%	-	-
[A.6] Abuse of access privileges	10	1%	10 %	50%	50%	-	-
[A.7] Misuse	1	-	50 %	100 %	-	-	-
[A.11] Unauthorised access	100	-	10 %	50%	-	-	-
[A.13] Repudiation (denial of actions)	1	-	-	-	-	50%	-

[DataE] Data Employees

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[E.15] Accidental alteration of the information	1	-	1%	-	-	-	-
[E.18] Destruction of information	1	1%	-	-	-	-	-
[E.19] Information leaks	1	-	-	10 %	-	-	-
[A.5] Masquerading of identity	10	-	10 %	50 %	100%	-	-
[A.6] Abuse of access privileges	10	1%	10	50	-	-	-

			%	%			
[A.11] Unauthorised access	100	-	10 %	50 %	-	-	-
[A.13] Repudiation (denial of actions)	1	-	-	-	-	50%	-

[DataF] Data Finance

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[E.15] Accidental alteration of the information	1	-	1%	-	-	-	-
[E.18] Destruction of information	1	1%	-	-	-	-	-
[E.19] Information leaks	1	-	-	10 %	-	-	-
[A.5] Masquerading of identity	10	-	10 %	50 %	100%	-	-
[A.6] Abuse of access privileges	10	1%	10 %	50 %	-	-	-
[A.11] Unauthorised access	100	-	10 %	50 %	-	-	-
[A.13] Repudiation (denial of actions)	1	-	-	-	-	50%	-

[S_NewP] Hospitalization

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[E.1] User errors	1	10 %	10 %	10 %	-	-	-
[E.2] System / Security administrator errors	1	20 %	20 %	20 %	-	-	-
[E.15] Accidental alteration of the information	1	-	10 %	-	-	-	-
[E.18] Destruction of information	1	10 %	-	-	-	-	-
[E.19] Information leaks	1	-	-	10 %	-	-	-
[E.24] System failure due to exhaustion of resources	10	50 %	-	-	-	-	-
[E.28] Staff shortage	1	10 %	-	-	-	-	-
[A.5] Masquerading of identity	10	-	50 %	50 %	100%	-	-
[A.6] Abuse of access privileges	10	1%	10 %	50 %	100%	-	-
[A.7] Misuse	1	1%	10 %	10 %	-	-	-
[A.11] Unauthorised access	100	-	10	50	100%	-	-

			%	%			
[A.13] Repudiation (denial of actions)	5	-	-	-	-	100 %	-
[A.15] Deliberate alteration of information	10	-	50 %	-	-	-	-
[A.18] Destruction of information	1	50 %	-	-	-	-	-
[A.19] Disclosure of information	10	-	-	20 %	-	-	-
[A.24] Denial of service	10	50 %	-	-	-	-	-
[A.28] Staff shortage	0.5	50 %	-	-	-	-	-
[A.29] Extortion	0.9	10 %	20 %	20 %	-	-	-
[A.30] Social engineering	0.5	10 %	20 %	20 %	-	-	-

[S_Blood] Blood Donation and Analysis

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[N.1] Fire	0.1	100 %	-	-	-	-	-
[N.2] Water	0.1	50%	-	-	-	-	-
[N.*] Other natural disasters	0.1	100 %	-	-	-	-	-
[I.1] Fire	0.5	100 %	-	-	-	-	-
[I.2] Water	0.5	50%	-	-	-	-	-
[I.*] Other industrial disasters	0.5	100 %	-	-	-	-	-
[I.3] Environmental pollution	1	50%	-	-	-	-	-
[I.4] Electromagnetic pollution	1	10%	-	-	-	-	-
[I.5.2] Hardware failure	1	50%	-	-	-	-	-
[I.6] Power interruption	1	100 %	-	-	-	-	-
[I.7] Unsuitable temperature or humidity conditions	1	100 %	-	-	-	-	-
[I.10] Media degradation	1	100 %	-	-	-	-	-
[I.11] Electromagnetic emanations (TEMPEST)	1	-	-	1%	-	-	-
[E.1] User errors	1	10%	10%	10%	-	-	-
[E.2] System / Security administrator errors	1	20%	20%	20%	-	-	-
[E.15] Accidental alteration of the information	1	-	10%	-	-	-	-

[E.18] Destruction of information	1	100 %	-	-	-	-	-
[E.19] Information leaks	1	-	-	10%	-	-	-
[E.23] Defects in hardware maintenance / updating	1	100 %	10%	50%	-	-	-
[E.24] System failure due to exhaustion of resources	10	50%	-	-	-	-	-
[E.25] Equipment loss	1	10%	-	50%	-	-	-
[E.28] Staff shortage	1	10%	-	-	-	-	-
[A.5] Masquerading of identity	10	-	50%	50%	100 %	-	-
[A.6] Abuse of access privileges	10	1%	10%	50%	100 %	-	-
[A.7] Misuse	1	1%	10%	10%	-	-	-
[A.11] Unauthorised access	100	-	10%	50%	100 %	-	-
[A.13] Repudiation (denial of actions)	5	-	-	-	-	100 %	-
[A.15] Deliberate alteration of information	10	-	100 %	-	-	-	-
[A.18] Destruction of information	1	100 %	-	-	-	-	-
[A.19] Disclosure of information	10	-	-	20%	-	-	-
[A.23] Hardware manipulation	0.1	50%	-	50%	-	-	-
[A.24] Denial of service	10	50%	-	-	-	-	-
[A.25] Theft	1	10%	-	100 %	-	-	-
[A.26] Destructive attack	1	10%	-	-	-	-	-
[A.28] Staff shortage	0.5	50%	-	-	-	-	-
[A.29] Extortion	0.9	10%	20%	20%	-	-	-
[A.30] Social engineering	0.5	10%	20%	20%	-	-	-

[S_Sal] Salary

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[N.1] Fire	0.1	100 %	-	-	-	-	-
[N.2] Water	0.1	50%	-	-	-	-	-
[N.*] Other natural disasters	0.1	100 %	-	-	-	-	-
[I.1] Fire	0.5	100 %	-	-	-	-	-
[I.2] Water	0.5	50%	-	-	-	-	-

[I.*] Other industrial disasters	0.5	100 %	-	-	-	-	-
[I.3] Environmental pollution	1	50%	-	-	-	-	-
[I.5.1] Software failure	1	50%	-	-	-	-	-
[I.7] Unsuitable temperature or humidity conditions	1	100 %	-	-	-	-	-
[I.10] Media degradation	1	100 %	-	-	-	-	-
[E.1] User errors	1	10%	10%	10%	-	-	-
[E.2] System / Security administrator errors	1	20%	20%	20%	-	-	-
[E.8] Malware diffusion	1	10%	10%	10%	-	-	-
[E.15] Accidental alteration of the information	1	-	10%	-	-	-	-
[E.18] Destruction of information	1	100 %	-	-	-	-	-
[E.19] Information leaks	1	-	-	10%	-	-	-
[E.20] Software vulnerabilities	1	1%	20%	20%	-	-	-
[E.21] Defects in software maintenance / updating	10	1%	10%	50%	-	-	-
[E.24] System failure due to exhaustion of resources	10	50%	-	-	-	-	-
[E.25] Equipment loss	1	10%	-	50%	-	-	-
[E.28] Staff shortage	1	10%	-	-	-	-	-
[A.5] Masquerading of identity	10	-	50%	50%	100 %	-	-
[A.6] Abuse of access privileges	10	1%	10%	50%	100 %	-	-
[A.7] Misuse	1	10%	10%	50%	-	-	-
[A.8] Malware diffusion	1	100 %	100 %	100 %	-	-	-
[A.11] Unauthorised access	100	-	10%	50%	100 %	-	-
[A.13] Repudiation (denial of actions)	5	-	-	-	-	100 %	-
[A.15] Deliberate alteration of information	10	-	100 %	-	-	-	-
[A.18] Destruction of information	1	100 %	-	-	-	-	-
[A.19] Disclosure of information	10	-	-	20%	-	-	-
[A.22] Software manipulation	1	50%	100 %	100 %	-	-	-
[A.24] Denial of service	10	50%	-	-	-	-	-
[A.25] Theft	1	10%	-	100 %	-	-	-
[A.26] Destructive attack	1	10%	-	-	-	-	-
[A.28] Staff shortage	0.5	50%	-	-	-	-	-
[A.29] Extortion	0.9	10%	20%	20%	-	-	-

[A.30] Social engineering	0.5	10%	20%	20%	-	-	-

[S_Sup] Supplies

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[E.1] User errors	1	10 %	10 %	10 %	-	-	-
[E.2] System / Security administrator errors	1	20 %	20 %	20 %	-	-	-
[E.15] Accidental alteration of the information	1	-	10 %	-	-	-	-
[E.18] Destruction of information	1	10 %	-	-	-	-	-
[E.19] Information leaks	1	-	-	10 %	-	-	-
[E.24] System failure due to exhaustion of resources	10	50 %	-	-	-	-	-
[E.28] Staff shortage	1	10 %	-	-	-	-	-
[A.5] Masquerading of identity	10	-	50 %	50 %	100%	-	-
[A.6] Abuse of access privileges	10	1%	10 %	50 %	100%	-	-
[A.7] Misuse	1	1%	10 %	10 %	-	-	-
[A.11] Unauthorised access	100	-	10 %	50 %	100%	-	-
[A.13] Repudiation (denial of actions)	5	-	-	-	-	100 %	-
[A.15] Deliberate alteration of information	10	-	50 %	-	-	-	-
[A.18] Destruction of information	1	50 %	-	-	-	-	-
[A.19] Disclosure of information	10	-	-	20 %	-	-	-
[A.24] Denial of service	10	50 %	-	-	-	-	-
[A.28] Staff shortage	0.5	50 %	-	-	-	-	-
[A.29] Extortion	0.9	10 %	20 %	20 %	-	-	-
[A.30] Social engineering	0.5	10 %	20 %	20 %	-	-	-

[Antivirus] Antivirus

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[I.5.1] Software failure	1	50%	-	-	-	-	-
[E.8] Malware diffusion	1	10%	10%	10%	-	-	-
[E.20] Software vulnerabilities	1	1%	20%	20%	-	-	-
[E.21] Defects in software maintenance / updating	10	1%	10%	50%	-	-	-
[A.7] Misuse	1	10%	10%	50%	-	-	-
[A.8] Malware diffusion	1	100 %	100 %	100 %	-	-	-
[A.22] Software manipulation	1	50%	100 %	100 %	-	-	-

[ERP] SAP

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[N.1] Fire	0.1	100 %	-	-	-	-	-
[N.2] Water	0.1	50%	-	-	-	-	-
[N.*] Other natural disasters	0.1	100 %	-	-	-	-	-
[I.1] Fire	0.5	100 %	-	-	-	-	-
[I.2] Water	0.5	50%	-	-	-	-	-
[I.*] Other industrial disasters	0.5	100 %	-	-	-	-	-
[I.3] Environmental pollution	0.1	50%	-	-	-	-	-
[I.4] Electromagnetic pollution	1	10%	-	-	-	-	-
[I.5.1] Software failure	1	50%	-	-	-	-	-
[I.5.2] Hardware failure	1	50%	-	-	-	-	-
[I.6] Power interruption	1	100 %	-	-	-	-	-
[I.7] Unsuitable temperature or humidity conditions	1	100 %	-	-	-	-	-
[I.8] Communications services failure	1	50%	-	-	-	-	-
[I.11] Electromagnetic emanations (TEMPEST)	1	-	-	1%	-	-	-

[E.1] User errors	1	10%	10%	10%	-	-	-
[E.2] System / Security administrator errors	1	20%	20%	20%	-	-	-
[E.3] Monitoring errors (log)	1	-	1%	-	-	-	-
[E.8] Malware diffusion	1	10%	10%	10%	-	-	-
[E.9] [Re-]routing errors	1	-	-	10%	-	-	-
[E.10] Sequence errors	1	-	10%	-	-	-	-
[E.15] Accidental alteration of the information	1	-	10%	-	-	-	-
[E.18] Destruction of information	1	10%	-	-	-	-	-
[E.19] Information leaks	1	-	-	10%	-	-	-
[E.20] Software vulnerabilities	1	1%	20%	20%	-	-	-
[E.21] Defects in software maintenance / updating	10	1%	10%	50%	-	-	-
[E.23] Defects in hardware maintenance / updating	1	10%	-	-	-	-	-
[E.24] System failure due to exhaustion of resources	10	50%	-	-	-	-	-
[E.25] Equipment loss	5	100 %	-	100 %	-	-	-
[E.28] Staff shortage	1	30%	-	-	-	-	-
[A.3] Manipulation of activity records (log)	100	-	50%	-	-	-	-
[A.5] Masquerading of identity	10	-	50%	50%	100 %	-	-
[A.6] Abuse of access privileges	10	1%	10%	50%	100 %	-	-
[A.7] Misuse	1	10%	10%	50%	-	-	-
[A.8] Malware diffusion	1	100 %	100 %	100 %	-	-	-
[A.9] [Re-]routing of messages	1	-	-	10%	-	-	-
[A.10] Sequence alteration	1	-	10%	-	-	-	-
[A.11] Unauthorised access	100	10%	10%	50%	100 %	-	-
[A.12] Traffic analysis	1	-	-	2%	-	-	-
[A.13] Repudiation (denial of actions)	5	-	-	-	-	100 %	-
[A.14] Eavesdropping	1	-	-	10%	-	-	-
[A.15] Deliberate alteration of information	10	-	50%	-	-	-	-
[A.18] Destruction of information	1	50%	-	-	-	-	-
[A.19] Disclosure of information	10	-	-	50%	-	-	-
[A.22] Software manipulation	1	50%	100 %	100 %	-	-	-
[A.23] Hardware manipulation	0.5	50%	-	50%	-	-	-
[A.24] Denial of service	10	100 %	-	-	-	-	-
[A.25] Theft	5	100 %	-	100 %	-	-	-
[A.26] Destructive attack	1	100	-	-	-	-	-

		%					
[A.28] Staff shortage	0.5	50%	-	-	-	-	-
[A.29] Extortion	0.9	50%	100 %	100 %	-	-	-
[A.30] Social engineering	0.5	50%	100 %	100 %	-	-	-

[SQL] My SQL

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[I.5.1] Software failure	1	50%	-	-	-	-	-
[E.8] Malware diffusion	1	10%	10%	10%	-	-	-
[E.20] Software vulnerabilities	1	1%	20%	20%	-	-	-
[E.21] Defects in software maintenance / updating	10	1%	10%	50%	-	-	-
[A.7] Misuse	1	10%	10%	50%	-	-	-
[A.8] Malware diffusion	1	100 %	100 %	100 %	-	-	-
[A.13] Repudiation (denial of actions)	1	-	-	-	-	50 %	-
[A.22] Software manipulation	1	50%	100 %	100 %	-	-	-

[LIS] LIS app

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[I.5.1] Software failure	1	50%	-	-	-	-	-
[I.9] Interruption of other services or essential supplies	1	50%	-	-	-	-	-
[E.1] User errors	1	10%	10%	10 %	-	-	-
[E.2] System / Security administrator errors	1	20%	20%	20 %	-	-	-
[E.8] Malware diffusion	1	10%	10%	10 %	-	-	-
[E.15] Accidental alteration of the information	1	-	10%	-	-	-	-
[E.18] Destruction of information	1	10%	-	-	-	-	-
[E.19] Information leaks	1	-	-	10 %	-	-	-
[E.20] Software vulnerabilities	1	1%	20%	20 %	-	-	-
[E.21] Defects in software maintenance / updating	10	1%	10%	50	-	-	-

				%			
[E.24] System failure due to exhaustion of resources	10	50%	-	-	-	-	-
[A.5] Masquerading of identity	10	-	100 %	100 %	100 %	-	-
[A.6] Abuse of access privileges	10	1%	10%	50 %	100 %	-	-
[A.7] Misuse	1	10%	10%	50 %	-	-	-
[A.8] Malware diffusion	1	100 %	100 %	100 %	-	-	-
[A.11] Unauthorised access	100	-	10%	50 %	100 %	-	-
[A.13] Repudiation (denial of actions)	5	-	-	-	-	100 %	-
[A.15] Deliberate alteration of information	10	-	50%	-	-	-	-
[A.18] Destruction of information	1	50%	-	-	-	-	-
[A.19] Disclosure of information	1	-	-	50 %	-	-	-
[A.22] Software manipulation	1	50%	100 %	100 %	-	-	-
[A.24] Denial of service	10	50%	-	-	-	-	-

[RIS] RIS app PACS

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[I.5.1] Software failure	1	50%	-	-	-	-	-
[I.9] Interruption of other services or essential supplies	1	50%	-	-	-	-	-
[E.1] User errors	1	10%	10%	10 %	-	-	-
[E.2] System / Security administrator errors	1	20%	20%	20 %	-	-	-
[E.8] Malware diffusion	1	10%	10%	10 %	-	-	-
[E.15] Accidental alteration of the information	1	-	10%	-	-	-	-
[E.18] Destruction of information	1	10%	-	-	-	-	-
[E.19] Information leaks	1	-	-	10 %	-	-	-
[E.20] Software vulnerabilities	1	1%	20%	20	-	-	-

				%			
[E.21] Defects in software maintenance / updating	10	1%	10%	50 %	-	-	-
[E.24] System failure due to exhaustion of resources	10	50%	-	-	-	-	-
[A.5] Masquerading of identity	10	-	100 %	100 %	10 0 %	-	-
[A.6] Abuse of access privileges	10	1%	10%	50 %	10 0 %	-	-
[A.7] Misuse	1	10%	10%	50 %	-	-	-
[A.8] Malware diffusion	1	100 %	100 %	100 %	-	-	-
[A.11] Unauthorised access	100	-	10%	50 %	10 0 %	-	-
[A.13] Repudiation (denial of actions)	5	-	-	-	-	10 0 %	-
[A.15] Deliberate alteration of information	10	-	50%	-	-	-	-
[A.18] Destruction of information	1	50%	-	-	-	-	-
[A.19] Disclosure of information	1	-	-	50 %	-	-	-
[A.22] Software manipulation	1	50%	100 %	100 %	-	-	-
[A.24] Denial of service	10	50%	-	-	-	-	-

[SRVDP] Main Server DB

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[N.1] Fire	1	100 %	-	-	-	-	-
[N.2] Water	1	100 %	-	-	-	-	-
[N.*] Other natural disasters	0.5	100 %	-	-	-	-	-
[I.1] Fire	1	100 %	-	-	-	-	-
[I.2] Water	1	100 %	-	-	-	-	-
[I.*] Other industrial disasters	1	100 %	-	-	-	-	-

[I.3] Environmental pollution	1	50%	-	-	-	-	-
[I.4] Electromagnetic pollution	1	10%	-	-	-	-	-
[I.5.1] Software failure	1	50%	-	-	-	-	-
[I.5.2] Hardware failure	1	50%	-	-	-	-	-
[I.6] Power interruption	1	100 %	-	-	-	-	-
[I.7] Unsuitable temperature or humidity conditions	1	100 %	-	-	-	-	-
[I.8] Communications services failure	1	50%	-	-	-	-	-
[I.10] Media degradation	1	100 %	-	-	-	-	-
[I.11] Electromagnetic emanations (TEMPEST)	1	-	-	1%	-	-	-
[E.1] User errors	1	10%	10%	10%	-	-	-
[E.2] System / Security administrator errors	1	20%	20%	20%	-	-	-
[E.3] Monitoring errors (log)	1	-	1%	-	-	-	-
[E.4] Configuration errors	1	-	1%	-	-	-	-
[E.8] Malware diffusion	1	10%	10%	10%	-	-	-
[E.9] [Re-]routing errors	1	-	-	10%	-	-	-
[E.10] Sequence errors	1	-	10%	-	-	-	-
[E.15] Accidental alteration of the information	1	-	50%	-	-	-	-
[E.18] Destruction of information	1	100 %	-	-	-	-	-
[E.19] Information leaks	1	-	-	10%	-	-	-
[E.20] Software vulnerabilities	1	1%	20%	20%	-	-	-
[E.21] Defects in software maintenance / updating	10	1%	10%	50%	-	-	-
[E.23] Defects in hardware maintenance / updating	1	100 %	10%	50%	-	-	-
[E.24] System failure due to exhaustion of resources	10	50%	-	-	-	-	-
[E.25] Equipment loss	1	100 %	-	100 %	-	-	-
[E.28] Staff shortage	1	20%	-	-	-	-	-
[A.3] Manipulation of activity records (log)	100	-	50%	-	-	-	-
[A.4] Manipulation of the configuration files	10	10%	10%	10%	-	-	-
[A.5] Masquerading of identity	10	-	50%	50%	100 %	-	-
[A.6] Abuse of access privileges	10	10%	100 %	100 %	100 %	-	-
[A.7] Misuse	1	50%	50%	100 %	-	-	-
[A.8] Malware diffusion	1	100 %	100 %	100 %	-	-	-
[A.9] [Re-]routing of messages	1	-	-	10%	-	-	-
[A.10] Sequence alteration	1	-	10%	-	-	-	-
[A.11] Unauthorised access	100	10%	100 %	100 %	100 %	-	-

[A.12] Traffic analysis	1	-	-	2%	-	-	-
[A.13] Repudiation (denial of actions)	5	-	-	-	-	100 %	-
[A.14] Eavesdropping	1	-	-	1%	-	-	-
[A.15] Deliberate alteration of information	10	-	100 %	-	-	-	-
[A.18] Destruction of information	1	100 %	-	-	-	-	-
[A.19] Disclosure of information	10	-	-	50%	-	-	-
[A.22] Software manipulation	1	50%	100 %	100 %	-	-	-
[A.23] Hardware manipulation	1	50%	-	50%	-	-	-
[A.24] Denial of service	10	100 %	-	-	-	-	-
[A.25] Theft	1	100 %	-	100 %	-	-	-
[A.26] Destructive attack	1	100 %	-	-	-	-	-
[A.27] Enemy over-run	1	100 %	-	-	-	-	-
[A.28] Staff shortage	0.5	20%	-	-	-	-	-
[A.29] Extortion	0.9	50%	100 %	100 %	-	-	-
[A.30] Social engineering	0.5	50%	100 %	100 %	-	-	-

[SRV_LIS] Server LIS

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[N.1] Fire	1	100 %	-	-	-	-	-
[N.2] Water	1	100 %	-	-	-	-	-
[N.*] Other natural disasters	0.5	100 %	-	-	-	-	-
[I.1] Fire	1	100 %	-	-	-	-	-
[I.2] Water	1	100 %	-	-	-	-	-
[I.*] Other industrial disasters	1	100 %	-	-	-	-	-
[I.3] Environmental pollution	1	50%	-	-	-	-	-
[I.4] Electromagnetic pollution	1	10%	-	-	-	-	-

[I.5.1] Software failure	1	50%	-	-	-	-	-
[I.5.2] Hardware failure	1	50%	-	-	-	-	-
[I.6] Power interruption	1	100 %	-	-	-	-	-
[I.7] Unsuitable temperature or humidity conditions	1	100 %	-	-	-	-	-
[I.8] Communications services failure	1	50%	-	-	-	-	-
[I.9] Interruption of other services or essential supplies	1	50%	-	-	-	-	-
[I.10] Media degradation	1	100 %	-	-	-	-	-
[I.11] Electromagnetic emanations (TEMPEST)	1	-	-	1%	-	-	-
[E.1] User errors	1	10%	10%	10 %	-	-	-
[E.2] System / Security administrator errors	1	20%	20%	20 %	-	-	-
[E.8] Malware diffusion	1	10%	10%	10 %	-	-	-
[E.9] [Re-]routing errors	1	-	-	10 %	-	-	-
[E.10] Sequence errors	1	-	10%	-	-	-	-
[E.15] Accidental alteration of the information	1	-	10%	-	-	-	-
[E.18] Destruction of information	1	100 %	-	-	-	-	-
[E.19] Information leaks	1	-	-	10 %	-	-	-
[E.20] Software vulnerabilities	1	1%	20%	20 %	-	-	-
[E.21] Defects in software maintenance / updating	10	1%	10%	50 %	-	-	-
[E.23] Defects in hardware maintenance / updating	1	100 %	10%	50 %	-	-	-
[E.24] System failure due to exhaustion of resources	10	50%	-	-	-	-	-
[E.25] Equipment loss	1	100 %	-	100 %	-	-	-
[E.28] Staff shortage	1	20%	-	-	-	-	-
[A.5] Masquerading of identity	10	-	100 %	100 %	100 %	-	-
[A.6] Abuse of access privileges	10	10%	100 %	100 %	100 %	-	-
[A.7] Misuse	1	50%	10%	100 %	-	-	-
[A.8] Malware diffusion	1	100 %	100 %	100 %	-	-	-
[A.9] [Re-]routing of messages	1	-	-	10	-	-	-

				%			
[A.10] Sequence alteration	1	-	10%	-	-	-	-
[A.11] Unauthorised access	100	10%	100 %	100 %	100 %	-	-
[A.12] Traffic analysis	1	-	-	2%	-	-	-
[A.13] Repudiation (denial of actions)	5	-	-	-	-	100 %	-
[A.14] Eavesdropping	1	-	-	1%	-	-	-
[A.15] Deliberate alteration of information	10	-	100 %	-	-	-	-
[A.18] Destruction of information	1	100 %	-	-	-	-	-
[A.19] Disclosure of information	10	-	-	50 %	-	-	-
[A.22] Software manipulation	1	50%	100 %	100 %	-	-	-
[A.23] Hardware manipulation	1	50%	-	50 %	-	-	-
[A.24] Denial of service	10	100 %	-	-	-	-	-
[A.25] Theft	1	100 %	-	100 %	-	-	-
[A.26] Destructive attack	1	100 %	-	-	-	-	-
[A.27] Enemy over-run	1	100 %	-	-	-	-	-
[A.28] Staff shortage	0.5	20%	-	-	-	-	-
[A.29] Extortion	0.9	50%	100 %	100 %	-	-	-
[A.30] Social engineering	0.5	50%	100 %	100 %	-	-	-

[SRV_RIS] Server RIS PACS

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[N.1] Fire	1	100 %	-	-	-	-	-
[N.2] Water	1	100 %	-	-	-	-	-
[N.*] Other natural disasters	0.5	100 %	-	-	-	-	-
[I.1] Fire	1	100	-	-	-	-	-

		%					
[I.2] Water	1	100 %	-	-	-	-	-
[I.*] Other industrial disasters	1	100 %	-	-	-	-	-
[I.3] Environmental pollution	1	50%	-	-	-	-	-
[I.4] Electromagnetic pollution	1	10%	-	-	-	-	-
[I.5.1] Software failure	1	50%	-	-	-	-	-
[I.5.2] Hardware failure	1	50%	-	-	-	-	-
[I.6] Power interruption	1	100 %	-	-	-	-	-
[I.7] Unsuitable temperature or humidity conditions	1	100 %	-	-	-	-	-
[I.8] Communications services failure	1	50%	-	-	-	-	-
[I.9] Interruption of other services or essential supplies	1	50%	-	-	-	-	-
[I.10] Media degradation	1	100 %	-	-	-	-	-
[I.11] Electromagnetic emanations (TEMPEST)	1	-	-	1%	-	-	-
[E.1] User errors	1	10%	10%	10 %	-	-	-
[E.2] System / Security administrator errors	1	20%	20%	20 %	-	-	-
[E.3] Monitoring errors (log)	1	-	1%	-	-	-	-
[E.8] Malware diffusion	1	10%	10%	10 %	-	-	-
[E.9] [Re-]routing errors	1	-	-	10 %	-	-	-
[E.10] Sequence errors	1	-	10%	-	-	-	-
[E.15] Accidental alteration of the information	1	-	10%	-	-	-	-
[E.18] Destruction of information	1	100 %	-	-	-	-	-
[E.19] Information leaks	1	-	-	10 %	-	-	-
[E.20] Software vulnerabilities	1	1%	20%	20 %	-	-	-
[E.21] Defects in software maintenance / updating	10	1%	10%	50 %	-	-	-
[E.23] Defects in hardware maintenance / updating	1	100 %	10%	50 %	-	-	-
[E.24] System failure due to exhaustion of resources	10	50%	-	-	-	-	-
[E.25] Equipment loss	1	100 %	-	100 %	-	-	-
[E.28] Staff shortage	1	20%	-	-	-	-	-
[A.3] Manipulation of activity records (log)	100	-	50%	-	-	-	-
[A.5] Masquerading of identity	10	-	100	100	10	-	-

			%	%	0 %		
[A.6] Abuse of access privileges	10	10%	100 %	100 %	10 0 %	-	-
[A.7] Misuse	1	50%	10%	100 %	-	-	-
[A.8] Malware diffusion	1	100 %	100 %	100 %	-	-	-
[A.9] [Re-]routing of messages	1	-	-	10 %	-	-	-
[A.10] Sequence alteration	1	-	10%	-	-	-	-
[A.11] Unauthorised access	100	10%	100 %	100 %	10 0 %	-	-
[A.12] Traffic analysis	1	-	-	2%	-	-	-
[A.13] Repudiation (denial of actions)	5	-	-	-	-	10 0 %	-
[A.14] Eavesdropping	1	-	-	1%	-	-	-
[A.15] Deliberate alteration of information	10	-	100 %	-	-	-	-
[A.18] Destruction of information	1	100 %	-	-	-	-	-
[A.19] Disclosure of information	10	-	-	50 %	-	-	-
[A.22] Software manipulation	1	50%	100 %	100 %	-	-	-
[A.23] Hardware manipulation	1	50%	-	50 %	-	-	-
[A.24] Denial of service	10	100 %	-	-	-	-	-
[A.25] Theft	1	100 %	-	100 %	-	-	-
[A.26] Destructive attack	1	100 %	-	-	-	-	-
[A.27] Enemy over-run	1	100 %	-	-	-	-	-
[A.28] Staff shortage	0.5	20%	-	-	-	-	-
[A.29] Extortion	0.9	50%	100 %	100 %	-	-	-
[A.30] Social engineering	0.5	50%	100 %	100 %	-	-	-

[SRVF] Server Finance

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[N.1] Fire	1	100 %	-	-	-	-	-
[N.2] Water	1	100 %	-	-	-	-	-
[N.*] Other natural disasters	0.5	100 %	-	-	-	-	-
[I.1] Fire	1	100 %	-	-	-	-	-
[I.2] Water	1	100 %	-	-	-	-	-
[I.*] Other industrial disasters	1	100 %	-	-	-	-	-
[I.3] Environmental pollution	1	50%	-	-	-	-	-
[I.4] Electromagnetic pollution	1	10%	-	-	-	-	-
[I.5.1] Software failure	1	50%	-	-	-	-	-
[I.5.2] Hardware failure	1	50%	-	-	-	-	-
[I.6] Power interruption	1	100 %	-	-	-	-	-
[I.7] Unsuitable temperature or humidity conditions	1	100 %	-	-	-	-	-
[I.8] Communications services failure	1	50%	-	-	-	-	-
[I.9] Interruption of other services or essential supplies	1	50%	-	-	-	-	-
[I.10] Media degradation	1	100 %	-	-	-	-	-
[I.11] Electromagnetic emanations (TEMPEST)	1	-	-	1%	-	-	-
[E.1] User errors	1	10%	10%	10 %	-	-	-
[E.2] System / Security administrator errors	1	20%	20%	20 %	-	-	-
[E.3] Monitoring errors (log)	1	-	1%	-	-	-	-
[E.8] Malware diffusion	1	10%	10%	10 %	-	-	-
[E.9] [Re-]routing errors	1	-	-	10 %	-	-	-
[E.10] Sequence errors	1	-	10%	-	-	-	-
[E.15] Accidental alteration of the information	1	-	10%	-	-	-	-
[E.18] Destruction of information	1	100 %	-	-	-	-	-

[E.19] Information leaks	1	-	-	10 %	-	-	-
[E.20] Software vulnerabilities	1	1%	20%	20 %	-	-	-
[E.21] Defects in software maintenance / updating	10	1%	10%	50 %	-	-	-
[E.23] Defects in hardware maintenance / updating	1	100 %	10%	50 %	-	-	-
[E.24] System failure due to exhaustion of resources	10	50%	-	-	-	-	-
[E.25] Equipment loss	1	100 %	-	100 %	-	-	-
[E.28] Staff shortage	1	30%	-	-	-	-	-
[A.3] Manipulation of activity records (log)	100	-	50%	-	-	-	-
[A.5] Masquerading of identity	10	-	100 %	100 %	100 %	-	-
[A.6] Abuse of access privileges	10	10%	100 %	100 %	100 %	-	-
[A.7] Misuse	1	50%	10%	100 %	-	-	-
[A.8] Malware diffusion	1	100 %	100 %	100 %	-	-	-
[A.9] [Re-]routing of messages	1	-	-	10 %	-	-	-
[A.10] Sequence alteration	1	-	10%	-	-	-	-
[A.11] Unauthorised access	100	10%	100 %	100 %	100 %	-	-
[A.12] Traffic analysis	1	-	-	2%	-	-	-
[A.13] Repudiation (denial of actions)	5	-	-	-	-	100 %	-
[A.14] Eavesdropping	1	-	-	1%	-	-	-
[A.15] Deliberate alteration of information	10	-	100 %	-	-	-	-
[A.18] Destruction of information	1	100 %	-	-	-	-	-
[A.19] Disclosure of information	10	-	-	50 %	-	-	-
[A.22] Software manipulation	1	50%	100 %	100 %	-	-	-
[A.23] Hardware manipulation	1	50%	-	50 %	-	-	-
[A.24] Denial of service	10	100 %	-	-	-	-	-
[A.25] Theft	1	100	-	100	-	-	-

		%		%			
[A.26] Destructive attack	1	100 %	-	-	-	-	-
[A.27] Enemy over-run	1	100 %	-	-	-	-	-
[A.28] Staff shortage	0.5	50%	-	-	-	-	-
[A.29] Extortion	0.9	50%	100 %	100 %	-	-	-
[A.30] Social engineering	0.5	50%	100 %	100 %	-	-	-

[SRV_Blood] Server Aimodosia

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[N.1] Fire	1	100 %	-	-	-	-	-
[N.2] Water	1	100 %	-	-	-	-	-
[N.*] Other natural disasters	0.5	100 %	-	-	-	-	-
[I.1] Fire	1	100 %	-	-	-	-	-
[I.2] Water	1	100 %	-	-	-	-	-
[I.*] Other industrial disasters	1	100 %	-	-	-	-	-
[I.3] Environmental pollution	1	50%	-	-	-	-	-
[I.4] Electromagnetic pollution	1	10%	-	-	-	-	-
[I.5.1] Software failure	1	50%	-	-	-	-	-
[I.5.2] Hardware failure	1	50%	-	-	-	-	-
[I.6] Power interruption	1	100 %	-	-	-	-	-
[I.7] Unsuitable temperature or humidity conditions	1	100 %	-	-	-	-	-
[I.8] Communications services failure	1	50%	-	-	-	-	-
[I.9] Interruption of other services or essential supplies	1	50%	-	-	-	-	-
[I.10] Media degradation	1	100 %	-	-	-	-	-
[I.11] Electromagnetic emanations (TEMPEST)	1	-	-	1%	-	-	-
[E.1] User errors	1	10%	10%	10 %	-	-	-
[E.2] System / Security administrator errors	1	20%	20%	20 %	-	-	-

[E.3] Monitoring errors (log)	1	-	1%	-	-	-	-
[E.8] Malware diffusion	1	10%	10%	10 %	-	-	-
[E.9] [Re-]routing errors	1	-	-	10 %	-	-	-
[E.10] Sequence errors	1	-	10%	-	-	-	-
[E.15] Accidental alteration of the information	1	-	50%	-	-	-	-
[E.18] Destruction of information	1	100 %	-	-	-	-	-
[E.19] Information leaks	1	-	-	10 %	-	-	-
[E.20] Software vulnerabilities	1	1%	20%	20 %	-	-	-
[E.21] Defects in software maintenance / updating	10	1%	10%	50 %	-	-	-
[E.23] Defects in hardware maintenance / updating	1	100 %	10%	50 %	-	-	-
[E.24] System failure due to exhaustion of resources	10	50%	-	-	-	-	-
[E.25] Equipment loss	1	100 %	-	100 %	-	-	-
[E.28] Staff shortage	1	30%	-	-	-	-	-
[A.3] Manipulation of activity records (log)	100	-	50%	-	-	-	-
[A.5] Masquerading of identity	10	-	100 %	100 %	100 %	-	-
[A.6] Abuse of access privileges	10	10%	100 %	100 %	100 %	-	-
[A.7] Misuse	1	50%	50%	100 %	-	-	-
[A.8] Malware diffusion	1	100 %	100 %	100 %	-	-	-
[A.9] [Re-]routing of messages	1	-	-	10 %	-	-	-
[A.10] Sequence alteration	1	-	10%	-	-	-	-
[A.11] Unauthorised access	100	10%	100 %	100 %	100 %	-	-
[A.12] Traffic analysis	1	-	-	2%	-	-	-
[A.13] Repudiation (denial of actions)	5	-	-	-	-	100 %	-
[A.14] Eavesdropping	1	-	-	1%	-	-	-
[A.15] Deliberate alteration of information	10	-	100 %	-	-	-	-
[A.18] Destruction of information	1	100 %	-	-	-	-	-

[A.19] Disclosure of information	10	-	-	50 %	-	-	-
[A.22] Software manipulation	1	50%	100 %	100 %	-	-	-
[A.23] Hardware manipulation	1	50%	-	50 %	-	-	-
[A.24] Denial of service	10	100 %	-	-	-	-	-
[A.25] Theft	1	100 %	-	100 %	-	-	-
[A.26] Destructive attack	1	100 %	-	-	-	-	-
[A.27] Enemy over-run	1	100 %	-	-	-	-	-
[A.28] Staff shortage	0.5	50%	-	-	-	-	-
[A.29] Extortion	0.9	50%	100 %	100 %	-	-	-
[A.30] Social engineering	0.5	50%	100 %	100 %	-	-	-

[SRVB] Server Back Up

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[N.1] Fire	1	100 %	-	-	-	-	-
[N.2] Water	1	100 %	-	-	-	-	-
[N.*] Other natural disasters	0.5	100 %	-	-	-	-	-
[I.1] Fire	1	100 %	-	-	-	-	-
[I.2] Water	1	100 %	-	-	-	-	-
[I.*] Other industrial disasters	1	100 %	-	-	-	-	-
[I.3] Environmental pollution	1	50%	-	-	-	-	-
[I.4] Electromagnetic pollution	1	10%	-	-	-	-	-
[I.5.1] Software failure	1	50%	-	-	-	-	-
[I.5.2] Hardware failure	1	50%	-	-	-	-	-
[I.6] Power interruption	1	100 %	-	-	-	-	-
[I.7] Unsuitable temperature or humidity	1	100	-	-	-	-	-

conditions		%					
[I.8] Communications services failure	1	50%	-	-	-	-	-
[I.10] Media degradation	1	100 %	-	-	-	-	-
[I.11] Electromagnetic emanations (TEMPEST)	1	-	-	1%	-	-	-
[E.1] User errors	1	10%	10%	10%	-	-	-
[E.2] System / Security administrator errors	1	20%	20%	20%	-	-	-
[E.3] Monitoring errors (log)	1	-	1%	-	-	-	-
[E.8] Malware diffusion	1	10%	10%	10%	-	-	-
[E.9] [Re-]routing errors	1	-	-	10%	-	-	-
[E.10] Sequence errors	1	-	10%	-	-	-	-
[E.15] Accidental alteration of the information	1	-	50%	-	-	-	-
[E.18] Destruction of information	1	100 %	-	-	-	-	-
[E.19] Information leaks	1	-	-	10%	-	-	-
[E.20] Software vulnerabilities	1	1%	20%	20%	-	-	-
[E.21] Defects in software maintenance / updating	10	1%	10%	50%	-	-	-
[E.23] Defects in hardware maintenance / updating	1	100 %	10%	50%	-	-	-
[E.24] System failure due to exhaustion of resources	10	50%	-	-	-	-	-
[E.25] Equipment loss	1	100 %	-	50%	-	-	-
[E.28] Staff shortage	1	20%	-	-	-	-	-
[A.3] Manipulation of activity records (log)	100	-	50%	-	-	-	-
[A.5] Masquerading of identity	10	-	50%	50%	100 %	-	-
[A.6] Abuse of access privileges	10	10%	10%	50%	100 %	-	-
[A.7] Misuse	1	10%	50%	100 %	-	-	-
[A.8] Malware diffusion	1	100 %	100 %	100 %	-	-	-
[A.9] [Re-]routing of messages	1	-	-	10%	-	-	-
[A.10] Sequence alteration	1	-	10%	-	-	-	-
[A.11] Unauthorised access	100	10%	10%	50%	100 %	-	-
[A.12] Traffic analysis	1	-	-	2%	-	-	-
[A.13] Repudiation (denial of actions)	5	-	-	-	-	100 %	-
[A.14] Eavesdropping	1	-	-	1%	-	-	-
[A.15] Deliberate alteration of information	10	-	100 %	-	-	-	-
[A.18] Destruction of information	1	100 %	-	-	-	-	-

[A.19] Disclosure of information	10	-	-	50%	-	-	-
[A.22] Software manipulation	1	50%	100 %	100 %	-	-	-
[A.23] Hardware manipulation	0.5	50%	-	50%	-	-	-
[A.24] Denial of service	10	100 %	-	-	-	-	-
[A.25] Theft	1	100 %	-	100 %	-	-	-
[A.26] Destructive attack	1	100 %	-	-	-	-	-
[A.27] Enemy over-run	1	100 %	-	-	-	-	-
[A.28] Staff shortage	0.5	20%	-	-	-	-	-
[A.29] Extortion	0.9	50%	100 %	100 %	-	-	-
[A.30] Social engineering	0.5	50%	100 %	100 %	-	-	-

[Lan_Pr] Lan Printer

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[N.1] Fire	1	100 %	-	-	-	-	-
[N.2] Water	1	100 %	-	-	-	-	-
[N.*] Other natural disasters	0.5	100 %	-	-	-	-	-
[I.1] Fire	1	100 %	-	-	-	-	-
[I.2] Water	1	100 %	-	-	-	-	-
[I.*] Other industrial disasters	1	100 %	-	-	-	-	-
[I.3] Environmental pollution	1	50%	-	-	-	-	-
[I.4] Electromagnetic pollution	1	10%	-	-	-	-	-
[I.5.2] Hardware failure	1	50%	-	-	-	-	-
[I.6] Power interruption	1	100 %	-	-	-	-	-
[I.7] Unsuitable temperature or humidity conditions	1	100 %	-	-	-	-	-
[I.8] Communications services failure	1	50%	-	-	-	-	-
[I.10] Media degradation	1	100 %	-	-	-	-	-
[I.11] Electromagnetic emanations (TEMPEST)	1	-	-	1%	-	-	-

[E.1] User errors	1	1%	5%	10%	-	-	-
[E.2] System / Security administrator errors	1	20%	20%	20%	-	-	-
[E.9] [Re-]routing errors	1	-	-	10%	-	-	-
[E.10] Sequence errors	1	-	10%	-	-	-	-
[E.15] Accidental alteration of the information	1	-	10%	-	-	-	-
[E.18] Destruction of information	1	100 %	-	-	-	-	-
[E.19] Information leaks	1	-	-	10%	-	-	-
[E.23] Defects in hardware maintenance / updating	1	10%	-	-	-	-	-
[E.24] System failure due to exhaustion of resources	10	50%	-	-	-	-	-
[E.25] Equipment loss	1	100 %	-	50%	-	-	-
[E.28] Staff shortage	1	30%	-	-	-	-	-
[A.5] Masquerading of identity	1	-	10%	50%	100 %	-	-
[A.6] Abuse of access privileges	1	10%	-	-	-	-	-
[A.7] Misuse	1	50%	10%	10%	-	-	-
[A.9] [Re-]routing of messages	1	-	-	10%	-	-	-
[A.10] Sequence alteration	1	-	10%	-	-	-	-
[A.11] Unauthorised access	1	10%	10%	50%	100 %	-	-
[A.12] Traffic analysis	1	-	-	2%	-	-	-
[A.14] Eavesdropping	1	-	-	1%	-	-	-
[A.15] Deliberate alteration of information	5	-	100 %	-	-	-	-
[A.18] Destruction of information	1	100 %	-	-	-	-	-
[A.19] Disclosure of information	10	-	-	50%	-	-	-
[A.23] Hardware manipulation	1	50%	-	50%	-	-	-
[A.24] Denial of service	10	100 %	-	-	-	-	-
[A.25] Theft	1	100 %	-	100 %	-	-	-
[A.26] Destructive attack	1	100 %	-	-	-	-	-
[A.27] Enemy over-run	1	100 %	-	-	-	-	-
[A.28] Staff shortage	0.5	50%	-	-	-	-	-
[A.29] Extortion	0.9	20%	20%	50%	-	-	-
[A.30] Social engineering	0.5	20%	20%	20%	-	-	-

[PC_RIS_PACS] Personal Computer_RIS

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[N.1] Fire	0.1	100 %	-	-	-	-	-
[N.2] Water	0.1	50%	-	-	-	-	-
[N.*] Other natural disasters	0.1	100 %	-	-	-	-	-
[I.1] Fire	0.5	100 %	-	-	-	-	-
[I.2] Water	0.5	50%	-	-	-	-	-
[I.*] Other industrial disasters	0.5	100 %	-	-	-	-	-
[I.3] Environmental pollution	1	50%	-	-	-	-	-
[I.4] Electromagnetic pollution	1	10%	-	-	-	-	-
[I.5.1] Software failure	1	50%	-	-	-	-	-
[I.5.2] Hardware failure	1	50%	-	-	-	-	-
[I.6] Power interruption	1	100 %	-	-	-	-	-
[I.7] Unsuitable temperature or humidity conditions	1	100 %	-	-	-	-	-
[I.8] Communications services failure	1	50%	-	-	-	-	-
[I.10] Media degradation	1	100 %	-	-	-	-	-
[I.11] Electromagnetic emanations (TEMPEST)	1	-	-	1%	-	-	-
[E.1] User errors	1	10%	10%	10%	-	-	-
[E.2] System / Security administrator errors	1	20%	20%	20%	-	-	-
[E.8] Malware diffusion	1	10%	10%	10%	-	-	-
[E.9] [Re-]routing errors	1	-	-	10%	-	-	-
[E.10] Sequence errors	1	-	10%	-	-	-	-
[E.15] Accidental alteration of the information	1	-	10%	-	-	-	-
[E.18] Destruction of information	1	100 %	-	-	-	-	-
[E.19] Information leaks	1	-	-	10%	-	-	-
[E.20] Software vulnerabilities	1	1%	20%	20%	-	-	-
[E.21] Defects in software maintenance / updating	10	1%	10%	50%	-	-	-
[E.23] Defects in hardware maintenance / updating	1	100 %	10%	50%	-	-	-
[E.24] System failure due to exhaustion of	10	50%	-	-	-	-	-

resources							
[E.25] Equipment loss	5	10%	-	50%	-	-	-
[E.28] Staff shortage	1	30%	-	-	-	-	-
[A.5] Masquerading of identity	10	-	50%	50%	100 %	-	-
[A.6] Abuse of access privileges	10	1%	10%	50%	100 %	-	-
[A.7] Misuse	1	10%	10%	50%	-	-	-
[A.8] Malware diffusion	1	100 %	100 %	100 %	-	-	-
[A.9] [Re-]routing of messages	1	-	-	10%	-	-	-
[A.10] Sequence alteration	1	-	10%	-	-	-	-
[A.11] Unauthorised access	100	10%	10%	50%	100 %	-	-
[A.12] Traffic analysis	1	-	-	2%	-	-	-
[A.13] Repudiation (denial of actions)	5	-	-	-	-	100 %	-
[A.14] Eavesdropping	1	-	-	1%	-	-	-
[A.15] Deliberate alteration of information	10	-	100 %	-	-	-	-
[A.18] Destruction of information	1	100 %	-	-	-	-	-
[A.19] Disclosure of information	10	-	-	50%	-	-	-
[A.22] Software manipulation	1	50%	100 %	100 %	-	-	-
[A.23] Hardware manipulation	0.5	50%	-	50%	-	-	-
[A.24] Denial of service	10	100 %	-	-	-	-	-
[A.25] Theft	5	10%	-	100 %	-	-	-
[A.26] Destructive attack	1	100 %	-	-	-	-	-
[A.28] Staff shortage	0.5	50%	-	-	-	-	-
[A.29] Extortion	0.9	20%	20%	50%	-	-	-
[A.30] Social engineering	0.5	20%	20%	20%	-	-	-

[PC_LIS] Personal Computer_LIS

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[N.1] Fire	0.1	100 %	-	-	-	-	-
[N.2] Water	0.1	50%	-	-	-	-	-
[N.*] Other natural disasters	0.1	100	-	-	-	-	-

		%					
[I.1] Fire	0.5	100 %	-	-	-	-	-
[I.2] Water	0.5	50%	-	-	-	-	-
[I.*] Other industrial disasters	0.5	100 %	-	-	-	-	-
[I.3] Environmental pollution	1	50%	-	-	-	-	-
[I.4] Electromagnetic pollution	1	10%	-	-	-	-	-
[I.5.1] Software failure	1	50%	-	-	-	-	-
[I.5.2] Hardware failure	1	50%	-	-	-	-	-
[I.6] Power interruption	1	100 %	-	-	-	-	-
[I.7] Unsuitable temperature or humidity conditions	1	100 %	-	-	-	-	-
[I.8] Communications services failure	1	50%	-	-	-	-	-
[I.10] Media degradation	1	100 %	-	-	-	-	-
[I.11] Electromagnetic emanations (TEMPEST)	1	-	-	1%	-	-	-
[E.1] User errors	1	10%	10%	10%	-	-	-
[E.2] System / Security administrator errors	1	20%	20%	20%	-	-	-
[E.8] Malware diffusion	1	10%	10%	10%	-	-	-
[E.9] [Re-]routing errors	1	-	-	10%	-	-	-
[E.10] Sequence errors	1	-	10%	-	-	-	-
[E.15] Accidental alteration of the information	1	-	10%	-	-	-	-
[E.18] Destruction of information	1	100 %	-	-	-	-	-
[E.19] Information leaks	1	-	-	10%	-	-	-
[E.20] Software vulnerabilities	1	1%	20%	20%	-	-	-
[E.21] Defects in software maintenance / updating	10	1%	10%	50%	-	-	-
[E.23] Defects in hardware maintenance / updating	1	100 %	10%	50%	-	-	-
[E.24] System failure due to exhaustion of resources	10	50%	-	-	-	-	-
[E.25] Equipment loss	5	10%	-	50%	-	-	-
[E.28] Staff shortage	1	30%	-	-	-	-	-
[A.5] Masquerading of identity	10	-	50%	50%	100 %	-	-
[A.6] Abuse of access privileges	10	1%	10%	50%	100 %	-	-
[A.7] Misuse	1	10%	10%	50%	-	-	-
[A.8] Malware diffusion	1	100 %	100 %	100 %	-	-	-
[A.9] [Re-]routing of messages	1	-	-	10%	-	-	-
[A.10] Sequence alteration	1	-	10%	-	-	-	-
[A.11] Unauthorised access	100	10%	10%	50%	100 %	-	-

[A.12] Traffic analysis	1	-	-	2%	-	-	-
[A.13] Repudiation (denial of actions)	5	-	-	-	-	100 %	-
[A.14] Eavesdropping	1	-	-	1%	-	-	-
[A.15] Deliberate alteration of information	10	-	100 %	-	-	-	-
[A.18] Destruction of information	1	100 %	-	-	-	-	-
[A.19] Disclosure of information	10	-	-	50%	-	-	-
[A.22] Software manipulation	1	50%	100 %	100 %	-	-	-
[A.23] Hardware manipulation	0.5	50%	-	50%	-	-	-
[A.24] Denial of service	10	100 %	-	-	-	-	-
[A.25] Theft	5	10%	-	100 %	-	-	-
[A.26] Destructive attack	1	100 %	-	-	-	-	-
[A.28] Staff shortage	0.5	50%	-	-	-	-	-
[A.29] Extortion	0.9	20%	20%	50%	-	-	-
[A.30] Social engineering	0.5	20%	20%	20%	-	-	-

[PC_S] Personal Computer_Salary

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[N.1] Fire	0.1	100 %	-	-	-	-	-
[N.2] Water	0.1	50%	-	-	-	-	-
[N.*] Other natural disasters	0.1	100 %	-	-	-	-	-
[I.1] Fire	0.5	100 %	-	-	-	-	-
[I.2] Water	0.5	50%	-	-	-	-	-
[I.*] Other industrial disasters	0.5	100 %	-	-	-	-	-
[I.3] Environmental pollution	1	50%	-	-	-	-	-
[I.4] Electromagnetic pollution	1	10%	-	-	-	-	-
[I.5.1] Software failure	1	50%	-	-	-	-	-
[I.5.2] Hardware failure	1	50%	-	-	-	-	-
[I.6] Power interruption	1	100 %	-	-	-	-	-
[I.7] Unsuitable temperature or humidity conditions	1	100 %	-	-	-	-	-

[I.8] Communications services failure	1	50%	-	-	-	-	-
[I.10] Media degradation	1	100 %	-	-	-	-	-
[I.11] Electromagnetic emanations (TEMPEST)	1	-	-	1%	-	-	-
[E.1] User errors	1	10%	10%	10%	-	-	-
[E.2] System / Security administrator errors	1	20%	20%	20%	-	-	-
[E.8] Malware diffusion	1	10%	10%	10%	-	-	-
[E.9] [Re-]routing errors	1	-	-	10%	-	-	-
[E.10] Sequence errors	1	-	10%	-	-	-	-
[E.15] Accidental alteration of the information	1	-	10%	-	-	-	-
[E.18] Destruction of information	1	100 %	-	-	-	-	-
[E.19] Information leaks	1	-	-	10%	-	-	-
[E.20] Software vulnerabilities	1	1%	20%	20%	-	-	-
[E.21] Defects in software maintenance / updating	10	1%	10%	50%	-	-	-
[E.23] Defects in hardware maintenance / updating	1	100 %	10%	50%	-	-	-
[E.24] System failure due to exhaustion of resources	10	50%	-	-	-	-	-
[E.25] Equipment loss	1	10%	-	50%	-	-	-
[E.28] Staff shortage	1	30%	-	-	-	-	-
[A.5] Masquerading of identity	10	-	50%	50%	100 %	-	-
[A.6] Abuse of access privileges	10	1%	10%	50%	100 %	-	-
[A.7] Misuse	1	10%	10%	50%	-	-	-
[A.8] Malware diffusion	1	100 %	100 %	100 %	-	-	-
[A.9] [Re-]routing of messages	1	-	-	10%	-	-	-
[A.10] Sequence alteration	1	-	10%	-	-	-	-
[A.11] Unauthorised access	100	-	10%	50%	100 %	-	-
[A.12] Traffic analysis	1	-	-	2%	-	-	-
[A.13] Repudiation (denial of actions)	5	-	-	-	-	100 %	-
[A.14] Eavesdropping	1	-	-	1%	-	-	-
[A.15] Deliberate alteration of information	10	-	100 %	-	-	-	-
[A.18] Destruction of information	1	100 %	-	-	-	-	-
[A.19] Disclosure of information	10	-	-	50%	-	-	-
[A.22] Software manipulation	1	50%	100 %	100 %	-	-	-
[A.23] Hardware manipulation	0.1	50%	-	50%	-	-	-
[A.24] Denial of service	10	50%	-	-	-	-	-

[A.25] Theft	1	10%	-	100 %	-	-	-
[A.26] Destructive attack	1	10%	-	-	-	-	-
[A.28] Staff shortage	0.5	50%	-	-	-	-	-
[A.29] Extortion	0.9	20%	20%	50%	-	-	-
[A.30] Social engineering	0.5	20%	20%	20%	-	-	-

[PC_Supply] Personal Computer Supply

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[N.1] Fire	0.1	100 %	-	-	-	-	-
[N.2] Water	0.1	50%	-	-	-	-	-
[N.*] Other natural disasters	0.1	100 %	-	-	-	-	-
[I.1] Fire	0.5	100 %	-	-	-	-	-
[I.2] Water	0.5	50%	-	-	-	-	-
[I.*] Other industrial disasters	0.5	100 %	-	-	-	-	-
[I.3] Environmental pollution	1	50%	-	-	-	-	-
[I.4] Electromagnetic pollution	1	10%	-	-	-	-	-
[I.5.1] Software failure	1	50%	-	-	-	-	-
[I.5.2] Hardware failure	1	50%	-	-	-	-	-
[I.6] Power interruption	1	100 %	-	-	-	-	-
[I.7] Unsuitable temperature or humidity conditions	1	100 %	-	-	-	-	-
[I.8] Communications services failure	1	50%	-	-	-	-	-
[I.10] Media degradation	1	100 %	-	-	-	-	-
[I.11] Electromagnetic emanations (TEMPEST)	1	-	-	1%	-	-	-
[E.1] User errors	1	10%	10%	10%	-	-	-
[E.2] System / Security administrator errors	1	20%	20%	20%	-	-	-
[E.8] Malware diffusion	1	10%	10%	10%	-	-	-
[E.9] [Re-]routing errors	1	-	-	10%	-	-	-
[E.10] Sequence errors	1	-	10%	-	-	-	-
[E.15] Accidental alteration of the information	1	-	10%	-	-	-	-
[E.18] Destruction of information	1	100 %	-	-	-	-	-
[E.19] Information leaks	1	-	-	10%	-	-	-
[E.20] Software vulnerabilities	1	1%	20%	20%	-	-	-
[E.21] Defects in software maintenance / updating	10	1%	10%	50%	-	-	-

[E.23] Defects in hardware maintenance / updating	1	100 %	10%	50%	-	-	-
[E.24] System failure due to exhaustion of resources	10	50%	-	-	-	-	-
[E.25] Equipment loss	5	10%	-	50%	-	-	-
[E.28] Staff shortage	1	30%	-	-	-	-	-
[A.5] Masquerading of identity	10	-	50%	50%	100 %	-	-
[A.6] Abuse of access privileges	10	1%	10%	50%	100 %	-	-
[A.7] Misuse	1	10%	10%	50%	-	-	-
[A.8] Malware diffusion	1	100 %	100 %	100 %	-	-	-
[A.9] [Re-]routing of messages	1	-	-	10%	-	-	-
[A.10] Sequence alteration	1	-	10%	-	-	-	-
[A.11] Unauthorised access	100	10%	10%	50%	100 %	-	-
[A.12] Traffic analysis	1	-	-	2%	-	-	-
[A.13] Repudiation (denial of actions)	5	-	-	-	-	100 %	-
[A.14] Eavesdropping	1	-	-	1%	-	-	-
[A.15] Deliberate alteration of information	10	-	100 %	-	-	-	-
[A.18] Destruction of information	1	100 %	-	-	-	-	-
[A.19] Disclosure of information	10	-	-	50%	-	-	-
[A.22] Software manipulation	1	50%	100 %	100 %	-	-	-
[A.23] Hardware manipulation	0.5	50%	-	50%	-	-	-
[A.24] Denial of service	10	100 %	-	-	-	-	-
[A.25] Theft	5	10%	-	100 %	-	-	-
[A.26] Destructive attack	1	100 %	-	-	-	-	-
[A.28] Staff shortage	0.5	50%	-	-	-	-	-
[A.29] Extortion	0.9	20%	20%	50%	-	-	-
[A.30] Social engineering	0.5	20%	20%	20%	-	-	-

[PC_Blood] Personal Computer Blood

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[N.1] Fire	1	100%	-	-	-	-	-
[N.2] Water	1	100%	-	-	-	-	-
[N.*] Other natural disasters	0.5	100%	-	-	-	-	-
[I.1] Fire	1	100%	-	-	-	-	-
[I.2] Water	1	100%	-	-	-	-	-
[I.*] Other industrial disasters	1	100%	-	-	-	-	-
[I.3] Environmental pollution	1	50%	-	-	-	-	-
[I.4] Electromagnetic pollution	1	10%	-	-	-	-	-
[I.5.1] Software failure	1	50%	-	-	-	-	-
[I.5.2] Hardware failure	1	50%	-	-	-	-	-
[I.6] Power interruption	1	100%	-	-	-	-	-
[I.7] Unsuitable temperature or humidity conditions	1	100%	-	-	-	-	-
[I.8] Communications services failure	1	50%	-	-	-	-	-
[I.10] Media degradation	1	100%	-	-	-	-	-
[I.11] Electromagnetic emanations (TEMPEST)	1	-	-	1%	-	-	-
[E.1] User errors	1	10%	10%	10%	-	-	-
[E.2] System / Security administrator errors	1	20%	20%	20%	-	-	-
[E.8] Malware diffusion	1	10%	10%	10%	-	-	-
[E.9] [Re-]routing errors	1	-	-	10%	-	-	-
[E.10] Sequence errors	1	-	10%	-	-	-	-
[E.15] Accidental alteration of the information	1	-	10%	-	-	-	-
[E.18] Destruction of information	1	100%	-	-	-	-	-
[E.19] Information leaks	1	-	-	10%	-	-	-
[E.20] Software vulnerabilities	1	1%	20%	20%	-	-	-
[E.21] Defects in software maintenance / updating	10	1%	10%	50%	-	-	-
[E.23] Defects in hardware maintenance / updating	1	100%	10%	50%	-	-	-
[E.24] System failure due to exhaustion of resources	10	50%	-	-	-	-	-
[E.25] Equipment loss	5	10%	-	50%	-	-	-
[E.28] Staff shortage	1	30%	-	-	-	-	-
[A.5] Masquerading of identity	10	-	50%	50%	100	-	-

					%		
[A.6] Abuse of access privileges	10	10%	10%	50%	100 %	-	-
[A.7] Misuse	1	10%	10%	50%	-	-	-
[A.8] Malware diffusion	1	100 %	100 %	100 %	-	-	-
[A.9] [Re-]routing of messages	1	-	-	10%	-	-	-
[A.10] Sequence alteration	1	-	10%	-	-	-	-
[A.11] Unauthorised access	100	10%	10%	50%	100 %	-	-
[A.12] Traffic analysis	1	-	-	2%	-	-	-
[A.13] Repudiation (denial of actions)	5	-	-	-	-	100 %	-
[A.14] Eavesdropping	1	-	-	1%	-	-	-
[A.15] Deliberate alteration of information	10	-	100 %	-	-	-	-
[A.18] Destruction of information	1	100 %	-	-	-	-	-
[A.19] Disclosure of information	10	-	-	50%	-	-	-
[A.22] Software manipulation	1	50%	100 %	100 %	-	-	-
[A.23] Hardware manipulation	0.5	50%	-	50%	-	-	-
[A.24] Denial of service	10	100 %	-	-	-	-	-
[A.25] Theft	5	10%	-	100 %	-	-	-
[A.26] Destructive attack	1	100 %	-	-	-	-	-
[A.27] Enemy over-run	1	100 %	-	-	-	-	-
[A.28] Staff shortage	0.5	50%	-	-	-	-	-
[A.29] Extortion	0.9	20%	20%	50%	-	-	-
[A.30] Social engineering	0.5	20%	20%	20%	-	-	-

[PC_Grammateia] Personal Computer

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[N.1] Fire	1	100 %	-	-	-	-	-
[N.2] Water	1	100 %	-	-	-	-	-
[N.*] Other natural disasters	0.5	100 %	-	-	-	-	-

[I.1] Fire	1	100 %	-	-	-	-	-
[I.2] Water	1	100 %	-	-	-	-	-
[I.*] Other industrial disasters	1	100 %	-	-	-	-	-
[I.3] Environmental pollution	1	50%	-	-	-	-	-
[I.4] Electromagnetic pollution	1	10%	-	-	-	-	-
[I.5.1] Software failure	1	50%	-	-	-	-	-
[I.5.2] Hardware failure	1	50%	-	-	-	-	-
[I.6] Power interruption	1	100 %	-	-	-	-	-
[I.7] Unsuitable temperature or humidity conditions	1	100 %	-	-	-	-	-
[I.8] Communications services failure	1	50%	-	-	-	-	-
[I.10] Media degradation	1	100 %	-	-	-	-	-
[I.11] Electromagnetic emanations (TEMPEST)	1	-	-	1%	-	-	-
[E.1] User errors	1	10%	10%	10%	-	-	-
[E.2] System / Security administrator errors	1	20%	20%	20%	-	-	-
[E.8] Malware diffusion	1	10%	10%	10%	-	-	-
[E.9] [Re-]routing errors	1	-	-	10%	-	-	-
[E.10] Sequence errors	1	-	10%	-	-	-	-
[E.15] Accidental alteration of the information	1	-	10%	-	-	-	-
[E.18] Destruction of information	1	100 %	-	-	-	-	-
[E.19] Information leaks	1	-	-	10%	-	-	-
[E.20] Software vulnerabilities	1	1%	20%	20%	-	-	-
[E.21] Defects in software maintenance / updating	10	1%	10%	50%	-	-	-
[E.23] Defects in hardware maintenance / updating	1	100 %	10%	50%	-	-	-
[E.24] System failure due to exhaustion of resources	10	50%	-	-	-	-	-
[E.25] Equipment loss	5	10%	-	50%	-	-	-
[E.28] Staff shortage	1	30%	-	-	-	-	-
[A.5] Masquerading of identity	10	-	50%	50%	100 %	-	-
[A.6] Abuse of access privileges	10	10%	10%	50%	100 %	-	-
[A.7] Misuse	1	10%	10%	50%	-	-	-
[A.8] Malware diffusion	1	100 %	100 %	100 %	-	-	-
[A.9] [Re-]routing of messages	1	-	-	10%	-	-	-
[A.10] Sequence alteration	1	-	10%	-	-	-	-
[A.11] Unauthorised access	100	10%	10%	50%	100 %	-	-

[A.12] Traffic analysis	1	-	-	2%	-	-	-
[A.13] Repudiation (denial of actions)	5	-	-	-	-	100 %	-
[A.14] Eavesdropping	1	-	-	1%	-	-	-
[A.15] Deliberate alteration of information	10	-	100 %	-	-	-	-
[A.18] Destruction of information	1	100 %	-	-	-	-	-
[A.19] Disclosure of information	10	-	-	50%	-	-	-
[A.22] Software manipulation	1	50%	100 %	100 %	-	-	-
[A.23] Hardware manipulation	0.5	50%	-	50%	-	-	-
[A.24] Denial of service	10	100 %	-	-	-	-	-
[A.25] Theft	5	10%	-	100 %	-	-	-
[A.26] Destructive attack	1	100 %	-	-	-	-	-
[A.27] Enemy over-run	1	100 %	-	-	-	-	-
[A.28] Staff shortage	0.5	50%	-	-	-	-	-
[A.29] Extortion	0.9	20%	20%	50%	-	-	-
[A.30] Social engineering	0.5	20%	20%	20%	-	-	-

[Router] Router

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[N.1] Fire	0.1	100 %	-	-	-	-	-
[N.2] Water	0.1	50%	-	-	-	-	-
[N.*] Other natural disasters	0.1	100 %	-	-	-	-	-
[I.1] Fire	0.5	100 %	-	-	-	-	-
[I.2] Water	0.5	50%	-	-	-	-	-
[I.*] Other industrial disasters	0.5	100 %	-	-	-	-	-
[I.3] Environmental pollution	0.1	50%	-	-	-	-	-
[I.4] Electromagnetic pollution	1	10%	-	-	-	-	-
[I.5.2] Hardware failure	1	50%	-	-	-	-	-
[I.6] Power interruption	1	100 %	-	-	-	-	-
[I.7] Unsuitable temperature or humidity	1	100	-	-	-	-	-

conditions		%					
[I.8] Communications services failure	1	50%	-	-	-	-	-
[I.11] Electromagnetic emanations (TEMPEST)	1	-	-	1%	-	-	-
[E.2] System / Security administrator errors	1	20%	20%	20%	-	-	-
[E.9] [Re-]routing errors	1	-	-	10%	-	-	-
[E.10] Sequence errors	1	-	10%	-	-	-	-
[E.15] Accidental alteration of the information	1	-	10%	-	-	-	-
[E.18] Destruction of information	1	1%	-	-	-	-	-
[E.19] Information leaks	1	-	-	10%	-	-	-
[E.23] Defects in hardware maintenance / updating	1	10%	-	-	-	-	-
[E.24] System failure due to exhaustion of resources	10	50%	-	-	-	-	-
[E.25] Equipment loss	1	20%	-	50%	-	-	-
[E.28] Staff shortage	1	10%	-	-	-	-	-
[A.5] Masquerading of identity	1	-	10%	50%	100 %	-	-
[A.7] Misuse	1	10%	10%	10%	-	-	-
[A.9] [Re-]routing of messages	1	-	-	10%	-	-	-
[A.10] Sequence alteration	1	-	10%	-	-	-	-
[A.11] Unauthorised access	1	10%	10%	50%	100 %	-	-
[A.12] Traffic analysis	1	-	-	2%	-	-	-
[A.14] Eavesdropping	1	-	-	1%	-	-	-
[A.15] Deliberate alteration of information	1	-	50%	-	-	-	-
[A.18] Destruction of information	1	50%	-	-	-	-	-
[A.19] Disclosure of information	10	-	-	50%	-	-	-
[A.23] Hardware manipulation	0.5	100 %	-	50%	-	-	-
[A.24] Denial of service	10	100 %	-	-	-	-	-
[A.25] Theft	0.5	20%	-	50%	-	-	-
[A.26] Destructive attack	1	100 %	-	-	-	-	-
[A.28] Staff shortage	0.5	20%	-	-	-	-	-
[A.29] Extortion	0.9	50%	100 %	100 %	-	-	-
[A.30] Social engineering	0.5	50%	100 %	100 %	-	-	-

[SWs] Switch

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[N.1] Fire	0.1	100 %	-	-	-	-	-
[N.2] Water	0.1	50%	-	-	-	-	-

[N.*] Other natural disasters	0.1	100 %	-	-	-	-	-
[I.1] Fire	0.5	100 %	-	-	-	-	-
[I.2] Water	0.5	50%	-	-	-	-	-
[I.*] Other industrial disasters	0.5	100 %	-	-	-	-	-
[I.3] Environmental pollution	0.1	50%	-	-	-	-	-
[I.4] Electromagnetic pollution	1	10%	-	-	-	-	-
[I.5.2] Hardware failure	1	50%	-	-	-	-	-
[I.6] Power interruption	1	100 %	-	-	-	-	-
[I.7] Unsuitable temperature or humidity conditions	1	100 %	-	-	-	-	-
[I.8] Communications services failure	1	50%	-	-	-	-	-
[I.11] Electromagnetic emanations (TEMPEST)	1	-	-	1%	-	-	-
[E.2] System / Security administrator errors	1	20%	20%	20%	-	-	-
[E.9] [Re-]routing errors	1	-	-	10%	-	-	-
[E.10] Sequence errors	1	-	10%	-	-	-	-
[E.15] Accidental alteration of the information	1	-	10%	-	-	-	-
[E.18] Destruction of information	1	1%	-	-	-	-	-
[E.19] Information leaks	1	-	-	10%	-	-	-
[E.23] Defects in hardware maintenance / updating	1	10%	-	-	-	-	-
[E.24] System failure due to exhaustion of resources	10	50%	-	-	-	-	-
[E.25] Equipment loss	1	20%	-	50%	-	-	-
[E.28] Staff shortage	1	10%	-	-	-	-	-
[A.5] Masquerading of identity	1	-	10%	50%	100 %	-	-
[A.7] Misuse	1	10%	10%	10%	-	-	-
[A.9] [Re-]routing of messages	1	-	-	10%	-	-	-
[A.10] Sequence alteration	1	-	10%	-	-	-	-
[A.11] Unauthorised access	1	10%	10%	50%	100 %	-	-
[A.12] Traffic analysis	1	-	-	2%	-	-	-
[A.14] Eavesdropping	1	-	-	1%	-	-	-
[A.15] Deliberate alteration of information	1	-	50%	-	-	-	-
[A.18] Destruction of information	1	50%	-	-	-	-	-
[A.19] Disclosure of information	10	-	-	50%	-	-	-
[A.23] Hardware manipulation	0.5	100 %	-	50%	-	-	-
[A.24] Denial of service	10	100 %	-	-	-	-	-
[A.25] Theft	0.5	20%	-	50%	-	-	-
[A.26] Destructive attack	1	100 %	-	-	-	-	-

[A.28] Staff shortage	0.5	20%	-	-	-	-	-
[A.29] Extortion	0.9	50%	100 %	100 %	-	-	-
[A.30] Social engineering	0.5	50%	100 %	100 %	-	-	-

[Modem] Modem

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[N.1] Fire	0.1	100 %	-	-	-	-	-
[N.2] Water	0.1	50%	-	-	-	-	-
[N.*] Other natural disasters	0.1	100 %	-	-	-	-	-
[I.1] Fire	0.5	100 %	-	-	-	-	-
[I.2] Water	0.5	50%	-	-	-	-	-
[I.*] Other industrial disasters	0.5	100 %	-	-	-	-	-
[I.3] Environmental pollution	0.1	50%	-	-	-	-	-
[I.4] Electromagnetic pollution	1	10%	-	-	-	-	-
[I.5.2] Hardware failure	1	50%	-	-	-	-	-
[I.6] Power interruption	1	100 %	-	-	-	-	-
[I.7] Unsuitable temperature or humidity conditions	1	100 %	-	-	-	-	-
[I.8] Communications services failure	1	50%	-	-	-	-	-
[I.11] Electromagnetic emanations (TEMPEST)	1	-	-	1%	-	-	-
[E.2] System / Security administrator errors	1	20%	20%	20%	-	-	-
[E.9] [Re-]routing errors	1	-	-	10%	-	-	-
[E.10] Sequence errors	1	-	10%	-	-	-	-
[E.15] Accidental alteration of the information	1	-	10%	-	-	-	-
[E.18] Destruction of information	1	1%	-	-	-	-	-
[E.19] Information leaks	1	-	-	10%	-	-	-
[E.23] Defects in hardware maintenance / updating	1	10%	-	-	-	-	-
[E.24] System failure due to exhaustion of resources	10	50%	-	-	-	-	-
[E.25] Equipment loss	1	20%	-	50%	-	-	-
[E.28] Staff shortage	1	10%	-	-	-	-	-
[A.5] Masquerading of identity	1	-	10%	50%	100 %	-	-
[A.7] Misuse	1	10%	10%	10%	-	-	-
[A.9] [Re-]routing of messages	1	-	-	10%	-	-	-

[A.10] Sequence alteration	1	-	10%	-	-	-	-
[A.11] Unauthorised access	1	10%	10%	50%	100 %	-	-
[A.12] Traffic analysis	1	-	-	2%	-	-	-
[A.14] Eavesdropping	1	-	-	10%	-	-	-
[A.15] Deliberate alteration of information	1	-	50%	-	-	-	-
[A.18] Destruction of information	1	50%	-	-	-	-	-
[A.19] Disclosure of information	10	-	-	50%	-	-	-
[A.23] Hardware manipulation	0.5	100 %	-	50%	-	-	-
[A.24] Denial of service	10	100 %	-	-	-	-	-
[A.25] Theft	0.5	20%	-	50%	-	-	-
[A.26] Destructive attack	1	100 %	-	-	-	-	-
[A.28] Staff shortage	0.5	20%	-	-	-	-	-
[A.29] Extortion	0.9	50%	100 %	100 %	-	-	-
[A.30] Social engineering	0.5	50%	100 %	100 %	-	-	-

[AP] Access Point

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[N.1] Fire	0.1	100 %	-	-	-	-	-
[N.2] Water	0.1	50%	-	-	-	-	-
[N.*] Other natural disasters	0.1	100 %	-	-	-	-	-
[I.1] Fire	0.5	100 %	-	-	-	-	-
[I.2] Water	0.5	50%	-	-	-	-	-
[I.*] Other industrial disasters	0.5	100 %	-	-	-	-	-
[I.3] Environmental pollution	0.1	50%	-	-	-	-	-
[I.4] Electromagnetic pollution	1	10%	-	-	-	-	-
[I.5.2] Hardware failure	1	50%	-	-	-	-	-
[I.6] Power interruption	1	100 %	-	-	-	-	-
[I.7] Unsuitable temperature or humidity conditions	1	100 %	-	-	-	-	-
[I.8] Communications services failure	1	50%	-	-	-	-	-
[I.11] Electromagnetic emanations (TEMPEST)	1	-	-	1%	-	-	-
[E.2] System / Security administrator errors	1	20%	20%	20%	-	-	-
[E.9] [Re-]routing errors	1	-	-	10%	-	-	-
[E.10] Sequence errors	1	-	10%	-	-	-	-

[E.15] Accidental alteration of the information	1	-	10%	-	-	-	-
[E.18] Destruction of information	1	1%	-	-	-	-	-
[E.19] Information leaks	1	-	-	10%	-	-	-
[E.23] Defects in hardware maintenance / updating	1	10%	-	-	-	-	-
[E.24] System failure due to exhaustion of resources	10	50%	-	-	-	-	-
[E.25] Equipment loss	1	20%	-	50%	-	-	-
[E.28] Staff shortage	1	10%	-	-	-	-	-
[A.5] Masquerading of identity	1	-	10%	50%	100 %	-	-
[A.7] Misuse	1	10%	10%	10%	-	-	-
[A.9] [Re-]routing of messages	1	-	-	10%	-	-	-
[A.10] Sequence alteration	1	-	10%	-	-	-	-
[A.11] Unauthorised access	1	10%	10%	50%	100 %	-	-
[A.12] Traffic analysis	1	-	-	2%	-	-	-
[A.14] Eavesdropping	1	-	-	10%	-	-	-
[A.15] Deliberate alteration of information	1	-	50%	-	-	-	-
[A.18] Destruction of information	1	50%	-	-	-	-	-
[A.19] Disclosure of information	10	-	-	50%	-	-	-
[A.23] Hardware manipulation	0.5	100 %	-	50%	-	-	-
[A.24] Denial of service	10	100 %	-	-	-	-	-
[A.25] Theft	0.5	20%	-	50%	-	-	-
[A.26] Destructive attack	1	100 %	-	-	-	-	-
[A.28] Staff shortage	0.5	20%	-	-	-	-	-
[A.29] Extortion	0.9	50%	100 %	100 %	-	-	-
[A.30] Social engineering	0.5	50%	100 %	100 %	-	-	-

[Firewall] Firewall

[LAN] Local Area Nettwork

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[I.8] Communications services failure	1	50 %	-	-	-	-	-
[E.2] System / Security administrator errors	1	20 %	20 %	20 %	-	-	-

[E.9] [Re-]routing errors	1	-	-	10 %	-	-	-
[E.10] Sequence errors	1	-	10 %	-	-	-	-
[E.15] Accidental alteration of the information	1	-	1%	-	-	-	-
[E.19] Information leaks	1	-	-	10 %	-	-	-
[E.24] System failure due to exhaustion of resources	1	50 %	-	-	-	-	-
[A.5] Masquerading of identity	1	-	10 %	50 %	100%	-	-
[A.7] Misuse	1	10 %	10 %	10 %	-	-	-
[A.9] [Re-]routing of messages	1	-	-	10 %	-	-	-
[A.10] Sequence alteration	1	-	10 %	-	-	-	-
[A.11] Unauthorised access	1	-	10 %	50 %	100%	-	-
[A.12] Traffic analysis	1	-	-	2%	-	-	-
[A.14] Eavesdropping	1	-	-	1%	-	-	-
[A.15] Deliberate alteration of information	1	-	10 %	-	-	-	-
[A.18] Destruction of information	1	50 %	-	-	-	-	-
[A.24] Denial of service	10	50 %	-	-	-	-	-

[WiFi] WiFi

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Ac]	[V]
[I.8] Communications services failure	1	50 %	-	-	-	-	-
[E.2] System / Security administrator errors	1	20 %	20 %	20 %	-	-	-
[E.9] [Re-]routing errors	1	-	-	10 %	-	-	-
[E.10] Sequence errors	1	-	10 %	-	-	-	-
[E.15] Accidental alteration of the information	1	-	1%	-	-	-	-
[E.19] Information leaks	1	-	-	10 %	-	-	-
[E.24] System failure due to exhaustion of resources	1	50 %	-	-	-	-	-
[A.5] Masquerading of identity	1	-	10	50	100%	-	-

			%	%			
[A.7] Misuse	1	10 %	10 %	10 %	-	-	-
[A.9] [Re-]routing of messages	1	-	-	10 %	-	-	-
[A.10] Sequence alteration	1	-	10 %	-	-	-	-
[A.11] Unauthorised access	1	-	10 %	50 %	100%	-	-
[A.12] Traffic analysis	1	-	-	2%	-	-	-
[A.14] Eavesdropping	1	-	-	10 %	-	-	-
[A.15] Deliberate alteration of information	1	-	10 %	-	-	-	-
[A.18] Destruction of information	1	50 %	-	-	-	-	-
[A.24] Denial of service	10	50 %	-	-	-	-	-

[Generator] Generator

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[N.1] Fire	1	100 %	-	-	-	-	-
[N.2] Water	1	100 %	-	-	-	-	-
[N.*] Other natural disasters	0.5	100 %	-	-	-	-	-
[I.1] Fire	1	100 %	-	-	-	-	-
[I.2] Water	1	100 %	-	-	-	-	-
[I.*] Other industrial disasters	1	100 %	-	-	-	-	-
[I.3] Environmental pollution	1	10%	-	-	-	-	-
[I.4] Electromagnetic pollution	0.1	10%	-	-	-	-	-
[I.9] Interruption of other services or essential supplies	1	50%	-	-	-	-	-
[E.15] Accidental alteration of the information	1	-	10%	-	-	-	-
[E.18] Destruction of information	1	10%	-	-	-	-	-
[E.19] Information leaks	1	-	-	10 %	-	-	-
[E.23] Defects in hardware maintenance / updating	1	1%	-	-	-	-	-

[A.5] Masquerading of identity	0.2	-	100 %	100 %	10 0 %	-	-
[A.6] Abuse of access privileges	1	10%	-	-	-	-	-
[A.7] Misuse	1	10%	-	-	-	-	-
[A.13] Repudiation (denial of actions)	1	-	-	-	-	10 0 %	-
[A.15] Deliberate alteration of information	1	-	50%	-	-	-	-
[A.18] Destruction of information	1	50%	-	-	-	-	-
[A.19] Disclosure of information	1	-	-	50 %	-	-	-
[A.23] Hardware manipulation	1	1%	-	-	-	-	-
[A.24] Denial of service	1	50%	-	-	-	-	-
[A.25] Theft	0.5	1%	-	-	-	-	-
[A.26] Destructive attack	1	100 %	-	-	-	-	-
[A.27] Enemy over-run	1	100 %	-	-	-	-	-

[Cabling] Cabling

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[N.1] Fire	1	100 %	-	-	-	-	-
[N.2] Water	1	100 %	-	-	-	-	-
[N.*] Other natural disasters	0.5	100 %	-	-	-	-	-
[I.1] Fire	1	100 %	-	-	-	-	-
[I.2] Water	1	100 %	-	-	-	-	-
[I.*] Other industrial disasters	1	100 %	-	-	-	-	-
[I.3] Environmental pollution	1	50%	-	-	-	-	-
[I.4] Electromagnetic pollution	0.5	10%	-	-	-	-	-
[I.11] Electromagnetic emanations (TEMPEST)	1	-	-	1%	-	-	-
[E.23] Defects in hardware maintenance / updating	1	10%	-	-	-	-	-
[A.6] Abuse of access privileges	1	10%	-	-	-	-	-
[A.7] Misuse	1	50%	1%	1%	-	-	-
[A.11] Unauthorised access	1	-	10 %	50 %	-	-	-

[A.23] Hardware manipulation	1	50%	-	50 %	-	-	-
[A.25] Theft	0.8	100 %	-	-	-	-	-
[A.26] Destructive attack	1	100 %	-	-	-	-	-
[A.27] Enemy over-run	1	100 %	-	-	-	-	-

[Surveillans] Camera

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[N.1] Fire	1	100 %	-	-	-	-	-
[N.2] Water	1	100 %	-	-	-	-	-
[N.*] Other natural disasters	0.5	100 %	-	-	-	-	-
[I.1] Fire	1	100 %	-	-	-	-	-
[I.2] Water	1	100 %	-	-	-	-	-
[I.*] Other industrial disasters	1	100 %	-	-	-	-	-
[I.3] Environmental pollution	1	50%	-	-	-	-	-
[I.4] Electromagnetic pollution	0.1	10%	-	-	-	-	-
[I.8] Communications services failure	1	50%	-	-	-	-	-
[E.2] System / Security administrator errors	1	20%	20 %	20 %	-	-	-
[E.9] [Re-]routing errors	1	-	-	10 %	-	-	-
[E.10] Sequence errors	1	-	10 %	-	-	-	-
[E.15] Accidental alteration of the information	1	-	1%	-	-	-	-
[E.19] Information leaks	1	-	-	10 %	-	-	-
[E.23] Defects in hardware maintenance / updating	1	10%	-	-	-	-	-
[E.24] System failure due to exhaustion of resources	1	50%	-	-	-	-	-
[A.5] Masquerading of identity	1	-	10 %	50 %	100%	-	-
[A.6] Abuse of access privileges	1	10%	-	-	-	-	-
[A.7] Misuse	1	50%	10 %	10 %	-	-	-
[A.9] [Re-]routing of messages	1	-	-	10 %	-	-	-

[A.10] Sequence alteration	1	-	10 %	-	-	-	-
[A.11] Unauthorised access	1	-	10 %	50 %	100%	-	-
[A.12] Traffic analysis	1	-	-	2%	-	-	-
[A.14] Eavesdropping	1	-	-	1%	-	-	-
[A.15] Deliberate alteration of information	1	-	10 %	-	-	-	-
[A.18] Destruction of information	1	50%	-	-	-	-	-
[A.23] Hardware manipulation	1	50%	-	50 %	-	-	-
[A.24] Denial of service	10	50%	-	-	-	-	-
[A.25] Theft	0.5	10%	-	50 %	-	-	-
[A.26] Destructive attack	1	100 %	-	-	-	-	-
[A.27] Enemy over-run	1	100 %	-	-	-	-	-

[UPS] UPS

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[N.1] Fire	1	100 %	-	-	-	-	-
[N.2] Water	1	100 %	-	-	-	-	-
[N.*] Other natural disasters	0.5	100 %	-	-	-	-	-
[I.1] Fire	1	100 %	-	-	-	-	-
[I.2] Water	1	100 %	-	-	-	-	-
[I.*] Other industrial disasters	1	100 %	-	-	-	-	-
[I.3] Environmental pollution	1	10%	-	-	-	-	-
[I.4] Electromagnetic pollution	0.1	10%	-	-	-	-	-
[I.9] Interruption of other services or essential supplies	1	50%	-	-	-	-	-
[E.15] Accidental alteration of the information	1	-	10%	-	-	-	-
[E.18] Destruction of information	1	10%	-	-	-	-	-
[E.19] Information leaks	1	-	-	10 %	-	-	-
[E.23] Defects in hardware maintenance / updating	1	1%	-	-	-	-	-

[A.5] Masquerading of identity	0.2	-	100 %	100 %	100 %	-	-
[A.6] Abuse of access privileges	1	10%	-	-	-	-	-
[A.7] Misuse	1	10%	-	-	-	-	-
[A.13] Repudiation (denial of actions)	1	-	-	-	-	100 %	-
[A.15] Deliberate alteration of information	1	-	50%	-	-	-	-
[A.18] Destruction of information	1	50%	-	-	-	-	-
[A.19] Disclosure of information	1	-	-	50 %	-	-	-
[A.23] Hardware manipulation	1	1%	-	-	-	-	-
[A.24] Denial of service	1	50%	-	-	-	-	-
[A.25] Theft	0.5	1%	-	-	-	-	-
[A.26] Destructive attack	1	100 %	-	-	-	-	-
[A.27] Enemy over-run	1	100 %	-	-	-	-	-
[A.28] Staff shortage	0.5	10%	-	-	-	-	-
[A.29] Extortion	0.9	10%	10%	50 %	-	-	-
[A.30] Social engineering	0.5	10%	10%	50 %	-	-	-

[Antena] Antena

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[N.1] Fire	1	100 %	-	-	-	-	-
[N.2] Water	1	100 %	-	-	-	-	-
[N.*] Other natural disasters	0.5	100 %	-	-	-	-	-
[I.1] Fire	1	100 %	-	-	-	-	-
[I.2] Water	1	100 %	-	-	-	-	-
[I.*] Other industrial disasters	1	100 %	-	-	-	-	-
[I.3] Environmental pollution	1	10%	-	-	-	-	-
[I.4] Electromagnetic pollution	0.1	10%	-	-	-	-	-
[I.8] Communications services failure	1	50%	-	-	-	-	-
[E.2] System / Security administrator errors	1	20%	20 %	20 %	-	-	-

[E.9] [Re-]routing errors	1	-	-	10 %	-	-	-
[E.10] Sequence errors	1	-	10 %	-	-	-	-
[E.15] Accidental alteration of the information	1	-	1%	-	-	-	-
[E.19] Information leaks	1	-	-	10 %	-	-	-
[E.24] System failure due to exhaustion of resources	1	50%	-	-	-	-	-
[A.5] Masquerading of identity	1	-	10 %	50 %	100%	-	-
[A.6] Abuse of access privileges	1	10%	-	-	-	-	-
[A.7] Misuse	1	10%	10 %	10 %	-	-	-
[A.9] [Re-]routing of messages	1	-	-	10 %	-	-	-
[A.10] Sequence alteration	1	-	10 %	-	-	-	-
[A.11] Unauthorised access	1	-	10 %	50 %	100%	-	-
[A.12] Traffic analysis	1	-	-	2%	-	-	-
[A.14] Eavesdropping	1	-	-	10 %	-	-	-
[A.15] Deliberate alteration of information	1	-	10 %	-	-	-	-
[A.18] Destruction of information	1	50%	-	-	-	-	-
[A.24] Denial of service	10	50%	-	-	-	-	-
[A.26] Destructive attack	0.1	100 %	-	-	-	-	-
[A.27] Enemy over-run	1	100 %	-	-	-	-	-

[RFID] RFID reader

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[N.1] Fire	0.1	100 %	-	-	-	-	-
[N.2] Water	0.1	50%	-	-	-	-	-
[N.*] Other natural disasters	0.1	100 %	-	-	-	-	-
[I.1] Fire	0.5	100 %	-	-	-	-	-
[I.2] Water	0.5	50%	-	-	-	-	-
[I.*] Other industrial disasters	0.5	100 %	-	-	-	-	-

[I.3] Environmental pollution	0.1	50%	-	-	-	-	-
[I.4] Electromagnetic pollution	1	10%	-	-	-	-	-
[I.5.2] Hardware failure	1	50%	-	-	-	-	-
[I.6] Power interruption	1	100 %	-	-	-	-	-
[I.7] Unsuitable temperature or humidity conditions	1	100 %	-	-	-	-	-
[I.11] Electromagnetic emanations (TEMPEST)	1	-	-	1%	-	-	-
[E.23] Defects in hardware maintenance / updating	1	10%	-	-	-	-	-
[E.24] System failure due to exhaustion of resources	10	50%	-	-	-	-	-
[E.25] Equipment loss	1	100 %	-	50 %	-	-	-
[A.11] Unauthorised access	1	10%	10 %	50 %	-	-	-
[A.23] Hardware manipulation	0.5	50%	-	50 %	-	-	-
[A.24] Denial of service	2	100 %	-	-	-	-	-
[A.25] Theft	0.5	100 %	-	50 %	-	-	-
[A.26] Destructive attack	1	100 %	-	-	-	-	-

[UHF] UHF

[InternetP] Internet Provider

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[I.5.1] Software failure	1	50%	-	-	-	-	-
[I.8] Communications services failure	1	100 %	-	-	-	-	-
[E.2] System / Security administrator errors	1	20%	20%	20%	-	-	-
[E.8] Malware diffusion	1	10%	10%	10%	-	-	-
[E.9] [Re-]routing errors	1	-	-	10%	-	-	-
[E.10] Sequence errors	1	-	10%	-	-	-	-
[E.15] Accidental alteration of the information	1	-	10%	-	-	-	-
[E.18] Destruction of information	1	10%	-	-	-	-	-
[E.19] Information leaks	1	-	-	10%	-	-	-
[E.20] Software vulnerabilities	1	1%	20%	20%	-	-	-
[E.21] Defects in software maintenance /	10	1%	10%	50%	-	-	-

updating							
[E.24] System failure due to exhaustion of resources	1	50%	-	-	-	-	-
[A.5] Masquerading of identity	1	-	100 %	100 %	100 %	-	-
[A.7] Misuse	1	10%	10%	50%	-	-	-
[A.8] Malware diffusion	1	100 %	100 %	100 %	-	-	-
[A.9] [Re-]routing of messages	1	-	-	10%	-	-	-
[A.10] Sequence alteration	1	-	10%	-	-	-	-
[A.11] Unauthorised access	1	-	10%	50%	100 %	-	-
[A.12] Traffic analysis	1	-	-	2%	-	-	-
[A.13] Repudiation (denial of actions)	1	-	-	-	-	100 %	-
[A.14] Eavesdropping	1	-	-	10%	-	-	-
[A.15] Deliberate alteration of information	1	-	50%	-	-	-	-
[A.18] Destruction of information	1	50%	-	-	-	-	-
[A.19] Disclosure of information	1	-	-	50%	-	-	-
[A.22] Software manipulation	1	50%	100 %	100 %	-	-	-
[A.24] Denial of service	10	50%	-	-	-	-	-

[Power] Electricity

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[N.1] Fire	0.1	100 %	-	-	-	-	-
[N.2] Water	0.1	50%	-	-	-	-	-
[N.*] Other natural disasters	0.1	100 %	-	-	-	-	-
[I.1] Fire	0.5	100 %	-	-	-	-	-
[I.2] Water	0.5	50%	-	-	-	-	-
[I.*] Other industrial disasters	0.5	100 %	-	-	-	-	-
[I.3] Environmental pollution	0.1	50%	-	-	-	-	-
[I.9] Interruption of other services or essential supplies	1	50%	-	-	-	-	-
[E.15] Accidental alteration of the information	1	-	10%	-	-	-	-
[E.18] Destruction of information	1	10%	-	-	-	-	-
[E.19] Information leaks	1	-	-	10 %	-	-	-

[E.23] Defects in hardware maintenance / updating	1	10%	-	-	-	-	-
[A.5] Masquerading of identity	0.2	-	100 %	100 %	100 %	-	-
[A.7] Misuse	1	50%	-	-	-	-	-
[A.13] Repudiation (denial of actions)	1	-	-	-	-	100 %	-
[A.15] Deliberate alteration of information	1	-	50%	-	-	-	-
[A.18] Destruction of information	1	50%	-	-	-	-	-
[A.19] Disclosure of information	1	-	-	50 %	-	-	-
[A.23] Hardware manipulation	1	50%	-	-	-	-	-
[A.24] Denial of service	1	50%	-	-	-	-	-
[A.25] Theft	0.5	100 %	-	-	-	-	-
[A.26] Destructive attack	1	100 %	-	-	-	-	-
[A.28] Staff shortage	0.5	10%	-	-	-	-	-
[A.29] Extortion	0.9	10%	10%	50 %	-	-	-
[A.30] Social engineering	0.5	10%	10%	50 %	-	-	-

[SRV_Room] Server Room

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[N.1] Fire	1	100 %	-	-	-	-	-
[N.2] Water	1	100 %	-	-	-	-	-
[N.*] Other natural disasters	0.5	100 %	-	-	-	-	-
[I.1] Fire	1	100 %	-	-	-	-	-
[I.2] Water	1	100 %	-	-	-	-	-
[I.*] Other industrial disasters	1	100 %	-	-	-	-	-
[I.3] Environmental pollution	1	10%	-	-	-	-	-
[I.4] Electromagnetic pollution	0.1	10%	-	-	-	-	-
[E.15] Accidental alteration of the information	1	-	10%	-	-	-	-
[E.18] Destruction of information	1	1%	-	-	-	-	-

[E.19] Information leaks	1	-	-	10%	-	-	-
[E.28] Staff shortage	1	20%	-	-	-	-	-
[A.6] Abuse of access privileges	1	10%	-	-	-	-	-
[A.7] Misuse	1	10%	-	-	-	-	-
[A.15] Deliberate alteration of information	1	-	50%	-	-	-	-
[A.18] Destruction of information	1	10%	-	-	-	-	-
[A.19] Disclosure of information	10	-	-	50%	-	-	-
[A.26] Destructive attack	0.1	100 %	-	-	-	-	-
[A.27] Enemy over-run	1	100 %	-	-	-	-	-
[A.28] Staff shortage	0.5	20%	-	-	-	-	-
[A.29] Extortion	0.9	50%	100 %	100 %	-	-	-
[A.30] Social engineering	0.5	50%	100 %	100 %	-	-	-

[Building] Building

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[N.1] Fire	1	100 %	-	-	-	-	-
[N.2] Water	1	100 %	-	-	-	-	-
[N.*] Other natural disasters	0.5	100 %	-	-	-	-	-
[I.1] Fire	1	100 %	-	-	-	-	-
[I.2] Water	1	100 %	-	-	-	-	-
[I.*] Other industrial disasters	1	100 %	-	-	-	-	-
[I.3] Environmental pollution	1	10%	-	-	-	-	-
[I.4] Electromagnetic pollution	0.1	10%	-	-	-	-	-
[E.15] Accidental alteration of the information	1	-	10%	-	-	-	-
[E.18] Destruction of information	1	1%	-	-	-	-	-
[E.19] Information leaks	1	-	-	10%	-	-	-
[E.28] Staff shortage	1	30%	-	-	-	-	-
[A.6] Abuse of access privileges	1	10%	-	-	-	-	-
[A.7] Misuse	1	10%	-	-	-	-	-
[A.15] Deliberate alteration of information	1	-	50%	-	-	-	-
[A.18] Destruction of information	1	10%	-	-	-	-	-
[A.19] Disclosure of information	10	-	-	50%	-	-	-
[A.26] Destructive attack	0.1	100	-	-	-	-	-

		%					
[A.27] Enemy over-run	1	100 %	-	-	-	-	-
[A.28] Staff shortage	0.5	50%	-	-	-	-	-
[A.29] Extortion	0.9	50%	100 %	100 %	-	-	-
[A.30] Social engineering	1	50%	100 %	100 %	-	-	-

[AirCon] Climatization

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[N.1] Fire	1	100 %	-	-	-	-	-
[N.2] Water	1	100 %	-	-	-	-	-
[N.*] Other natural disasters	0.5	100 %	-	-	-	-	-
[I.1] Fire	1	100 %	-	-	-	-	-
[I.2] Water	1	100 %	-	-	-	-	-
[I.*] Other industrial disasters	1	100 %	-	-	-	-	-
[I.3] Environmental pollution	1	50%	-	-	-	-	-
[I.4] Electromagnetic pollution	1	10%	-	-	-	-	-
[I.5.2] Hardware failure	1	50%	-	-	-	-	-
[I.6] Power interruption	1	100 %	-	-	-	-	-
[I.7] Unsuitable temperature or humidity conditions	1	100 %	-	-	-	-	-
[I.9] Interruption of other services or essential supplies	1	50%	-	-	-	-	-
[I.11] Electromagnetic emanations (TEMPEST)	1	-	-	1%	-	-	-
[E.15] Accidental alteration of the information	1	-	10%	-	-	-	-
[E.18] Destruction of information	1	10%	-	-	-	-	-
[E.19] Information leaks	1	-	-	10 %	-	-	-
[E.23] Defects in hardware maintenance / updating	1	10%	-	-	-	-	-
[E.24] System failure due to exhaustion of resources	10	50%	-	-	-	-	-
[E.25] Equipment loss	1	100 %	-	50 %	-	-	-
[A.5] Masquerading of identity	0.2	-	100 %	100 %	100	-	-

					%		
[A.6] Abuse of access privileges	1	10%	-	-	-	-	-
[A.7] Misuse	1	10%	-	-	-	-	-
[A.11] Unauthorised access	1	10%	10%	50 %	-	-	-
[A.13] Repudiation (denial of actions)	1	-	-	-	-	100 %	-
[A.15] Deliberate alteration of information	1	-	50%	-	-	-	-
[A.18] Destruction of information	1	50%	-	-	-	-	-
[A.19] Disclosure of information	1	-	-	50 %	-	-	-
[A.23] Hardware manipulation	1	50%	-	50 %	-	-	-
[A.24] Denial of service	2	100 %	-	-	-	-	-
[A.25] Theft	0.5	100 %	-	50 %	-	-	-
[A.26] Destructive attack	1	100 %	-	-	-	-	-
[A.27] Enemy over-run	1	100 %	-	-	-	-	-

[Blood_Room] Blood Room

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[N.1] Fire	1	100 %	-	-	-	-	-
[N.2] Water	1	100 %	-	-	-	-	-
[N.*] Other natural disasters	0.5	100 %	-	-	-	-	-
[I.1] Fire	1	100 %	-	-	-	-	-
[I.2] Water	1	100 %	-	-	-	-	-
[I.*] Other industrial disasters	1	100 %	-	-	-	-	-
[I.3] Environmental pollution	1	10%	-	-	-	-	-
[I.4] Electromagnetic pollution	0.1	10%	-	-	-	-	-
[E.15] Accidental alteration of the information	1	-	10%	-	-	-	-
[E.18] Destruction of information	1	1%	-	-	-	-	-
[E.19] Information leaks	1	-	-	10%	-	-	-
[E.28] Staff shortage	1	30%	-	-	-	-	-

[A.6] Abuse of access privileges	1	10%	-	-	-	-	-
[A.7] Misuse	1	10%	-	-	-	-	-
[A.15] Deliberate alteration of information	1	-	50%	-	-	-	-
[A.18] Destruction of information	1	10%	-	-	-	-	-
[A.19] Disclosure of information	10	-	-	50%	-	-	-
[A.26] Destructive attack	0.1	100 %	-	-	-	-	-
[A.27] Enemy over-run	1	100 %	-	-	-	-	-
[A.28] Staff shortage	0.5	50%	-	-	-	-	-
[A.29] Extortion	0.9	50%	100 %	100 %	-	-	-
[A.30] Social engineering	1	50%	100 %	100 %	-	-	-

[Laboratories] Laboratories

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[N.1] Fire	1	100 %	-	-	-	-	-
[N.2] Water	1	100 %	-	-	-	-	-
[N.*] Other natural disasters	0.5	100 %	-	-	-	-	-
[I.1] Fire	1	100 %	-	-	-	-	-
[I.2] Water	1	100 %	-	-	-	-	-
[I.*] Other industrial disasters	1	100 %	-	-	-	-	-
[I.3] Environmental pollution	1	10%	-	-	-	-	-
[I.4] Electromagnetic pollution	0.1	10%	-	-	-	-	-
[E.15] Accidental alteration of the information	1	-	10%	-	-	-	-
[E.18] Destruction of information	1	1%	-	-	-	-	-
[E.19] Information leaks	1	-	-	10%	-	-	-
[E.28] Staff shortage	1	30%	-	-	-	-	-
[A.6] Abuse of access privileges	1	10%	-	-	-	-	-
[A.7] Misuse	1	10%	-	-	-	-	-
[A.15] Deliberate alteration of information	1	-	50%	-	-	-	-
[A.18] Destruction of information	1	10%	-	-	-	-	-
[A.19] Disclosure of information	10	-	-	50%	-	-	-
[A.26] Destructive attack	0.1	100 %	-	-	-	-	-
[A.27] Enemy over-run	1	100	-	-	-	-	-

		%					
[A.28] Staff shortage	0.5	50%	-	-	-	-	-
[A.29] Extortion	0.9	50%	100 %	100 %	-	-	-
[A.30] Social engineering	0.5	50%	100 %	100 %	-	-	-

[FD_Room] Financial Department

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[N.1] Fire	1	100 %	-	-	-	-	-
[N.2] Water	1	100 %	-	-	-	-	-
[N.*] Other natural disasters	0.5	100 %	-	-	-	-	-
[I.1] Fire	1	100 %	-	-	-	-	-
[I.2] Water	1	100 %	-	-	-	-	-
[I.*] Other industrial disasters	1	100 %	-	-	-	-	-
[I.3] Environmental pollution	1	10%	-	-	-	-	-
[I.4] Electromagnetic pollution	0.1	10%	-	-	-	-	-
[E.15] Accidental alteration of the information	1	-	10%	-	-	-	-
[E.18] Destruction of information	1	1%	-	-	-	-	-
[E.19] Information leaks	1	-	-	10%	-	-	-
[E.28] Staff shortage	1	30%	-	-	-	-	-
[A.6] Abuse of access privileges	1	10%	-	-	-	-	-
[A.7] Misuse	1	10%	-	-	-	-	-
[A.15] Deliberate alteration of information	1	-	50%	-	-	-	-
[A.18] Destruction of information	1	10%	-	-	-	-	-
[A.19] Disclosure of information	10	-	-	50%	-	-	-
[A.26] Destructive attack	0.1	100 %	-	-	-	-	-
[A.27] Enemy over-run	1	100 %	-	-	-	-	-
[A.28] Staff shortage	0.5	50%	-	-	-	-	-
[A.29] Extortion	0.9	50%	100 %	100 %	-	-	-
[A.30] Social engineering	0.5	50%	100 %	100 %	-	-	-

[MedS] Medical Staff

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[E.15] Accidental alteration of the information	1	-	10 %	-	-	-	-
[E.18] Destruction of information	1	1%	-	-	-	-	-
[E.19] Information leaks	1	-	-	10 %	-	-	-
[E.28] Staff shortage	1	10 %	-	-	-	-	-
[A.15] Deliberate alteration of information	1	-	50 %	-	-	-	-
[A.18] Destruction of information	1	10 %	-	-	-	-	-
[A.19] Disclosure of information	10	-	-	20 %	-	-	-
[A.28] Staff shortage	0.5	50 %	-	-	-	-	-
[A.29] Extortion	0.9	10 %	20 %	20 %	-	-	-
[A.30] Social engineering	0.5	10 %	20 %	20 %	-	-	-

[IT] IS Engineer

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[E.15] Accidental alteration of the information	1	-	10%	-	-	-	-
[E.18] Destruction of information	1	1%	-	-	-	-	-
[E.19] Information leaks	1	-	-	10%	-	-	-
[E.28] Staff shortage	1	20 %	-	-	-	-	-
[A.15] Deliberate alteration of information	1	-	50%	-	-	-	-
[A.18] Destruction of information	1	10 %	-	-	-	-	-
[A.19] Disclosure of information	10	-	-	50%	-	-	-
[A.28] Staff shortage	0.5	50 %	-	-	-	-	-
[A.29] Extortion	0.9	50 %	100 %	100 %	-	-	-
[A.30] Social engineering	0.5	50 %	100 %	100 %	-	-	-

[Admin] Administrative Staff

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[E.15] Accidental alteration of the information	1	-	10 %	-	-	-	-
[E.18] Destruction of information	1	1%	-	-	-	-	-
[E.19] Information leaks	1	-	-	10 %	-	-	-
[E.28] Staff shortage	1	30 %	-	-	-	-	-
[A.15] Deliberate alteration of information	1	-	50 %	-	-	-	-
[A.18] Destruction of information	1	10 %	-	-	-	-	-
[A.19] Disclosure of information	10	-	-	50 %	-	-	-
[A.28] Staff shortage	0.5	50 %	-	-	-	-	-
[A.29] Extortion	0.9	20 %	20 %	50 %	-	-	-
[A.30] Social engineering	0.5	20 %	20 %	20 %	-	-	-

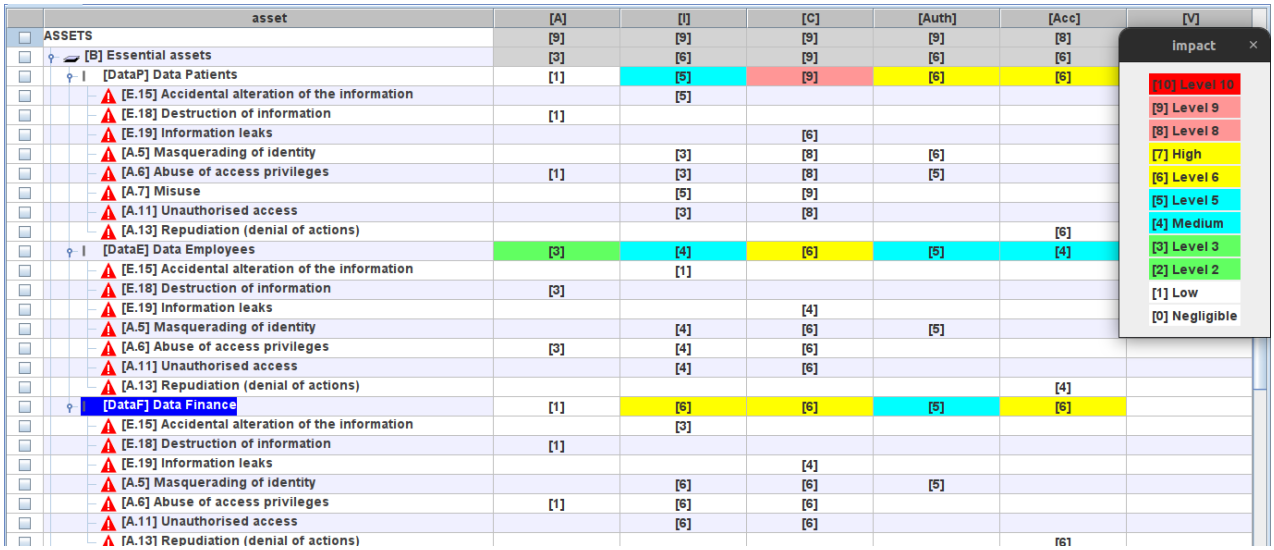
[OPS] Operators

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[E.15] Accidental alteration of the information	1	-	10 %	-	-	-	-
[E.18] Destruction of information	1	1%	-	-	-	-	-
[E.19] Information leaks	1	-	-	10 %	-	-	-
[E.28] Staff shortage	1	30 %	-	-	-	-	-
[A.15] Deliberate alteration of information	1	-	50 %	-	-	-	-
[A.18] Destruction of information	1	10 %	-	-	-	-	-
[A.19] Disclosure of information	10	-	-	50 %	-	-	-
[A.28] Staff shortage	0.5	50 %	-	-	-	-	-
[A.29] Extortion	0.9	20 %	10 %	50 %	-	-	-
[A.30] Social engineering	0.5	20 %	20 %	20 %	-	-	-

[CU] Common User

threat	***frequency***	[A]	[I]	[C]	[Auth]	[Acc]	[V]
[E.15] Accidental alteration of the information	1	-	10 %	-	-	-	-
[E.18] Destruction of information	1	1%	-	-	-	-	-
[E.19] Information leaks	1	-	-	10 %	-	-	-
[E.28] Staff shortage	1	10 %	-	-	-	-	-
[A.15] Deliberate alteration of information	1	-	50 %	-	-	-	-
[A.18] Destruction of information	1	10 %	-	-	-	-	-
[A.19] Disclosure of information	10	-	-	20 %	-	-	-
[A.28] Staff shortage	0.5	50 %	-	-	-	-	-
[A.29] Extortion	0.9	10 %	20 %	20 %	-	-	-
[A.30] Social engineering	0.5	10 %	20 %	20 %	-	-	-

ΠΑΡΑΡΤΗΜΑ Δ. Πίνακας Επίπτωσης/Αγαθό



asset	[A]	[I]	[C]	[Auth]	[Acc]	[V]
ASSETS	[9]	[9]	[9]	[9]	[8]	
[B] Essential assets	[3]	[6]	[9]	[6]	[6]	
[DataP] Data Patients	[1]	[5]	[9]	[6]	[6]	
[E.15] Accidental alteration of the information		[5]				
[E.18] Destruction of information	[1]					
[E.19] Information leaks			[6]			
[A.5] Masquerading of identity		[3]	[8]	[6]		
[A.6] Abuse of access privileges	[1]	[3]	[8]	[5]		
[A.7] Misuse		[5]	[9]			
[A.11] Unauthorised access		[3]	[8]			
[A.13] Repudiation (denial of actions)					[6]	
[DataE] Data Employees	[3]	[4]	[6]	[5]	[4]	
[E.15] Accidental alteration of the information		[1]				
[E.18] Destruction of information	[3]					
[E.19] Information leaks			[4]			
[A.5] Masquerading of identity		[4]	[6]	[5]		
[A.6] Abuse of access privileges	[3]	[4]	[6]			
[A.11] Unauthorised access		[4]	[6]			
[A.13] Repudiation (denial of actions)					[4]	
[DataF] Data Finance	[1]	[6]	[6]	[5]	[6]	
[E.15] Accidental alteration of the information		[3]				
[E.18] Destruction of information	[1]					
[E.19] Information leaks			[4]			
[A.5] Masquerading of identity		[6]	[6]	[5]		
[A.6] Abuse of access privileges	[1]	[6]	[6]			
[A.11] Unauthorised access		[6]	[6]			
[A.13] Repudiation (denial of actions)					[6]	

impact

[10] Level 10
[9] Level 9
[8] Level 8
[7] High
[6] Level 6
[5] Level 5
[4] Medium
[3] Level 3
[2] Level 2
[1] Low
[0] Negligible

is	[S_Blood] Blood Donation and Analysis	[7]	[6]	[9]	[6]	[7]
	[N.1] Fire	[7]				
	[N.2] Water	[6]				
	[N.*] Other natural disasters	[7]				
	[I.1] Fire	[7]				
	[I.2] Water	[6]				
	[I.*] Other industrial disasters	[7]				
	[I.3] Environmental pollution	[6]				
	[I.4] Electromagnetic pollution	[4]				
	[I.5.2] Hardware failure	[6]				
	[I.6] Power interruption	[7]				
	[I.7] Unsuitable temperature or humidity conditions	[7]				
	[I.10] Media degradation	[7]				
	[I.11] Electromagnetic emanations (TEMPEST)			[3]		
	[E.1] User errors	[4]	[3]	[6]		
	[E.2] System / Security administrator errors	[5]	[4]	[7]		
	[E.15] Accidental alteration of the information		[3]			
	[E.18] Destruction of information	[7]				
	[E.19] Information leaks			[6]		
	[E.23] Defects in hardware maintenance / updating	[7]	[3]	[8]		
	[E.24] System failure due to exhaustion of resources	[6]				
	[E.25] Equipment loss	[4]		[8]		
	[E.28] Staff shortage	[4]				
	[A.5] Masquerading of identity		[5]	[8]	[6]	
	[A.6] Abuse of access privileges	[1]	[3]	[8]	[6]	
	[A.7] Misuse	[1]	[3]	[6]		
	[A.11] Unauthorised access		[3]	[8]	[6]	
	[A.13] Repudiation (denial of actions)					[7]
	[A.15] Deliberate alteration of information		[6]			
	[A.18] Destruction of information	[7]				
	[A.19] Disclosure of information			[7]		
	[A.23] Hardware manipulation	[6]		[8]		
	[A.24] Denial of service	[6]				
	[A.25] Theft	[4]		[9]		
	[A.26] Destructive attack	[4]				
	[A.28] Staff shortage	[6]				
	[A.29] Extortion	[4]	[4]	[7]		
	[A.30] Social engineering	[4]	[4]	[7]		

is [S_Sal] Salary	[9]	[9]	[7]	[5]	[7]
[N.1] Fire	[9]				
[N.2] Water	[8]				
[N.*] Other natural disasters	[9]				
[I.1] Fire	[9]				
[I.2] Water	[8]				
[I.*] Other industrial disasters	[9]				
[I.3] Environmental pollution	[8]				
[I.5.1] Software failure	[8]				
[I.7] Unsuitable temperature or humidity conditions	[9]				
[I.10] Media degradation	[9]				
[E.1] User errors	[6]	[6]	[4]		
[E.2] System / Security administrator errors	[7]	[7]	[5]		
[E.8] Malware diffusion	[6]	[6]	[4]		
[E.15] Accidental alteration of the information		[6]			
[E.18] Destruction of information	[9]				
[E.19] Information leaks			[4]		
[E.20] Software vulnerabilities	[3]	[7]	[5]		
[E.21] Defects in software maintenance / updating	[3]	[6]	[6]		
[E.24] System failure due to exhaustion of resources	[8]				
[E.25] Equipment loss	[6]		[6]		
[E.28] Staff shortage	[6]				
[A.5] Masquerading of identity		[8]	[6]	[5]	
[A.6] Abuse of access privileges	[3]	[6]	[6]	[5]	
[A.7] Misuse	[6]	[6]	[6]		
[A.8] Malware diffusion	[9]	[9]	[7]		
[A.11] Unauthorised access		[6]	[6]	[5]	
[A.13] Repudiation (denial of actions)					[7]
[A.15] Deliberate alteration of information		[9]			
[A.18] Destruction of information	[9]				
[A.19] Disclosure of information			[5]		
[A.22] Software manipulation	[8]	[9]	[7]		
[A.24] Denial of service	[8]				
[A.25] Theft	[6]		[7]		
[A.26] Destructive attack	[6]				
[A.28] Staff shortage	[8]				
[A.29] Extortion	[6]	[7]	[5]		
[A.30] Social engineering	[6]	[7]	[5]		

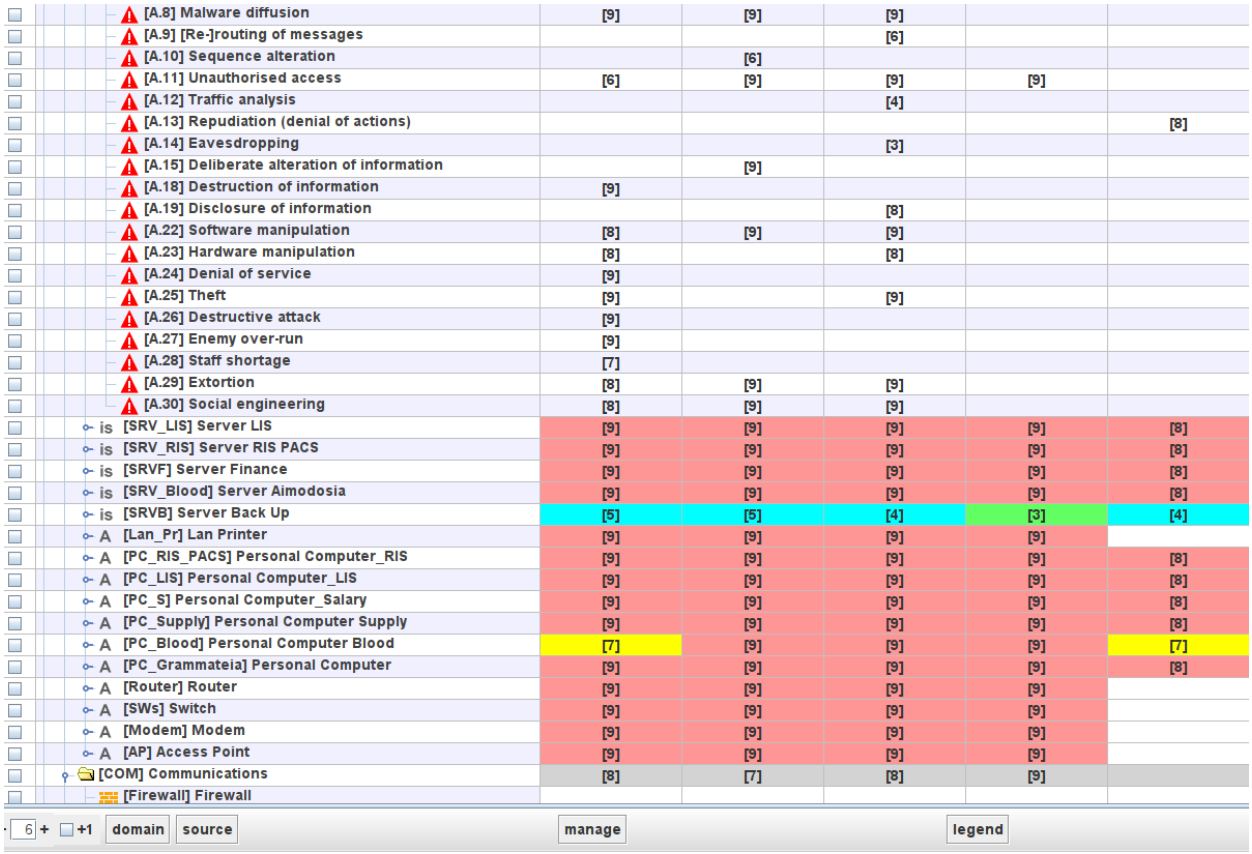
is [S_Sup] Supplies	[8]	[6]	[6]	[7]	[5]
[E.1] User errors	[6]	[4]	[4]		
[E.2] System / Security administrator errors	[7]	[5]	[5]		
[E.15] Accidental alteration of the information		[4]			
[E.18] Destruction of information	[6]				
[E.19] Information leaks			[4]		
[E.24] System failure due to exhaustion of resources	[8]				
[E.28] Staff shortage	[6]				
[A.5] Masquerading of identity		[6]	[6]	[7]	
[A.6] Abuse of access privileges	[3]	[4]	[6]	[7]	
[A.7] Misuse	[3]	[4]	[4]		
[A.11] Unauthorised access		[4]	[6]	[7]	
[A.13] Repudiation (denial of actions)					[5]
[A.15] Deliberate alteration of information		[6]			
[A.18] Destruction of information	[8]				
[A.19] Disclosure of information			[5]		
[A.24] Denial of service	[8]				
[A.28] Staff shortage	[8]				
[A.29] Extortion	[6]	[5]	[5]		
[A.30] Social engineering	[6]	[5]	[5]		
[E] Equipment	[9]	[9]	[9]	[9]	[8]
[SW] Applications	[9]	[9]	[9]	[9]	[7]
A [Antivirus] Antivirus	[7]	[6]	[9]		
[I.5.1] Software failure	[6]				
[E.8] Malware diffusion	[4]	[3]	[6]		
[E.20] Software vulnerabilities	[1]	[4]	[7]		
[E.21] Defects in software maintenance / updating	[1]	[3]	[8]		
[A.7] Misuse	[4]	[3]	[8]		
[A.8] Malware diffusion	[7]	[6]	[9]		
[A.22] Software manipulation	[6]	[6]	[9]		

asset	[A]	[I]	[C]	[Auth]	[Acc]
[ERP] SAP	[9]	[9]	[9]	[9]	[7]
[N.1] Fire	[9]				
[N.2] Water	[8]				
[N.*] Other natural disasters	[9]				
[I.1] Fire	[9]				
[I.2] Water	[8]				
[I.*] Other industrial disasters	[9]				
[I.3] Environmental pollution	[8]				
[I.4] Electromagnetic pollution	[6]				
[I.5.1] Software failure	[8]				
[I.5.2] Hardware failure	[8]				
[I.6] Power interruption	[9]				
[I.7] Unsuitable temperature or humidity conditions	[9]				
[I.8] Communications services failure	[8]				
[I.11] Electromagnetic emanations (TEMPEST)			[3]		
[E.1] User errors	[6]	[6]	[6]		
[E.2] System / Security administrator errors	[7]	[7]	[7]		
[E.3] Monitoring errors (log)		[3]			
[E.8] Malware diffusion	[6]	[6]	[6]		
[E.9] [Re-]routing errors			[6]		
[E.10] Sequence errors		[6]			
[E.15] Accidental alteration of the information		[6]			
[E.18] Destruction of information	[6]				
[E.19] Information leaks			[6]		
[E.20] Software vulnerabilities	[3]	[7]	[7]		
[E.21] Defects in software maintenance / updating	[3]	[6]	[8]		
[E.23] Defects in hardware maintenance / updating	[6]				
[E.24] System failure due to exhaustion of resources	[8]				
[E.25] Equipment loss	[9]		[9]		
[E.28] Staff shortage	[7]				
[A.3] Manipulation of activity records (log)		[8]			
[A.5] Masquerading of identity		[8]	[8]	[9]	
[A.6] Abuse of access privileges	[3]	[6]	[8]	[9]	
[A.7] Misuse	[6]	[6]	[8]		
[A.8] Malware diffusion	[9]	[9]	[9]		
[A.9] [Re-]routing of messages			[6]		
[A.10] Sequence alteration		[6]			
[A.11] Unauthorised access	[6]	[6]	[8]	[9]	
[A.12] Traffic analysis			[4]		
[A.13] Repudiation (denial of actions)					[7]

	[A.14] Eavesdropping			[6]		
	[A.15] Deliberate alteration of information		[8]			
	[A.18] Destruction of information	[8]				
	[A.19] Disclosure of information			[8]		
	[A.22] Software manipulation	[8]	[9]	[9]		
	[A.23] Hardware manipulation	[8]		[8]		
	[A.24] Denial of service	[9]				
	[A.25] Theft	[9]		[9]		
	[A.26] Destructive attack	[9]				
	[A.28] Staff shortage	[8]				
	[A.29] Extortion	[8]	[9]	[9]		
	[A.30] Social engineering	[8]	[9]	[9]		
is	[SQL] My SQL	[9]	[9]	[9]		[7]
	[I.5.1] Software failure	[8]				
	[E.8] Malware diffusion	[6]	[6]	[6]		
	[E.20] Software vulnerabilities	[3]	[7]	[7]		
	[E.21] Defects in software maintenance / updating	[3]	[6]	[8]		
	[A.7] Misuse	[6]	[6]	[8]		
	[A.8] Malware diffusion	[9]	[9]	[9]		
	[A.13] Repudiation (denial of actions)					[7]
	[A.22] Software manipulation	[8]	[9]	[9]		
is	[LIS] LIS app	[7]	[9]	[9]	[9]	[7]
is	[RIS] RIS app PACS	[7]	[9]	[9]	[9]	[7]
	[HW] Hardware	[9]	[9]	[9]	[9]	[8]
it	[SRVDP] Main Server DB	[9]	[9]	[9]	[9]	[8]
is	[SRV_LIS] Server LIS	[9]	[9]	[9]	[9]	[8]
is	[SRV_RIS] Server RIS PACS	[9]	[9]	[9]	[9]	[8]
is	[SRVF] Server Finance	[9]	[9]	[9]	[9]	[8]
is	[SRV_Blood] Server Aimodosia	[9]	[9]	[9]	[9]	[8]
is	[SRVB] Server Back Up	[5]	[5]	[4]	[3]	[4]
A	[Lan_Pr] Lan Printer	[9]	[9]	[9]	[9]	
A	[PC_RIS_PACS] Personal Computer_RIS	[9]	[9]	[9]	[9]	[8]
A	[PC_LIS] Personal Computer_LIS	[9]	[9]	[9]	[9]	[8]
A	[PC_S] Personal Computer_Salary	[9]	[9]	[9]	[9]	[8]
A	[PC_Supply] Personal Computer Supply	[9]	[9]	[9]	[9]	[8]
A	[PC_Blood] Personal Computer Blood	[7]	[9]	[9]	[9]	[7]

	[HW] Hardware	[9]	[9]	[9]	[9]	[8]
it	[SRVDP] Main Server DB	[9]	[9]	[9]	[9]	[8]
	[N.1] Fire	[9]				
	[N.2] Water	[9]				
	[N.*] Other natural disasters	[9]				
	[I.1] Fire	[9]				
	[I.2] Water	[9]				
	[I.*] Other industrial disasters	[9]				
	[I.3] Environmental pollution	[8]				
	[I.4] Electromagnetic pollution	[6]				
	[I.5.1] Software failure	[8]				
	[I.5.2] Hardware failure	[8]				
	[I.6] Power interruption	[9]				
	[I.7] Unsuitable temperature or humidity conditions	[9]				
	[I.8] Communications services failure	[8]				
	[I.10] Media degradation	[9]				
	[I.11] Electromagnetic emanations (TEMPEST)			[3]		
	[E.1] User errors	[6]	[6]	[6]		
	[E.2] System / Security administrator errors	[7]	[7]	[7]		
	[E.3] Monitoring errors (log)		[3]			
	[E.4] Configuration errors		[3]			
	[E.8] Malware diffusion	[6]	[6]	[6]		
	[E.9] [Re-]routing errors			[6]		
	[E.10] Sequence errors		[6]			
	[E.15] Accidental alteration of the information		[8]			
	[E.18] Destruction of information	[9]				
	[E.19] Information leaks			[6]		
	[E.20] Software vulnerabilities	[3]	[7]	[7]		
	[E.21] Defects in software maintenance / updating	[3]	[6]	[8]		
	[E.23] Defects in hardware maintenance / updating	[9]	[6]	[8]		
	[E.24] System failure due to exhaustion of resources	[8]				
	[E.25] Equipment loss	[9]		[9]		
	[E.28] Staff shortage	[7]				
	[A.3] Manipulation of activity records (log)		[8]			
	[A.4] Manipulation of the configuration files	[6]	[6]	[6]		
	[A.5] Masquerading of identity		[8]	[8]	[9]	
	[A.6] Abuse of access privileges	[6]	[9]	[9]	[9]	
	[A.7] Misuse	[8]	[8]	[9]		
	[A.8] Malware diffusion	[9]	[9]	[9]		

.



	[A.8] Malware diffusion	[9]	[9]	[9]		
	[A.9] [Re-]routing of messages			[6]		
	[A.10] Sequence alteration		[6]			
	[A.11] Unauthorised access	[6]	[9]	[9]	[9]	
	[A.12] Traffic analysis			[4]		
	[A.13] Repudiation (denial of actions)					[8]
	[A.14] Eavesdropping			[3]		
	[A.15] Deliberate alteration of information		[9]			
	[A.18] Destruction of information	[9]				
	[A.19] Disclosure of information			[8]		
	[A.22] Software manipulation	[8]	[9]	[9]		
	[A.23] Hardware manipulation	[8]		[8]		
	[A.24] Denial of service	[9]				
	[A.25] Theft	[9]		[9]		
	[A.26] Destructive attack	[9]				
	[A.27] Enemy over-run	[9]				
	[A.28] Staff shortage	[7]				
	[A.29] Extortion	[8]	[9]	[9]		
	[A.30] Social engineering	[8]	[9]	[9]		
is	[SRV_LIS] Server LIS	[9]	[9]	[9]	[9]	[8]
is	[SRV_RIS] Server RIS PACS	[9]	[9]	[9]	[9]	[8]
is	[SRVF] Server Finance	[9]	[9]	[9]	[9]	[8]
is	[SRV_Blood] Server Aimodosia	[9]	[9]	[9]	[9]	[8]
is	[SRVB] Server Back Up	[5]	[5]	[4]	[3]	[4]
A	[Lan_Pr] Lan Printer	[9]	[9]	[9]	[9]	
A	[PC_RIS_PACS] Personal Computer_RIS	[9]	[9]	[9]	[9]	[8]
A	[PC_LIS] Personal Computer_LIS	[9]	[9]	[9]	[9]	[8]
A	[PC_S] Personal Computer_Salary	[9]	[9]	[9]	[9]	[8]
A	[PC_Supply] Personal Computer Supply	[9]	[9]	[9]	[9]	[8]
A	[PC_Blood] Personal Computer Blood	[7]	[9]	[9]	[9]	[7]
A	[PC_Grammateia] Personal Computer	[9]	[9]	[9]	[9]	[8]
A	[Router] Router	[9]	[9]	[9]	[9]	
A	[SWs] Switch	[9]	[9]	[9]	[9]	
A	[Modem] Modem	[9]	[9]	[9]	[9]	
A	[AP] Access Point	[9]	[9]	[9]	[9]	
	[COM] Communications	[8]	[7]	[8]	[9]	
	[Firewall] Firewall					

6 + +1 domain source manage legend

[PC_Grammateia] Personal Computer	[9]	[9]	[9]	[9]	[8]
[N.1] Fire	[9]				
[N.2] Water	[9]				
[N.*] Other natural disasters	[9]				
[I.1] Fire	[9]				
[I.2] Water	[9]				
[I.*] Other industrial disasters	[9]				
[I.3] Environmental pollution	[8]				
[I.4] Electromagnetic pollution	[6]				
[I.5.1] Software failure	[8]				
[I.5.2] Hardware failure	[8]				
[I.6] Power interruption	[9]				
[I.7] Unsuitable temperature or humidity conditions	[9]				
[I.8] Communications services failure	[8]				
[I.10] Media degradation	[9]				
[I.11] Electromagnetic emanations (TEMPEST)			[3]		
[E.1] User errors	[6]	[6]	[6]		
[E.2] System / Security administrator errors	[6]	[7]	[7]		
[E.8] Malware diffusion	[6]	[6]	[6]		
[E.9] [Re-]routing errors			[6]		
[E.10] Sequence errors		[6]			
[E.15] Accidental alteration of the information		[6]			
[E.18] Destruction of information	[9]				
[E.19] Information leaks			[6]		
[E.20] Software vulnerabilities	[3]	[7]	[7]		
[E.21] Defects in software maintenance / updating	[3]	[6]	[8]		
[E.23] Defects in hardware maintenance / updating	[9]	[6]	[8]		
[E.24] System failure due to exhaustion of resources	[8]				
[E.25] Equipment loss	[6]		[8]		
[E.28] Staff shortage	[7]				
[A.5] Masquerading of identity		[8]	[8]	[9]	
[A.6] Abuse of access privileges	[6]	[6]	[8]	[9]	
[A.7] Misuse	[6]	[6]	[8]		
[A.8] Malware diffusion	[9]	[9]	[9]		
[A.9] [Re-]routing of messages			[6]		
[A.10] Sequence alteration		[6]			
[A.11] Unauthorised access	[6]	[6]	[8]	[9]	
[A.12] Traffic analysis			[4]		
[A.13] Repudiation (denial of actions)					[8]
[A.14] Eavesdropping			[3]		

[A.15] Deliberate alteration of information		[9]			
[A.18] Destruction of information	[9]				
[A.19] Disclosure of information			[8]		
[A.22] Software manipulation	[8]	[9]	[9]		
[A.23] Hardware manipulation	[8]		[8]		
[A.24] Denial of service	[9]				
[A.25] Theft	[6]		[9]		
[A.26] Destructive attack	[9]				
[A.27] Enemy over-run	[9]				
[A.28] Staff shortage	[8]				
[A.29] Extortion	[6]	[7]	[8]		
[A.30] Social engineering	[6]	[7]	[7]		
[Router] Router	[9]	[9]	[9]	[9]	
[SWs] Switch	[9]	[9]	[9]	[9]	
[Modem] Modem	[9]	[9]	[9]	[9]	
[AP] Access Point	[9]	[9]	[9]	[9]	
[COM] Communications	[8]	[7]	[8]	[9]	
[Firewall] Firewall					
[LAN] Local Area Nettwork	[8]	[7]	[8]	[9]	
[WiFi] WiFi	[8]	[7]	[8]	[9]	
[AUX] Other elements	[9]	[9]	[9]	[9]	[8]
[Generator] Generator	[5]	[3]	[4]	[4]	[5]
[Cabling] Cabling	[9]	[6]	[8]		
[Surveillans] Camera	[9]	[7]	[8]	[9]	
[UPS] UPS	[9]	[9]	[9]	[9]	[8]
[Antena] Antena	[2]	[0]	[0]	[2]	
[RFID] RFID reader	[9]	[6]	[8]		
[UHF] UHF					
[SS] Subcontracted services	[9]	[9]	[9]	[9]	[8]
[InternetP] Internet Provider	[9]	[9]	[9]	[9]	[8]
[Power] Electricity	[6]	[3]	[4]	[4]	[4]
[L] Facilities	[9]	[9]	[9]	[9]	[8]
[SRV_Room] Server Room	[9]	[9]	[9]		
[Building] Building	[9]	[9]	[9]		
[AirCon] Climatization	[9]	[9]	[9]	[9]	[8]
[Blood_Room] Blood Room	[9]	[9]	[9]		

[LAN] Local Area Nettwork	[8]	[7]	[8]	[9]	
[I.8] Communications services failure	[8]				
[E.2] System / Security administrator errors	[7]	[7]	[7]		
[E.9] [Re-]routing errors			[6]		
[E.10] Sequence errors		[6]			
[E.15] Accidental alteration of the information		[3]			
[E.19] Information leaks			[6]		
[E.24] System failure due to exhaustion of resources	[8]				
[A.5] Masquerading of identity		[6]	[8]	[9]	
[A.7] Misuse	[6]	[6]	[6]		
[A.9] [Re-]routing of messages			[6]		
[A.10] Sequence alteration		[6]			
[A.11] Unauthorised access		[6]	[8]	[9]	
[A.12] Traffic analysis			[4]		
[A.14] Eavesdropping			[3]		
[A.15] Deliberate alteration of information		[6]			
[A.18] Destruction of information	[8]				
[A.24] Denial of service	[8]				
[WiFi] WiFi	[8]	[7]	[8]	[9]	
[I.8] Communications services failure	[8]				
[E.2] System / Security administrator errors	[7]	[7]	[7]		
[E.9] [Re-]routing errors			[6]		
[E.10] Sequence errors		[6]			
[E.15] Accidental alteration of the information		[3]			
[E.19] Information leaks			[6]		
[E.24] System failure due to exhaustion of resources	[8]				
[A.5] Masquerading of identity		[6]	[8]	[9]	
[A.7] Misuse	[6]	[6]	[6]		
[A.9] [Re-]routing of messages			[6]		
[A.10] Sequence alteration		[6]			
[A.11] Unauthorised access		[6]	[8]	[9]	
[A.12] Traffic analysis			[4]		
[A.14] Eavesdropping			[6]		
[A.15] Deliberate alteration of information		[6]			
[A.18] Destruction of information	[8]				
[A.24] Denial of service	[8]				

[UPS] UPS	[9]	[9]	[9]	[9]	[8]
[N.1] Fire	[9]				
[N.2] Water	[9]				
[N.*] Other natural disasters	[9]				
[I.1] Fire	[9]				
[I.2] Water	[9]				
[I.*] Other industrial disasters	[9]				
[I.3] Environmental pollution	[6]				
[I.4] Electromagnetic pollution	[6]				
[I.9] Interruption of other services or essential supplie	[8]				
[E.15] Accidental alteration of the information		[6]			
[E.18] Destruction of information	[6]				
[E.19] Information leaks			[6]		
[E.23] Defects in hardware maintenance / updating	[3]				
[A.5] Masquerading of identity		[9]	[9]	[9]	
[A.6] Abuse of access privileges	[6]				
[A.7] Misuse	[6]				
[A.13] Repudiation (denial of actions)					[8]
[A.15] Deliberate alteration of information		[8]			
[A.18] Destruction of information	[8]				
[A.19] Disclosure of information			[8]		
[A.23] Hardware manipulation	[3]				
[A.24] Denial of service	[8]				
[A.25] Theft	[3]				
[A.26] Destructive attack	[9]				
[A.27] Enemy over-run	[9]				
[A.28] Staff shortage	[6]				
[A.29] Extortion	[6]	[6]	[8]		
[A.30] Social engineering	[6]	[6]	[8]		
[Antena] Antena	[2]	[0]	[0]	[2]	
[RFID] RFID reader	[9]	[6]	[8]		
[UHF] UHF					

[InternetP] Internet Provider	[9]	[9]	[9]	[9]	[8]
[I.5.1] Software failure	[8]				
[I.8] Communications services failure	[9]				
[E.2] System / Security administrator errors	[7]	[7]	[7]		
[E.8] Malware diffusion	[6]	[6]	[6]		
[E.9] [Re-]routing errors			[6]		
[E.10] Sequence errors		[6]			
[E.15] Accidental alteration of the information		[6]			
[E.18] Destruction of information	[6]				
[E.19] Information leaks			[6]		
[E.20] Software vulnerabilities	[3]	[7]	[7]		
[E.21] Defects in software maintenance / updating	[3]	[6]	[8]		
[E.24] System failure due to exhaustion of resources	[8]				
[A.5] Masquerading of identity		[9]	[9]	[9]	
[A.7] Misuse	[6]	[6]	[8]		
[A.8] Malware diffusion	[9]	[9]	[9]		
[A.9] [Re-]routing of messages			[6]		
[A.10] Sequence alteration		[6]			
[A.11] Unauthorised access		[6]	[8]	[9]	
[A.12] Traffic analysis			[4]		
[A.13] Repudiation (denial of actions)					[8]
[A.14] Eavesdropping			[6]		
[A.15] Deliberate alteration of information		[8]			
[A.18] Destruction of information	[8]				
[A.19] Disclosure of information			[8]		
[A.22] Software manipulation	[8]	[9]	[9]		
[A.24] Denial of service	[8]				
[Power] Electricity	[6]	[3]	[4]	[4]	[4]

[L] Facilities	[9]	[9]	[9]	[9]	[8]
[SRV_Room] Server Room	[9]	[9]	[9]		
[N.1] Fire	[9]				
[N.2] Water	[9]				
[N.*] Other natural disasters	[9]				
[I.1] Fire	[9]				
[I.2] Water	[9]				
[I.*] Other industrial disasters	[9]				
[I.3] Environmental pollution	[6]				
[I.4] Electromagnetic pollution	[6]				
[E.15] Accidental alteration of the information		[6]			
[E.18] Destruction of information	[3]				
[E.19] Information leaks			[6]		
[E.28] Staff shortage	[7]				
[A.6] Abuse of access privileges	[6]				
[A.7] Misuse	[6]				
[A.15] Deliberate alteration of information		[8]			
[A.18] Destruction of information	[6]				
[A.19] Disclosure of information			[8]		
[A.26] Destructive attack	[9]				
[A.27] Enemy over-run	[9]				
[A.28] Staff shortage	[7]				
[A.29] Extortion	[8]	[9]	[9]		
[A.30] Social engineering	[8]	[9]	[9]		
[Building] Building	[9]	[9]	[9]		
[AirCon] Climatization	[9]	[9]	[9]	[9]	[8]
[Blood_Room] Blood Room	[9]	[9]	[9]		
[Laboratories] Laboratories	[9]	[9]	[9]		
[FD_Room] Financial Department	[9]	[9]	[9]		

[P] Personnel	[8]	[9]	[9]		
[MedS] Medical Staff	[8]	[8]	[7]		
[E.15] Accidental alteration of the information		[6]			
[E.18] Destruction of information	[3]				
[E.19] Information leaks			[6]		
[E.28] Staff shortage	[6]				
[A.15] Deliberate alteration of information		[8]			
[A.18] Destruction of information	[6]				
[A.19] Disclosure of information			[7]		
[A.28] Staff shortage	[8]				
[A.29] Extortion	[6]	[7]	[7]		
[A.30] Social engineering	[6]	[7]	[7]		
[IT] IS Engineer	[8]	[9]	[9]		
[E.15] Accidental alteration of the information		[6]			
[E.18] Destruction of information	[3]				
[E.19] Information leaks			[6]		
[E.28] Staff shortage	[7]				
[A.15] Deliberate alteration of information		[8]			
[A.18] Destruction of information	[6]				
[A.19] Disclosure of information			[8]		
[A.28] Staff shortage	[8]				
[A.29] Extortion	[8]	[9]	[9]		
[A.30] Social engineering	[8]	[9]	[9]		
[Admin] Administrative Staff	[8]	[8]	[8]		
[OPS] Operators	[8]	[8]	[8]		
[CU] Common User	[8]	[8]	[7]		

ΠΑΡΑΡΤΗΜΑ Ε. Ανακλώμενος Κίνδυνος (Deflected Risk)

[GH] A.7.3. Deflected values > A.7.3.3. table

Export

potential | current | target | PILAR | summary (impact) | summary (risk)

father	dimension	child	dimension	threat	risk	current	target	PILAR
[DataP] Data Patients	[C]	[SRVDP] Main Server DB	[C]	[A.11] Unauthorised access	(8.0)	(7.1)	(5.7)	(4.5)
[DataP] Data Patients	[C]	[SRVDP] Main Server DB	[I]	[A.11] Unauthorised access	(8.0)	(7.1)	(5.7)	(4.5)
[DataP] Data Patients	[C]	[SRV_Blood] Server Aimodosia	[I]	[A.11] Unauthorised access	(8.0)	(7.1)	(5.7)	(4.5)
[DataP] Data Patients	[C]	[SRV_Blood] Server Aimodosia	[C]	[A.11] Unauthorised access	(8.0)	(7.1)	(5.7)	(4.5)
[DataF] Data Finance	[I]	[SRVDP] Main Server DB	[C]	[A.11] Unauthorised access	(8.0)	(7.1)	(5.7)	(4.5)
[DataF] Data Finance	[I]	[SRVDP] Main Server DB	[I]	[A.11] Unauthorised access	(8.0)	(7.1)	(5.7)	(4.5)
[DataF] Data Finance	[I]	[SRV_Blood] Server Aimodosia	[I]	[A.11] Unauthorised access	(8.0)	(7.1)	(5.7)	(4.5)
[DataF] Data Finance	[I]	[SRV_Blood] Server Aimodosia	[C]	[A.11] Unauthorised access	(8.0)	(7.1)	(5.7)	(4.5)
[SRVDP] Main Server DB	[I]	[SRVDP] Main Server DB	[I]	[A.11] Unauthorised access	(8.0)	(7.1)	(5.7)	(4.5)
[SRVDP] Main Server DB	[C]	[SRVDP] Main Server DB	[C]	[A.11] Unauthorised access	(8.0)	(7.1)	(5.7)	(4.5)
[SRV_Blood] Server Aimodosia	[I]	[SRV_Blood] Server Aimodosia	[I]	[A.11] Unauthorised access	(8.0)	(7.1)	(5.7)	(4.5)
[SRV_Blood] Server Aimodosia	[C]	[SRV_Blood] Server Aimodosia	[C]	[A.11] Unauthorised access	(8.0)	(7.1)	(5.7)	(4.5)
[DataP] Data Patients	[C]	[SRVF] Server Finance	[I]	[A.11] Unauthorised access	(8.0)	(7.0)	(5.7)	(4.5)
[DataP] Data Patients	[C]	[SRVF] Server Finance	[C]	[A.11] Unauthorised access	(8.0)	(7.0)	(5.7)	(4.5)
[DataP] Data Patients	[C]	[SRV_RIS] Server RIS PACS	[C]	[A.11] Unauthorised access	(8.0)	(7.0)	(5.7)	(4.5)
[DataP] Data Patients	[C]	[SRV_RIS] Server RIS PACS	[I]	[A.11] Unauthorised access	(8.0)	(7.0)	(5.7)	(4.5)
[DataP] Data Patients	[C]	[SRV_LIS] Server LIS	[C]	[A.11] Unauthorised access	(8.0)	(7.0)	(5.7)	(4.5)
[DataP] Data Patients	[C]	[SRV_LIS] Server LIS	[I]	[A.11] Unauthorised access	(8.0)	(7.0)	(5.7)	(4.5)
[DataF] Data Finance	[I]	[SRVF] Server Finance	[I]	[A.11] Unauthorised access	(8.0)	(7.0)	(5.7)	(4.5)
[DataF] Data Finance	[I]	[SRVF] Server Finance	[C]	[A.11] Unauthorised access	(8.0)	(7.0)	(5.7)	(4.5)
[DataF] Data Finance	[I]	[SRV_RIS] Server RIS PACS	[C]	[A.11] Unauthorised access	(8.0)	(7.0)	(5.7)	(4.5)
[DataF] Data Finance	[I]	[SRV_RIS] Server RIS PACS	[I]	[A.11] Unauthorised access	(8.0)	(7.0)	(5.7)	(4.5)
[DataF] Data Finance	[I]	[SRV_LIS] Server LIS	[C]	[A.11] Unauthorised access	(8.0)	(7.0)	(5.7)	(4.5)
[DataF] Data Finance	[I]	[SRV_LIS] Server LIS	[I]	[A.11] Unauthorised access	(8.0)	(7.0)	(5.7)	(4.5)
[SRV_LIS] Server LIS	[I]	[SRV_LIS] Server LIS	[I]	[A.11] Unauthorised access	(8.0)	(7.0)	(5.7)	(4.5)
[SRV_LIS] Server LIS	[C]	[SRV_LIS] Server LIS	[C]	[A.11] Unauthorised access	(8.0)	(7.0)	(5.7)	(4.5)
[SRV_RIS] Server RIS PACS	[I]	[SRV_RIS] Server RIS PACS	[I]	[A.11] Unauthorised access	(8.0)	(7.0)	(5.7)	(4.5)
[SRV_RIS] Server RIS PACS	[C]	[SRV_RIS] Server RIS PACS	[C]	[A.11] Unauthorised access	(8.0)	(7.0)	(5.7)	(4.5)
[SRVF] Server Finance	[I]	[SRVF] Server Finance	[I]	[A.11] Unauthorised access	(8.0)	(7.0)	(5.7)	(4.5)
[SRVF] Server Finance	[C]	[SRVF] Server Finance	[C]	[A.11] Unauthorised access	(8.0)	(7.0)	(5.7)	(4.5)
[DataP] Data Patients	[C]	[DataP] Data Patients	[C]	[A.11] Unauthorised access	(7.5)	(6.7)	(5.2)	(4.1)
[DataP] Data Patients	[C]	[S_Blood] Blood Donation and A...	[C]	[A.11] Unauthorised access	(7.5)	(6.6)	(5.2)	(4.1)
[DataP] Data Patients	[C]	[RIS] RIS app PACS	[C]	[A.11] Unauthorised access	(7.5)	(6.6)	(5.2)	(4.1)
[DataP] Data Patients	[C]	[LIS] LIS app	[C]	[A.11] Unauthorised access	(7.5)	(6.6)	(5.2)	(4.1)
[DataP] Data Patients	[C]	[PC_RIS_PACS] Personal Compu...	[C]	[A.11] Unauthorised access	(7.5)	(6.6)	(5.2)	(4.1)
[DataP] Data Patients	[C]	[S_NewP] Hospitalization	[C]	[A.11] Unauthorised access	(7.5)	(6.6)	(5.2)	(4.1)
[DataP] Data Patients	[C]	[PC_S] Personal Computer_Salary	[C]	[A.11] Unauthorised access	(7.5)	(6.6)	(5.2)	(4.1)
[DataP] Data Patients	[C]	[PC_LIS] Personal Computer_LIS	[C]	[A.11] Unauthorised access	(7.5)	(6.6)	(5.2)	(4.1)
[DataP] Data Patients	[C]	[PC_Supply] Personal Computer ...	[C]	[A.11] Unauthorised access	(7.5)	(6.6)	(5.2)	(4.1)
[DataF] Data Finance	[I]	[PC_RIS_PACS] Personal Compu...	[C]	[A.11] Unauthorised access	(7.5)	(6.6)	(5.2)	(4.1)

[DataF] Data Finance	[I]	[PC_S] Personal Computer_Salary	[C]	[A.11] Unauthorised access	(7.5)	(6.6)	(5.2)	(4.1)
[DataF] Data Finance	[I]	[PC_LIS] Personal Computer_LIS	[C]	[A.11] Unauthorised access	(7.5)	(6.6)	(5.2)	(4.1)
[DataF] Data Finance	[I]	[PC_Supply] Personal Computer ...	[C]	[A.11] Unauthorised access	(7.5)	(6.6)	(5.2)	(4.1)
[LIS] LIS app	[C]	[LIS] LIS app	[C]	[A.11] Unauthorised access	(7.5)	(6.6)	(5.2)	(4.1)
[RIS] RIS app PACS	[C]	[RIS] RIS app PACS	[C]	[A.11] Unauthorised access	(7.5)	(6.6)	(5.2)	(4.1)
[PC_RIS_PACS] Personal Compu...	[C]	[PC_RIS_PACS] Personal Compu...	[C]	[A.11] Unauthorised access	(7.5)	(6.6)	(5.2)	(4.1)
[PC_LIS] Personal Computer_LIS	[C]	[PC_LIS] Personal Computer_LIS	[C]	[A.11] Unauthorised access	(7.5)	(6.6)	(5.2)	(4.1)
[PC_S] Personal Computer_Salary	[C]	[PC_S] Personal Computer_Salary	[C]	[A.11] Unauthorised access	(7.5)	(6.6)	(5.2)	(4.1)
[PC_Supply] Personal Computer ...	[C]	[PC_Supply] Personal Computer ...	[C]	[A.11] Unauthorised access	(7.5)	(6.6)	(5.2)	(4.1)
[DataP] Data Patients	[C]	[PC_Supply] Personal Computer ...	[Auth]	[A.11] Unauthorised access	(8.0)	(6.5)	(3.6)	(5.0)
[DataP] Data Patients	[C]	[RIS] RIS app PACS	[Auth]	[A.11] Unauthorised access	(8.0)	(6.5)	(3.5)	(4.9)
[DataP] Data Patients	[C]	[PC_LIS] Personal Computer_LIS	[Auth]	[A.11] Unauthorised access	(8.0)	(6.5)	(3.6)	(5.0)
[DataP] Data Patients	[C]	[PC_S] Personal Computer_Salary	[Auth]	[A.11] Unauthorised access	(8.0)	(6.5)	(3.6)	(5.0)
[DataP] Data Patients	[C]	[PC_RIS_PACS] Personal Compu...	[Auth]	[A.11] Unauthorised access	(8.0)	(6.5)	(3.6)	(5.0)
[DataP] Data Patients	[C]	[LIS] LIS app	[Auth]	[A.11] Unauthorised access	(8.0)	(6.5)	(3.5)	(4.9)
[DataF] Data Finance	[I]	[PC_Supply] Personal Computer ...	[Auth]	[A.11] Unauthorised access	(8.0)	(6.5)	(3.6)	(5.0)
[DataF] Data Finance	[I]	[PC_LIS] Personal Computer_LIS	[Auth]	[A.11] Unauthorised access	(8.0)	(6.5)	(3.6)	(5.0)
[DataF] Data Finance	[I]	[PC_S] Personal Computer_Salary	[Auth]	[A.11] Unauthorised access	(8.0)	(6.5)	(3.6)	(5.0)
[DataF] Data Finance	[I]	[PC_RIS_PACS] Personal Compu...	[Auth]	[A.11] Unauthorised access	(8.0)	(6.5)	(3.6)	(5.0)
[LIS] LIS app	[Auth]	[LIS] LIS app	[Auth]	[A.11] Unauthorised access	(8.0)	(6.5)	(3.5)	(4.9)
[RIS] RIS app PACS	[Auth]	[RIS] RIS app PACS	[Auth]	[A.11] Unauthorised access	(8.0)	(6.5)	(3.5)	(4.9)
[PC_RIS_PACS] Personal Compu...	[Auth]	[PC_RIS_PACS] Personal Compu...	[Auth]	[A.11] Unauthorised access	(8.0)	(6.5)	(3.6)	(5.0)
[PC_LIS] Personal Computer_LIS	[Auth]	[PC_LIS] Personal Computer_LIS	[Auth]	[A.11] Unauthorised access	(8.0)	(6.5)	(3.6)	(5.0)
[PC_S] Personal Computer_Salary	[Auth]	[PC_S] Personal Computer_Salary	[Auth]	[A.11] Unauthorised access	(8.0)	(6.5)	(3.6)	(5.0)
[PC_Supply] Personal Computer ...	[Auth]	[PC_Supply] Personal Computer ...	[Auth]	[A.11] Unauthorised access	(8.0)	(6.5)	(3.6)	(5.0)
[DataP] Data Patients	[C]	[ERP] SAP	[C]	[A.11] Unauthorised access	(7.5)	(6.5)	(5.2)	(4.1)
[DataP] Data Patients	[C]	[PC_Grammateia] Personal Com...	[C]	[A.11] Unauthorised access	(7.5)	(6.5)	(5.2)	(4.0)
[DataP] Data Patients	[C]	[PC_Blood] Personal Computer ...	[C]	[A.11] Unauthorised access	(7.5)	(6.5)	(5.2)	(4.0)
[DataF] Data Finance	[I]	[ERP] SAP	[C]	[A.11] Unauthorised access	(7.5)	(6.5)	(5.2)	(4.1)
[DataF] Data Finance	[I]	[PC_Grammateia] Personal Com...	[C]	[A.11] Unauthorised access	(7.5)	(6.5)	(5.2)	(4.0)
[DataF] Data Finance	[I]	[PC_Blood] Personal Computer ...	[C]	[A.11] Unauthorised access	(7.5)	(6.5)	(5.2)	(4.0)
[ERP] SAP	[C]	[ERP] SAP	[C]	[A.11] Unauthorised access	(7.5)	(6.5)	(5.2)	(4.1)
[PC_Blood] Personal Computer ...	[C]	[PC_Blood] Personal Computer ...	[C]	[A.11] Unauthorised access	(7.5)	(6.5)	(5.2)	(4.0)
[PC_Grammateia] Personal Com...	[C]	[PC_Grammateia] Personal Com...	[C]	[A.11] Unauthorised access	(7.5)	(6.5)	(5.2)	(4.0)
[SQL] My SQL	[Acc]	[SRVDP] Main Server DB	[I]	[A.11] Unauthorised access	(7.4)	(6.5)	(5.1)	(3.9)
[SQL] My SQL	[Acc]	[SRV_Blood] Server Aimodosia	[I]	[A.11] Unauthorised access	(7.4)	(6.5)	(5.1)	(3.9)
[DataP] Data Patients	[C]	[SRV_Blood] Server Aimodosia	[Auth]	[A.11] Unauthorised access	(8.0)	(6.4)	(3.3)	(4.8)
[DataP] Data Patients	[C]	[ERP] SAP	[Auth]	[A.11] Unauthorised access	(8.0)	(6.4)	(3.7)	(5.0)
[DataP] Data Patients	[C]	[SRVDP] Main Server DB	[Auth]	[A.11] Unauthorised access	(8.0)	(6.4)	(3.3)	(4.8)

[DataF] Data Finance	[I]	[SRV_Blood] Server Aimodosia	[Auth]	[A.11] Unauthorised access	(8.0)	(6.4)	(3.3)	(4.8)
[DataF] Data Finance	[I]	[ERP] SAP	[Auth]	[A.11] Unauthorised access	(8.0)	(6.4)	(3.7)	(5.0)
[DataF] Data Finance	[I]	[SRVDP] Main Server DB	[Auth]	[A.11] Unauthorised access	(8.0)	(6.4)	(3.3)	(4.8)
[ERP] SAP	[Auth]	[ERP] SAP	[Auth]	[A.11] Unauthorised access	(8.0)	(6.4)	(3.7)	(5.0)
[SRVDP] Main Server DB	[Auth]	[SRVDP] Main Server DB	[Auth]	[A.11] Unauthorised access	(8.0)	(6.4)	(3.3)	(4.8)
[SRV_Blood] Server Aimodosia	[Auth]	[SRV_Blood] Server Aimodosia	[Auth]	[A.11] Unauthorised access	(8.0)	(6.4)	(3.3)	(4.8)
[SQL] My SQL	[Acc]	[SRVF] Server Finance	[I]	[A.11] Unauthorised access	(7.4)	(6.4)	(5.1)	(3.9)
[SQL] My SQL	[Acc]	[SRV_RIS] Server RIS PACS	[I]	[A.11] Unauthorised access	(7.4)	(6.4)	(5.1)	(3.9)
[SQL] My SQL	[Acc]	[SRV_LIS] Server LIS	[I]	[A.11] Unauthorised access	(7.4)	(6.4)	(5.1)	(3.9)
[DataP] Data Patients	[C]	[SRV_RIS] Server RIS PACS	[Auth]	[A.11] Unauthorised access	(8.0)	(6.3)	(3.5)	(4.7)
[DataP] Data Patients	[C]	[PC_Grammateia] Personal Com...	[Auth]	[A.11] Unauthorised access	(8.0)	(6.3)	(3.4)	(4.7)
[DataP] Data Patients	[C]	[SRV_LIS] Server LIS	[Auth]	[A.11] Unauthorised access	(8.0)	(6.3)	(3.5)	(4.7)
[DataP] Data Patients	[C]	[PC_Blood] Personal Computer ...	[Auth]	[A.11] Unauthorised access	(8.0)	(6.3)	(3.4)	(4.7)
[DataP] Data Patients	[C]	[SRVF] Server Finance	[Auth]	[A.11] Unauthorised access	(8.0)	(6.3)	(3.5)	(4.7)
[DataF] Data Finance	[I]	[SRV_RIS] Server RIS PACS	[Auth]	[A.11] Unauthorised access	(8.0)	(6.3)	(3.5)	(4.7)
[DataF] Data Finance	[I]	[PC_Grammateia] Personal Com...	[Auth]	[A.11] Unauthorised access	(8.0)	(6.3)	(3.4)	(4.7)
[DataF] Data Finance	[I]	[SRV_LIS] Server LIS	[Auth]	[A.11] Unauthorised access	(8.0)	(6.3)	(3.5)	(4.7)
[DataF] Data Finance	[I]	[PC_Blood] Personal Computer ...	[Auth]	[A.11] Unauthorised access	(8.0)	(6.3)	(3.4)	(4.7)
[DataF] Data Finance	[I]	[SRVF] Server Finance	[Auth]	[A.11] Unauthorised access	(8.0)	(6.3)	(3.5)	(4.7)
[SRV_LIS] Server LIS	[Auth]	[SRV_LIS] Server LIS	[Auth]	[A.11] Unauthorised access	(8.0)	(6.3)	(3.5)	(4.7)
[SRV_RIS] Server RIS PACS	[Auth]	[SRV_RIS] Server RIS PACS	[Auth]	[A.11] Unauthorised access	(8.0)	(6.3)	(3.5)	(4.7)
[SRVF] Server Finance	[Auth]	[SRVF] Server Finance	[Auth]	[A.11] Unauthorised access	(8.0)	(6.3)	(3.5)	(4.7)
[PC_Blood] Personal Computer ...	[Auth]	[PC_Blood] Personal Computer ...	[Auth]	[A.11] Unauthorised access	(8.0)	(6.3)	(3.4)	(4.7)
[PC_Grammateia] Personal Com...	[Auth]	[PC_Grammateia] Personal Com...	[Auth]	[A.11] Unauthorised access	(8.0)	(6.3)	(3.4)	(4.7)
[DataP] Data Patients	[C]	[SRV_RIS] Server RIS PACS	[I]	[A.3] Manipulation of activity rec...	(7.5)	(6.3)	(5.2)	(4.1)
[DataP] Data Patients	[C]	[SRVF] Server Finance	[I]	[A.3] Manipulation of activity rec...	(7.5)	(6.3)	(5.2)	(4.1)
[DataP] Data Patients	[C]	[ERP] SAP	[I]	[A.3] Manipulation of activity rec...	(7.5)	(6.3)	(5.2)	(4.2)
[DataP] Data Patients	[C]	[SRV_Blood] Server Aimodosia	[I]	[A.3] Manipulation of activity rec...	(7.5)	(6.3)	(5.2)	(4.1)
[DataP] Data Patients	[C]	[SRVDP] Main Server DB	[I]	[A.3] Manipulation of activity rec...	(7.5)	(6.3)	(5.2)	(4.1)
[DataF] Data Finance	[I]	[SRV_RIS] Server RIS PACS	[I]	[A.3] Manipulation of activity rec...	(7.5)	(6.3)	(5.2)	(4.1)
[DataF] Data Finance	[I]	[SRVF] Server Finance	[I]	[A.3] Manipulation of activity rec...	(7.5)	(6.3)	(5.2)	(4.1)
[DataF] Data Finance	[I]	[ERP] SAP	[I]	[A.3] Manipulation of activity rec...	(7.5)	(6.3)	(5.2)	(4.2)
[DataF] Data Finance	[I]	[SRV_Blood] Server Aimodosia	[I]	[A.3] Manipulation of activity rec...	(7.5)	(6.3)	(5.2)	(4.1)
[DataF] Data Finance	[I]	[SRVDP] Main Server DB	[I]	[A.3] Manipulation of activity rec...	(7.5)	(6.3)	(5.2)	(4.1)
[ERP] SAP	[I]	[ERP] SAP	[I]	[A.3] Manipulation of activity rec...	(7.5)	(6.3)	(5.2)	(4.2)
[SRVDP] Main Server DB	[I]	[SRVDP] Main Server DB	[I]	[A.3] Manipulation of activity rec...	(7.5)	(6.3)	(5.2)	(4.1)
[SRV_RIS] Server RIS PACS	[I]	[SRV_RIS] Server RIS PACS	[I]	[A.3] Manipulation of activity rec...	(7.5)	(6.3)	(5.2)	(4.1)
[SRVF] Server Finance	[I]	[SRVF] Server Finance	[I]	[A.3] Manipulation of activity rec...	(7.5)	(6.3)	(5.2)	(4.1)
[SRV_Blood] Server Aimodosia	[I]	[SRV_Blood] Server Aimodosia	[I]	[A.3] Manipulation of activity rec...	(7.5)	(6.3)	(5.2)	(4.1)

[DataP] Data Patients	[C]	[SRV_Blood] Server Aimodosia	[I]	[A.6] Abuse of access privileges	{7.1}	{6.3}	{4.8}	{3.7}
[DataE] Data Employees	[A]	[Router] Router	[A]	[A.24] Denial of service	{7.1}	{6.3}	{4.9}	{3.8}
[DataE] Data Employees	[A]	[PC_Supply] Personal Computer ...	[A]	[A.24] Denial of service	{7.1}	{6.3}	{4.9}	{3.8}
[DataE] Data Employees	[A]	[SRV_Blood] Server Aimodosia	[A]	[A.24] Denial of service	{7.1}	{6.3}	{4.9}	{3.8}
[DataE] Data Employees	[A]	[SRV_RIS] Server RIS PACS	[A]	[A.24] Denial of service	{7.1}	{6.3}	{4.9}	{3.8}
[DataE] Data Employees	[A]	[Modem] Modem	[A]	[A.24] Denial of service	{7.1}	{6.3}	{4.9}	{3.8}
[DataE] Data Employees	[A]	[ERP] SAP	[A]	[A.24] Denial of service	{7.1}	{6.3}	{4.9}	{3.8}
[DataE] Data Employees	[A]	[SWs] Switch	[A]	[A.24] Denial of service	{7.1}	{6.3}	{4.9}	{3.8}
[DataE] Data Employees	[A]	[SRV_LIS] Server LIS	[A]	[A.24] Denial of service	{7.1}	{6.3}	{4.9}	{3.8}
[DataE] Data Employees	[A]	[AP] Access Point	[A]	[A.24] Denial of service	{7.1}	{6.3}	{4.9}	{3.8}
[DataE] Data Employees	[A]	[SRVDP] Main Server DB	[A]	[A.24] Denial of service	{7.1}	{6.3}	{4.9}	{3.8}
[DataE] Data Employees	[A]	[SRVF] Server Finance	[A]	[A.24] Denial of service	{7.1}	{6.3}	{4.9}	{3.8}
[DataF] Data Finance	[I]	[SRV_Blood] Server Aimodosia	[I]	[A.6] Abuse of access privileges	{7.1}	{6.3}	{4.8}	{3.7}
[ERP] SAP	[A]	[ERP] SAP	[A]	[A.24] Denial of service	{7.1}	{6.3}	{4.9}	{3.8}
[SRVDP] Main Server DB	[A]	[SRVDP] Main Server DB	[A]	[A.24] Denial of service	{7.1}	{6.3}	{4.9}	{3.8}
[SRV_LIS] Server LIS	[A]	[SRV_LIS] Server LIS	[A]	[A.24] Denial of service	{7.1}	{6.3}	{4.9}	{3.8}
[SRV_RIS] Server RIS PACS	[A]	[SRV_RIS] Server RIS PACS	[A]	[A.24] Denial of service	{7.1}	{6.3}	{4.9}	{3.8}
[SRVF] Server Finance	[A]	[SRVF] Server Finance	[A]	[A.24] Denial of service	{7.1}	{6.3}	{4.9}	{3.8}
[SRV_Blood] Server Aimodosia	[A]	[SRV_Blood] Server Aimodosia	[A]	[A.24] Denial of service	{7.1}	{6.3}	{4.9}	{3.8}
[SRV_Blood] Server Aimodosia	[I]	[SRV_Blood] Server Aimodosia	[I]	[A.6] Abuse of access privileges	{7.1}	{6.3}	{4.8}	{3.7}
[PC_Supply] Personal Computer ...	[A]	[PC_Supply] Personal Computer ...	[A]	[A.24] Denial of service	{7.1}	{6.3}	{4.9}	{3.8}
[Router] Router	[A]	[Router] Router	[A]	[A.24] Denial of service	{7.1}	{6.3}	{4.9}	{3.8}
[SWs] Switch	[A]	[SWs] Switch	[A]	[A.24] Denial of service	{7.1}	{6.3}	{4.9}	{3.8}
[Modem] Modem	[A]	[Modem] Modem	[A]	[A.24] Denial of service	{7.1}	{6.3}	{4.9}	{3.8}
[AP] Access Point	[A]	[AP] Access Point	[A]	[A.24] Denial of service	{7.1}	{6.3}	{4.9}	{3.8}
[DataP] Data Patients	[C]	[SRV_Blood] Server Aimodosia	[I]	[A.5] Masquerading of identity	{7.1}	{6.2}	{4.8}	{3.8}
[DataP] Data Patients	[C]	[SRV_Blood] Server Aimodosia	[C]	[A.5] Masquerading of identity	{7.1}	{6.2}	{4.8}	{3.8}
[DataP] Data Patients	[C]	[SRVDP] Main Server DB	[C]	[A.6] Abuse of access privileges	{7.1}	{6.2}	{4.8}	{3.7}
[DataP] Data Patients	[C]	[SRVDP] Main Server DB	[I]	[A.6] Abuse of access privileges	{7.1}	{6.2}	{4.8}	{3.7}
[DataP] Data Patients	[C]	[SRV_Blood] Server Aimodosia	[C]	[A.6] Abuse of access privileges	{7.1}	{6.2}	{4.8}	{3.7}
[DataE] Data Employees	[A]	[Lan_Pr] Lan Printer	[A]	[A.24] Denial of service	{7.1}	{6.2}	{4.8}	{3.8}
[DataF] Data Finance	[I]	[SRV_Blood] Server Aimodosia	[I]	[A.5] Masquerading of identity	{7.1}	{6.2}	{4.8}	{3.8}
[DataF] Data Finance	[I]	[SRV_Blood] Server Aimodosia	[C]	[A.5] Masquerading of identity	{7.1}	{6.2}	{4.8}	{3.8}
[DataF] Data Finance	[I]	[SRVDP] Main Server DB	[C]	[A.6] Abuse of access privileges	{7.1}	{6.2}	{4.8}	{3.7}
[DataF] Data Finance	[I]	[SRVDP] Main Server DB	[I]	[A.6] Abuse of access privileges	{7.1}	{6.2}	{4.8}	{3.7}
[DataF] Data Finance	[I]	[SRV_Blood] Server Aimodosia	[C]	[A.6] Abuse of access privileges	{7.1}	{6.2}	{4.8}	{3.7}
[SRVDP] Main Server DB	[I]	[SRVDP] Main Server DB	[I]	[A.6] Abuse of access privileges	{7.1}	{6.2}	{4.8}	{3.7}
[SRVDP] Main Server DB	[C]	[SRVDP] Main Server DB	[C]	[A.6] Abuse of access privileges	{7.1}	{6.2}	{4.8}	{3.7}
[SRV_Blood] Server Aimodosia	[I]	[SRV_Blood] Server Aimodosia	[I]	[A.5] Masquerading of identity	{7.1}	{6.2}	{4.8}	{3.8}

[SRV_Blood] Server Aimodosia	[C]	[SRV_Blood] Server Aimodosia	[C]	[A.5] Masquerading of identity	{7.1}	{6.2}	{4.8}	{3.8}
[SRV_Blood] Server Aimodosia	[C]	[SRV_Blood] Server Aimodosia	[C]	[A.6] Abuse of access privileges	{7.1}	{6.2}	{4.8}	{3.7}
[Lan_Pr] Lan Printer	[A]	[Lan_Pr] Lan Printer	[A]	[A.24] Denial of service	{7.1}	{6.2}	{4.8}	{3.8}
[DataE] Data Employees	[A]	[S_Sup] Supplies	[A]	[E.24] System failure due to exh...	{6.6}	{6.2}	{4.3}	{3.3}
[DataE] Data Employees	[A]	[S_Sup] Supplies	[A]	[A.24] Denial of service	{6.6}	{6.2}	{4.3}	{3.3}
[DataE] Data Employees	[A]	[S_Sal] Salary	[A]	[E.24] System failure due to exh...	{6.6}	{6.2}	{4.3}	{3.3}
[DataP] Data Patients	[C]	[PC_S] Personal Computer_Salary	[I]	[A.15] Deliberate alteration of inf...	{7.1}	{6.1}	{4.9}	{3.8}
[DataP] Data Patients	[C]	[SRV_LIS] Server LIS	[I]	[A.15] Deliberate alteration of inf...	{7.1}	{6.1}	{4.9}	{3.8}
[DataP] Data Patients	[C]	[PC_LIS] Personal Computer_LIS	[I]	[A.15] Deliberate alteration of inf...	{7.1}	{6.1}	{4.9}	{3.8}
[DataP] Data Patients	[C]	[SRVF] Server Finance	[C]	[A.6] Abuse of access privileges	{7.1}	{6.1}	{4.8}	{3.7}
[DataP] Data Patients	[C]	[SRVF] Server Finance	[I]	[A.6] Abuse of access privileges	{7.1}	{6.1}	{4.8}	{3.7}
[DataP] Data Patients	[C]	[PC_Grammateia] Personal Com...	[I]	[A.15] Deliberate alteration of inf...	{7.1}	{6.1}	{4.9}	{3.8}
[DataP] Data Patients	[C]	[PC_RIS_PACS] Personal Compu...	[I]	[A.15] Deliberate alteration of inf...	{7.1}	{6.1}	{4.9}	{3.8}
[DataP] Data Patients	[C]	[SRV_RIS] Server RIS PACS	[C]	[A.6] Abuse of access privileges	{7.1}	{6.1}	{4.8}	{3.7}
[DataP] Data Patients	[C]	[SRV_RIS] Server RIS PACS	[I]	[A.6] Abuse of access privileges	{7.1}	{6.1}	{4.8}	{3.7}
[DataP] Data Patients	[C]	[SRV_Blood] Server Aimodosia	[I]	[A.15] Deliberate alteration of inf...	{7.1}	{6.1}	{4.9}	{3.8}
[DataP] Data Patients	[C]	[SRV_LIS] Server LIS	[I]	[A.6] Abuse of access privileges	{7.1}	{6.1}	{4.8}	{3.7}
[DataP] Data Patients	[C]	[SRV_LIS] Server LIS	[C]	[A.6] Abuse of access privileges	{7.1}	{6.1}	{4.8}	{3.7}
[DataP] Data Patients	[C]	[SRVF] Server Finance	[I]	[A.15] Deliberate alteration of inf...	{7.1}	{6.1}	{4.9}	{3.8}
[DataP] Data Patients	[C]	[LIS] LIS app	[I]	[A.5] Masquerading of identity	{7.1}	{6.1}	{4.8}	{3.8}
[DataP] Data Patients	[C]	[LIS] LIS app	[C]	[A.5] Masquerading of identity	{7.1}	{6.1}	{4.8}	{3.8}
[DataP] Data Patients	[C]	[RIS] RIS app PACS	[C]	[A.5] Masquerading of identity	{7.1}	{6.1}	{4.8}	{3.8}
[DataP] Data Patients	[C]	[SRV_RIS] Server RIS PACS	[I]	[A.15] Deliberate alteration of inf...	{7.1}	{6.1}	{4.9}	{3.8}
[DataP] Data Patients	[C]	[RIS] RIS app PACS	[I]	[A.5] Masquerading of identity	{7.1}	{6.1}	{4.8}	{3.8}
[DataP] Data Patients	[C]	[SRVDP] Main Server DB	[I]	[A.15] Deliberate alteration of inf...	{7.1}	{6.1}	{4.9}	{3.8}
[DataP] Data Patients	[C]	[PC_Supply] Personal Computer ...	[I]	[A.15] Deliberate alteration of inf...	{7.1}	{6.1}	{4.9}	{3.8}
[DataP] Data Patients	[C]	[PC_Blood] Personal Computer ...	[I]	[A.15] Deliberate alteration of inf...	{7.1}	{6.1}	{4.9}	{3.8}
[DataF] Data Finance	[I]	[PC_S] Personal Computer_Salary	[I]	[A.15] Deliberate alteration of inf...	{7.1}	{6.1}	{4.9}	{3.8}
[DataF] Data Finance	[I]	[SRV_LIS] Server LIS	[I]	[A.15] Deliberate alteration of inf...	{7.1}	{6.1}	{4.9}	{3.8}
[DataF] Data Finance	[I]	[PC_LIS] Personal Computer_LIS	[I]	[A.15] Deliberate alteration of inf...	{7.1}	{6.1}	{4.9}	{3.8}
[DataF] Data Finance	[I]	[SRVF] Server Finance	[C]	[A.6] Abuse of access privileges	{7.1}	{6.1}	{4.8}	{3.7}
[DataF] Data Finance	[I]	[SRVF] Server Finance	[I]	[A.6] Abuse of access privileges	{7.1}	{6.1}	{4.8}	{3.7}
[DataF] Data Finance	[I]	[PC_Grammateia] Personal Com...	[I]	[A.15] Deliberate alteration of inf...	{7.1}	{6.1}	{4.9}	{3.8}
[DataF] Data Finance	[I]	[PC_RIS_PACS] Personal Compu...	[I]	[A.15] Deliberate alteration of inf...	{7.1}	{6.1}	{4.9}	{3.8}
[DataF] Data Finance	[I]	[SRV_RIS] Server RIS PACS	[C]	[A.6] Abuse of access privileges	{7.1}	{6.1}	{4.8}	{3.7}
[DataF] Data Finance	[I]	[SRV_RIS] Server RIS PACS	[I]	[A.6] Abuse of access privileges	{7.1}	{6.1}	{4.8}	{3.7}
[DataF] Data Finance	[I]	[SRV_Blood] Server Aimodosia	[I]	[A.15] Deliberate alteration of inf...	{7.1}	{6.1}	{4.9}	{3.8}
[DataF] Data Finance	[I]	[SRV_LIS] Server LIS	[I]	[A.6] Abuse of access privileges	{7.1}	{6.1}	{4.8}	{3.7}
[DataF] Data Finance	[I]	[SRV_LIS] Server LIS	[C]	[A.6] Abuse of access privileges	{7.1}	{6.1}	{4.8}	{3.7}

[DataF] Data Finance	[I]	[SRVF] Server Finance	[I]	[A.15] Deliberate alteration of inf...	{7.1}	{6.1}	{4.9}	{3.8}
[DataF] Data Finance	[I]	[SRV_RIS] Server RIS PACS	[I]	[A.15] Deliberate alteration of inf...	{7.1}	{6.1}	{4.9}	{3.8}
[DataF] Data Finance	[I]	[S_Sal] Salary	[I]	[A.15] Deliberate alteration of inf...	{7.1}	{6.1}	{4.9}	{3.8}
[DataF] Data Finance	[I]	[SRVDP] Main Server DB	[I]	[A.15] Deliberate alteration of inf...	{7.1}	{6.1}	{4.9}	{3.8}
[DataF] Data Finance	[I]	[PC_Supply] Personal Computer ...	[I]	[A.15] Deliberate alteration of inf...	{7.1}	{6.1}	{4.9}	{3.8}
[DataF] Data Finance	[I]	[PC_Blood] Personal Computer ...	[I]	[A.15] Deliberate alteration of inf...	{7.1}	{6.1}	{4.9}	{3.8}
[LIS] LIS app	[I]	[LIS] LIS app	[I]	[A.5] Masquerading of identity	{7.1}	{6.1}	{4.8}	{3.8}
[LIS] LIS app	[C]	[LIS] LIS app	[C]	[A.5] Masquerading of identity	{7.1}	{6.1}	{4.8}	{3.8}
[RIS] RIS app PACS	[I]	[RIS] RIS app PACS	[I]	[A.5] Masquerading of identity	{7.1}	{6.1}	{4.8}	{3.8}
[RIS] RIS app PACS	[C]	[RIS] RIS app PACS	[C]	[A.5] Masquerading of identity	{7.1}	{6.1}	{4.8}	{3.8}
[SRVDP] Main Server DB	[I]	[SRVDP] Main Server DB	[I]	[A.15] Deliberate alteration of inf...	{7.1}	{6.1}	{4.9}	{3.8}
[SRV_LIS] Server LIS	[I]	[SRV_LIS] Server LIS	[I]	[A.15] Deliberate alteration of inf...	{7.1}	{6.1}	{4.9}	{3.8}
[SRV_LIS] Server LIS	[I]	[SRV_LIS] Server LIS	[I]	[A.6] Abuse of access privileges	{7.1}	{6.1}	{4.8}	{3.7}
[SRV_LIS] Server LIS	[C]	[SRV_LIS] Server LIS	[C]	[A.6] Abuse of access privileges	{7.1}	{6.1}	{4.8}	{3.7}
[SRV_RIS] Server RIS PACS	[I]	[SRV_RIS] Server RIS PACS	[I]	[A.6] Abuse of access privileges	{7.1}	{6.1}	{4.8}	{3.7}
[SRV_RIS] Server RIS PACS	[I]	[SRV_RIS] Server RIS PACS	[I]	[A.15] Deliberate alteration of inf...	{7.1}	{6.1}	{4.9}	{3.8}
[SRV_RIS] Server RIS PACS	[C]	[SRV_RIS] Server RIS PACS	[C]	[A.6] Abuse of access privileges	{7.1}	{6.1}	{4.8}	{3.7}
[SRVF] Server Finance	[I]	[SRVF] Server Finance	[I]	[A.6] Abuse of access privileges	{7.1}	{6.1}	{4.8}	{3.7}
[SRVF] Server Finance	[I]	[SRVF] Server Finance	[I]	[A.15] Deliberate alteration of inf...	{7.1}	{6.1}	{4.9}	{3.8}
[SRVF] Server Finance	[C]	[SRVF] Server Finance	[C]	[A.6] Abuse of access privileges	{7.1}	{6.1}	{4.8}	{3.7}
[SRV_Blood] Server Aimodosia	[I]	[SRV_Blood] Server Aimodosia	[I]	[A.15] Deliberate alteration of inf...	{7.1}	{6.1}	{4.9}	{3.8}
[PC_RIS_PACS] Personal Compu...	[I]	[PC_RIS_PACS] Personal Compu...	[I]	[A.15] Deliberate alteration of inf...	{7.1}	{6.1}	{4.9}	{3.8}
[PC_LIS] Personal Computer_LIS	[I]	[PC_LIS] Personal Computer_LIS	[I]	[A.15] Deliberate alteration of inf...	{7.1}	{6.1}	{4.9}	{3.8}
[PC_S] Personal Computer_Salary	[I]	[PC_S] Personal Computer_Salary	[I]	[A.15] Deliberate alteration of inf...	{7.1}	{6.1}	{4.9}	{3.8}
[PC_Supply] Personal Computer ...	[I]	[PC_Supply] Personal Computer ...	[I]	[A.15] Deliberate alteration of inf...	{7.1}	{6.1}	{4.9}	{3.8}
[PC_Blood] Personal Computer ...	[I]	[PC_Blood] Personal Computer ...	[I]	[A.15] Deliberate alteration of inf...	{7.1}	{6.1}	{4.9}	{3.8}
[PC_Grammateia] Personal Com...	[I]	[PC_Grammateia] Personal Com...	[I]	[A.15] Deliberate alteration of inf...	{7.1}	{6.1}	{4.9}	{3.8}
[DataE] Data Employees	[A]	[PC_LIS] Personal Computer_LIS	[A]	[A.24] Denial of service	{6.9}	{6.1}	{4.6}	{3.6}
[DataE] Data Employees	[A]	[PC_RIS_PACS] Personal Compu...	[A]	[A.24] Denial of service	{6.9}	{6.1}	{4.6}	{3.6}
[PC_RIS_PACS] Personal Compu...	[A]	[PC_RIS_PACS] Personal Compu...	[A]	[A.24] Denial of service	{6.9}	{6.1}	{4.6}	{3.6}
[PC_LIS] Personal Computer_LIS	[A]	[PC_LIS] Personal Computer_LIS	[A]	[A.24] Denial of service	{6.9}	{6.1}	{4.6}	{3.6}
[DataE] Data Employees	[A]	[S_Sal] Salary	[A]	[A.24] Denial of service	{6.6}	{6.1}	{4.3}	{3.3}
[DataP] Data Patients	[C]	[SRVF] Server Finance	[C]	[A.5] Masquerading of identity	{7.1}	{6.0}	{4.9}	{3.8}
[DataP] Data Patients	[C]	[SRVF] Server Finance	[I]	[A.5] Masquerading of identity	{7.1}	{6.0}	{4.9}	{3.8}
[DataP] Data Patients	[C]	[SRV_LIS] Server LIS	[I]	[A.5] Masquerading of identity	{7.1}	{6.0}	{4.9}	{3.8}
[DataP] Data Patients	[C]	[SRV_LIS] Server LIS	[C]	[A.5] Masquerading of identity	{7.1}	{6.0}	{4.9}	{3.8}
[DataP] Data Patients	[C]	[SRV_RIS] Server RIS PACS	[I]	[A.5] Masquerading of identity	{7.1}	{6.0}	{4.9}	{3.8}
[DataP] Data Patients	[C]	[SRV_RIS] Server RIS PACS	[C]	[A.5] Masquerading of identity	{7.1}	{6.0}	{4.9}	{3.8}
[DataF] Data Finance	[I]	[SRVF] Server Finance	[C]	[A.5] Masquerading of identity	{7.1}	{6.0}	{4.9}	{3.8}

[DataF] Data Finance	[I]	[SRVF] Server Finance	[I]	[A.5] Masquerading of identity	{7.1}	{6.0}	{4.9}	{3.8}
[DataF] Data Finance	[I]	[SRV_LIS] Server LIS	[I]	[A.5] Masquerading of identity	{7.1}	{6.0}	{4.9}	{3.8}
[DataF] Data Finance	[I]	[SRV_LIS] Server LIS	[C]	[A.5] Masquerading of identity	{7.1}	{6.0}	{4.9}	{3.8}
[DataF] Data Finance	[I]	[SRV_RIS] Server RIS PACS	[I]	[A.5] Masquerading of identity	{7.1}	{6.0}	{4.9}	{3.8}
[DataF] Data Finance	[I]	[SRV_RIS] Server RIS PACS	[C]	[A.5] Masquerading of identity	{7.1}	{6.0}	{4.9}	{3.8}
[SRV_LIS] Server LIS	[I]	[SRV_LIS] Server LIS	[I]	[A.5] Masquerading of identity	{7.1}	{6.0}	{4.9}	{3.8}
[SRV_LIS] Server LIS	[C]	[SRV_LIS] Server LIS	[C]	[A.5] Masquerading of identity	{7.1}	{6.0}	{4.9}	{3.8}
[SRV_RIS] Server RIS PACS	[I]	[SRV_RIS] Server RIS PACS	[I]	[A.5] Masquerading of identity	{7.1}	{6.0}	{4.9}	{3.8}
[SRV_RIS] Server RIS PACS	[C]	[SRV_RIS] Server RIS PACS	[C]	[A.5] Masquerading of identity	{7.1}	{6.0}	{4.9}	{3.8}
[SRVF] Server Finance	[I]	[SRVF] Server Finance	[I]	[A.5] Masquerading of identity	{7.1}	{6.0}	{4.9}	{3.8}
[SRVF] Server Finance	[C]	[SRVF] Server Finance	[C]	[A.5] Masquerading of identity	{7.1}	{6.0}	{4.9}	{3.8}
[DataP] Data Patients	[C]	[PC_LIS] Personal Computer_LIS	[C]	[A.25] Theft	{6.9}	{6.0}	{4.6}	{3.7}
[DataP] Data Patients	[C]	[PC_RIS_PACS] Personal Compu...	[C]	[A.25] Theft	{6.9}	{6.0}	{4.6}	{3.7}
[DataP] Data Patients	[C]	[PC_Supply] Personal Computer ...	[C]	[A.25] Theft	{6.9}	{6.0}	{4.6}	{3.7}
[DataP] Data Patients	[C]	[PC_Grammateia] Personal Com...	[C]	[A.25] Theft	{6.9}	{6.0}	{4.6}	{3.5}
[DataP] Data Patients	[C]	[PC_Blood] Personal Computer ...	[C]	[A.25] Theft	{6.9}	{6.0}	{4.6}	{3.5}
[DataE] Data Employees	[A]	[PC_Grammateia] Personal Com...	[A]	[A.24] Denial of service	{6.9}	{6.0}	{4.6}	{3.6}
[DataF] Data Finance	[I]	[PC_LIS] Personal Computer_LIS	[C]	[A.25] Theft	{6.9}	{6.0}	{4.6}	{3.7}
[DataF] Data Finance	[I]	[PC_RIS_PACS] Personal Compu...	[C]	[A.25] Theft	{6.9}	{6.0}	{4.6}	{3.7}
[DataF] Data Finance	[I]	[PC_Supply] Personal Computer ...	[C]	[A.25] Theft	{6.9}	{6.0}	{4.6}	{3.7}
[DataF] Data Finance	[I]	[PC_Grammateia] Personal Com...	[C]	[A.25] Theft	{6.9}	{6.0}	{4.6}	{3.5}
[DataF] Data Finance	[I]	[PC_Blood] Personal Computer ...	[C]	[A.25] Theft	{6.9}	{6.0}	{4.6}	{3.5}
[SQL] My SQL	[Acc]	[PC_RIS_PACS] Personal Compu...	[C]	[A.11] Unauthorised access	{6.9}	{6.0}	{4.6}	{3.6}
[SQL] My SQL	[Acc]	[PC_S] Personal Computer_Salary	[C]	[A.11] Unauthorised access	{6.9}	{6.0}	{4.6}	{3.5}
[SQL] My SQL	[Acc]	[PC_LIS] Personal Computer_LIS	[C]	[A.11] Unauthorised access	{6.9}	{6.0}	{4.6}	{3.6}
[SQL] My SQL	[Acc]	[PC_Supply] Personal Computer ...	[C]	[A.11] Unauthorised access	{6.9}	{6.0}	{4.6}	{3.6}
[PC_RIS_PACS] Personal Compu...	[C]	[PC_RIS_PACS] Personal Compu...	[C]	[A.25] Theft	{6.9}	{6.0}	{4.6}	{3.7}
[PC_LIS] Personal Computer_LIS	[C]	[PC_LIS] Personal Computer_LIS	[C]	[A.25] Theft	{6.9}	{6.0}	{4.6}	{3.7}
[PC_Supply] Personal Computer ...	[C]	[PC_Supply] Personal Computer ...	[C]	[A.25] Theft	{6.9}	{6.0}	{4.6}	{3.7}
[PC_Blood] Personal Computer ...	[C]	[PC_Blood] Personal Computer ...	[C]	[A.25] Theft	{6.9}	{6.0}	{4.6}	{3.5}
[PC_Grammateia] Personal Com...	[A]	[PC_Grammateia] Personal Com...	[A]	[A.24] Denial of service	{6.9}	{6.0}	{4.6}	{3.6}
[PC_Grammateia] Personal Com...	[C]	[PC_Grammateia] Personal Com...	[C]	[A.25] Theft	{6.9}	{6.0}	{4.6}	{3.5}
[DataE] Data Employees	[A]	[RFID] RFID reader	[A]	[E.24] System failure due to exh...	{6.6}	{6.0}	{4.3}	{3.3}
[DataE] Data Employees	[A]	[AirCon] Climatization	[A]	[E.24] System failure due to exh...	{6.6}	{6.0}	{4.3}	{3.3}
[RFID] RFID reader	[A]	[RFID] RFID reader	[A]	[E.24] System failure due to exh...	{6.6}	{6.0}	{4.3}	{3.3}
[AirCon] Climatization	[A]	[AirCon] Climatization	[A]	[E.24] System failure due to exh...	{6.6}	{6.0}	{4.3}	{3.3}

ΠΑΡΑΡΤΗΜΑ Ζ

[27002:2022] Information security controls (beta 20.6.2022)

project: [GH] General Hospital

1. Project data

GH	General Hospital
organisation	Health Care
description	General Hospital in Athens
version	1
date	02/01/2023
system owner	Ioannis Vasilas
library	[std] INFOSEC library (1.2.2022)

roles

is likely to result in high risk? (Art. 35.1; see WP 248)

Evaluation or scoring

Automated-decision making with legal or similar significant effect

Systematic monitoring

Sensitive data or data of a highly personal nature

Data processes on a large scale

Matching or combining datasets

Data concerning vulnerable data subjects

Innovative use or applying new technological or organisational solutions

Prevents data subjects from exercising a right or using a service or a contract

data

controls

License

[edu] Information & Communication Systems Security
Dept. of Information & Communication Systems Eng.
Univ. of the Aegean
[... 1.3.2023]

maturity levels

L0 - non existent
L1 - initial / ad hoc

L2 - repeatable but intuitive
L3 - defined process
L4 - managed and measurable
L5 - optimised

2. Security domains

[base] Base

3. Project phases

[current] current situation
[target] target situation
[PILAR] recommendation

Stage: [base]

4. Security domain: [base] Base

4.1. [5] Organizational controls /PR CR DC

control	level	R	[current]	[target]	[PILAR]
[5] Organizational controls /PR CR DC		4	(_-L2)	(_-L5)	L2-L3 (L2-L4)

4.2. [6] People controls /PR CR DC

control	level	R	[current]	[target]	[PILAR]
[6] People controls /PR CR DC		4	(L2)	(L4)	L3 (L2-L3)

4.3. [7] Physical controls /PR DC

control	level	R	[current]	[target]	[PILAR]
[7] Physical controls /PR DC		4	(L0-L2)	(L4-L5)	L2-L3 (L2-L4)

4.4. [8] Technological controls /PR CR DC

control	level	R	[current]	[target]	[PILAR]
[8] Technological controls /PR CR DC		4	(L0-L2)	(L4-L5)	L2-L3 (L2-L5)

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. International standard ISO/IEC 27000: 2013 2th edition
2. MAGERIT – version 2 Methodology for Information Systems Risk Analysis and Management Book I – The Method
3. MAGERIT – version 3 Methodology for Information Systems Risk Analysis and Management Book I – The Method
4. A comparison of security safeguard selection methods –Thomas Neubauer
5. MAGERIT – version 2 Methodology for Information Systems Risk Analysis and Management III – Techniques
6. PILAR Basic Risk Analysis and Management Help Files
7. Thesis: Karina del Rocío Gaona Vásquez - UNIVERSIDAD POLITÉCNICA SALESIANA SEDE CUENCA - "APLICACIÓN DE LA METODOLOGÍA MAGERIT PARA EL ANÁLISIS Y GESTIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN APLICADO A LA EMPRESA PESQUERA E INDUSTRIAL BRAVITO S.A. EN LA CIUDAD DE MACHALA"
8. Basuki Rahmad - Telkom University, Suhono H Supangkat-Bandung Institute of Technology, Jaka Sembiring, Bandung Institute of Technology, Kridanto Surendro-Bandung Institute of Technology - Threat Scenario Dependency - Based Model of Information Security Risk Analysis
9. Adrián Fernandez, Daniel F. Garcia Department of Informatics University of Oviedo Gijon, Spain (4 December 2016) - Complex vs. Simple Asset Modeling Approaches for Information Security Risk Assessment Evaluation with MAGERIT methodology
10. MAGERIT – version 2 Methodology for Information Systems Risk Analysis and Management II - Catalogue of Elements
11. Thesis: PUYÉN SANTOS VICENTE RAÚL and RIVAS PALACIOS BETTY GUILIANA- Universidad Nacional "Pedro Ruiz Gallo" - "MODELO DE GESTIÓN DE RIESGOS BASADOS EN LA NORMA ISO/IEC 27005 Y METODOLOGÍA MAGERIT PARA MEJORAR LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL HOSPITAL REGIONAL DE LAMBAYEQUE"
12. Haleh Ayatollahi and Ghazal Shagerdi* (2017 Sep 14) - Information Security Risk Assessment in Hospitals - open medical informatics journal
13. Jakub Breier - Asset Valuation Method for Dependent Entities∗
14. Dr Abdollah Salleh (July 21, 2014) - INFORMATION SYSTEMS IN HEALTHCARE
15. Lilian Mitrou, Maria Karyda (August 2006) - Employees' privacy vs. employers' security: Can they be balanced?
16. Maria Karydaa, Evangelos Kiountouzisa, Spyros Kokolakis - Information systems security policies: a contextual perspective
17. S. Tyali and D. Pottas 2010 - Information Security Management Systems in the Healthcare Context

18. Pedro Tubío Figueira, Cristina López Bravo, José Luis Rivas López - Improving information security risk analysis by including threat-occurrence predictive models
19. E. Vicente, A. Mateos, A. Jiménez-Martín - Risk analysis in information systems: A fuzzification of the MAGERIT methodology
20. Γεώργιος Καμπουράκης "Εισαγωγή στην ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων" Σημειώσεις, Τμήμα Μηχανικών Πληροφοριακών Συστημάτων Πανεπιστήμιο Αιγαίου
21. Thesis: EDGAR ALONSO BOJACA GARAVITO - UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA ESCUELA DE CIENCIAS BASICAS E INGENIERIA ESPECIALIZACION EN SEGURIDAD INFORMATICA GACHETA CUNDINAMARCA 2016 – "DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMATICA BASADO EN LA NORMA ISO/IEC 27001- 27002 PARA EL AREA ADMINISTRATIVA Y DE HISTORIAS CLINICAS DEL HOSPITAL SAN FRANCISCO DE GACHETÁ"
22. Thesis: Motaki Katerina - UNIVERSITY OF PIRAEUS DEPARTMENT OF DIGITAL SYSTEMS DIGITAL SYSTEMS SECURITY DIRECTION – "Risk Analysis and Risk Management in Critical Infrastructures"

ΠΗΓΕΣ ΔΙΑΔΙΚΤΥΟΥ

1. https://www.enisa.europa.eu/
2. https://repository.kallipos.gr/bitstream/11419/1035/1/05_chapter_11.pdf
3. http://www.greece.lrqa.com/standards-and-schemes/iso-iec27001
4. http://www.itworks.lu/risk-analysis
5. https://www.ar-tools.com/magerit/index.html
6. https://www.ar-tools.com/doc/manual_rm_en_20211.pdf
7. Hospital Asset Tracking Software: A Guide for Healthcare Orgs (scnsoft.com)
8. https://www.ar-tools.com/en/