# ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑΩΣ

# ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

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


## ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

# *Policy Enforcement Tool and Procedures*


**ΧΑΡΑΛΑΜΠΟΣ ΚΑΛΕΥΡΟΣΟΓΛΟΥ**



**ΙΟΥΝΙΟΣ, 2015**

## Επιβλέπων Καθηγητής

## Αναπληρωτής Καθηγητής Κωνσταντίνος Λαμπρινουδάκης, Πανεπιστήμιο Πειραιώς

# Εξεταστική Επιτροπή

Καθηγητής Σωκράτης Κάτσικας

Αναπληρωτής Καθηγητής Κωνσταντίνος Λαμπρινουδάκης

Αναπληρωτής Καθηγητής Χρήστος Ξενάκης

# Περιεχόμενα

# Ευχαριστίες

*Για την ολοκλήρωση αυτής της διπλωματικής εργασίας συντέλεσαν αρκετοί παράγοντες. Αρχικά θα ήθελα να ευχαριστήσω τον κ. Λαμπρινουδάκη, υπεύθυνο καθηγητή, για την καθοδήγηση και βοήθεια την οποία μου παρείχε.*

*Επίσης θα ήθελα να ευχαριστήσω το προσωπικό του Λόχου Κυβερνοάμυνας του Κέντρου Πληροφορικής Υποστήριξης του Ελληνικού Στρατού για την άψογη συνεργασία κατά τη διάρκεια εκπόνησης της διπλωματικής εργασίας.*

*Τέλος θα ήθελα να ευχαριστήσω ιδιαίτερα το φίλο μου Αποστόλη για την πολύτιμη βοήθεια του καθώς επίσης και για τη στήριξη την οποία μου παρείχε.*

# Περίληψη

Η ασφάλεια των υπολογιστικών συστημάτων πλέον έχει εξελιχθεί κατά πολύ. Σε οποιαδήποτε μορφή οργανισμού ή εταιρείας το ζήτημα της ασφάλειας των ψηφιακών συστημάτων είναι ιδιαίτερα σημαντικό και βέβαια θα μπορούσε να χαρακτηριστεί ως κρίσιμο. Η κρισιμότητα αυτή απορρέει από το πόσο σημαντικές είναι οι πληροφορίες τις οποίες διαχειρίζεται η εταιρία.

Έχει επέλθει λοιπόν ένα σημείο το οποίο χαρακτηρίζεται από έντονη ανταγωνιστικότητα στον εργασιακό χώρο για τις εταιρείες ασφάλειας. Προκειμένου λοιπόν να προσεγγίσουν επιπλέον πελατεία οι εταιρείες χρειάζεται να απορρέουν αξιοπιστία προς τον πελάτη. Η αξιοπιστία αυτή μπορεί να επιτευχθεί μέσα από διεθνείς πιστοποιήσεις προτύπων ασφαλείας, όπως τα πρότυπα ISO/IEC, PCI κ.τ.λ.

Η συγκεκριμένη διπλωματική εργασία χωρίζεται σε δύο βασικά μέρη. Αρχικά θα αναλυθούν οι διαφορές των προτύπων ISO/IEC 27001:2005 και ISO/IEC 27001:2013. Στη συνέχεια θα αναλυθούν οι απαιτήσεις της εφαρμογής, η οποία δημιουργήθηκε για τις ανάγκες της διπλωματικής εργασίας, καθώς επίσης θα αναπτυχθεί και ένας οδηγός χρήσης της εφαρμογής, ο οποίος θα εξηγεί επακριβώς τη λειτουργικότητα αυτής.

# Κεφάλαιο 1

## Εισαγωγή

Η ασφάλεια πληροφοριών διαδραματίζει σημαντικό ρόλο σε όλες τις πτυχές της πληροφορικής. Η εκάστοτε εταιρεία επιθυμεί να αναπτύξει Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών για τον καλύτερο δυνατό έλεγχο της ασφάλειας των δεδομένων των οποίων διαχειρίζεται. Κάτι τέτοιο για να υλοποιηθεί χρειάζεται μια σειρά διαδικασιών οι οποίες θα διέπουν το σύστημα. Αυτές τις διαδικασίες τις ορίζουν τα πρότυπα ασφάλειας πληροφοριών.

Ως πρότυπο ασφάλειας μπορεί να οριστεί ένα σύνολο κανόνων και διαδικασιών, τα οποία διέπουν τη λειτουργία ενός συστήματος το οποίο διαχειρίζεται την ασφάλεια πληροφοριών, ενός οργανισμού ή μιας εταιρείας. Ένα από αυτά τα πρότυπα, και βέβαια από τα σημαντικότερα στο χώρο της ασφάλειας, είναι το ISO 27001.

Το ISO 27001:2013 ως πρότυπο δημιουργεί ένα κλίμα εμπιστοσύνης προς τους πελάτες των εταιρειών που το διαθέτουν καθώς, πέραν της ευρείας αναγνωρισιμότητας του, εγγυάται την ύπαρξη ενός συνόλου κανόνων και διαδικασιών για την επίτευξη του βέλτιστου δυνατού επιπέδου ασφάλειας..

Βέβαια, πέραν του ISO ένα πολύ σημαντικό κομμάτι στη διαχείριση της ασφάλειας είναι η ανάλυση επικινδυνότητας. Η ανάλυση και η διαχείριση κατ' επέκταση των κινδύνων που αντιμετωπίζει ένα πληροφοριακό σύστημα διαδραματίζει πολύ σημαντικό ρόλο στην πρόληψη των απειλών ως προς την ασφάλεια του συστήματος. Για την ανάλυση επικινδυνότητας υπάρχουν διάφορες μέθοδοι οι οποίες βοηθούν ώστε να υλοποιηθεί. Οι χαρακτηριστικότερες αυτών είναι η CRAMM, NIST SP 800-30, ISO 27005, ISO 31000. Σαφώς υπάρχουν και άλλες μέθοδοι οι οποίες μπορούν να επιφέρουν αντίστοιχο αποτέλεσμα. Το σημαντικότερο για την επιλογή μιας μεθόδου είναι το κατά πόσο είναι πλήρης ώστε να καλύψει όλη τη διαδικασία της ανάλυσης επικινδυνότητας που σχετίζεται.

Σαφώς όλα τα προαναφερθέντα θα αναλυθούν περαιτέρω στη συνέχεια καθώς θα αναλυθεί και ο τρόπος με τον οποίο χρησιμοποιήθηκαν για τις ανάγκες της διπλωματικής εργασίας.

## Σκοπός

Σκοπός της διπλωματικής εργασίας είναι η συγκριτική μελέτη των δύο εκδόσεων του ISO 27001 (2005 & 2013) καθώς επίσης και η δημιουργία web εφαρμογής, η οποία έχει ως στόχο να διευκολύνει τον Information Security Officer στη διαχείριση του ISO 27001:2013 καθώς και στην ανάλυση επικινδυνότητας.

Η εφαρμογή παρέχει τη δυνατότητα στο χρήστη να διαχειριστεί τους πόρους (assets) του συστήματος καθώς και να εφαρμόσει στους πόρους τόσο το ISO 27001:2013 καθώς επίσης και τη CRAMM η οποία έχει επιλεχθεί ως μέθοδος ανάλυσης επικινδυνότητας. Οι λόγοι επιλογής της συγκεκριμένης μεθόδου θα αναλυθούν στη συνέχεια εκτενέστερα.

# Κεφάλαιο 2

## Συγκριτική Μελέτη Εκδόσεων του ISO/IEC 27001

### 2.1 Ιστορική Αναδρομή του Προτύπου

Το πρότυπο ISO 27001 δημοσιεύθηκε για πρώτη φορά τον Οκτώβριο του 2005, όταν και ουσιαστικά αντικατέστησε τον προκάτοχο του, το πρότυπο BS7799-2. Το BS7799-2 είχε το ρόλο των προδιαγραφών ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS). Καθώς το BS7799-2 εκδόθηκε στις αρχές της δεκαετίας του ’90, όπως είναι λογικό χρειαζόταν μία ανανέωση στο περιεχόμενό του καθώς και να εναρμονιστεί με τις απαιτήσεις της εποχής. Για αυτόν το λόγο δημοσιεύθηκε το ISO 27001:2005 το οποίο αφενός χρησιμοποίησε το περιεχόμενο του προκατόχου του αλλά αφετέρου διαμορφώθηκε με τέτοιον τρόπο ώστε να συμβαδίζει και με τα υπόλοιπα πρότυπα.

Το κύριο αντικείμενο του προτύπου είναι να παρέχει τις κατάλληλες απαιτήσεις για τη θέσπιση, υλοποίηση, συντήρηση και συνεχή βελτίωση ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ). Επιπροσθέτως, ο σχεδιασμός και η υλοποίηση ενός ΣΔΑΠ σε έναν οργανισμό επηρεάζεται σε πολύ μεγάλο βαθμό από τις ανάγκες του οργανισμού και τα αντικείμενα τα οποία πραγματεύεται, τις απαιτήσεις ασφάλειας, τις οργανωτικές διαδικασίες, τις οποίες χρησιμοποιεί καθώς και τη δομή του οργανισμού.

Η έκδοση του ISO 2005 εισήγαγε το μοντέλο “PDCA”, Plan-Do-Check-Act (Σχεδιασμός-Υλοποίησης-Έλεγχος-Δράση) για τη διάρθρωση των διαδικασιών που προβλέπει το πρότυπο. Ωστόσο στην έκδοση του προτύπου 2013, δίνεται περισσότερη έμφαση στις μεθόδους μέτρησης και αξιολόγησης στο κατά πόσο αποτελεσματικά ένας οργανισμός εφαρμόζει το ΣΔΑΠ.


Εικόνα 1 - Εξέλιξη του ISO

## 2.2 Πλεονεκτήματα χρήσης του ISO 27001:2013

Η απόφαση ενός οργανισμού ή μιας εταιρείας να προχωρήσει στην απόκτηση της πιστοποίησης του ISO 27001:2013 είναι μια απόφαση στρατηγικής σημασίας για τον οργανισμό και το προφίλ αυτού. Αυτό απορρέει από το γεγονός ότι το ISO 27001 μπορεί να προσφέρει πληθώρα πλεονεκτημάτων σε αυτόν που το υιοθετεί.

Αρχικά μέσω των διαδικασιών, τις οποίες ο οργανισμός υποχρεούται να ακολουθήσει, καταλήγει σε σημείο όπου μπορεί να διατηρεί τις πληροφορίες, τις οποίες φιλοξενεί ασφαλείς. Αυτό μπορεί να επιτευχθεί από την εφαρμογή των Controls του Annex A. Σαφώς το πρότυπο παρέχει στον οργανισμό ένα ανταγωνιστικό πλεονέκτημα σε σχέση με τους ανταγωνιστές καθώς η πιστοποίηση ως προς το ISO 27001 δημιουργεί κλίμα εμπιστοσύνης.

Βέβαια ένα ακόμα σημαντικό πλεονέκτημα είναι η καλλιέργεια κουλτούρας ασφάλειας στο προσωπικό του οργανισμού, το οποίο μπαίνει στη διαδικασία πιστοποίησης. Είναι γνωστό ότι ο ανθρώπινος παράγοντας είναι υπεύθυνος για πολλά από τα λάθη τα οποία γίνονται στον τομέα της ασφάλειας. Άρα, με το να είναι ευαισθητοποιημένο το προσωπικό του οργανισμού ως προς την ασφάλεια εξασφαλίζει ότι υπάρχει ένα επίπεδο ασφάλειας το οποίο αποτρέπει τα λάθη, τα οποία προέρχονται από τον ανθρώπινο παράγοντα.

Επιπλέον, μέσω του προτύπου υπάρχουν διαδικασίες οι οποίες μπορούν να παρέχουν τρόπο διαχείρισης του ρίσκου και σαφώς με τη σωστή διαχείριση μπορεί να επέλθει και ελάττωση του ρίσκου, κάτι το οποίο εξασφαλίζει, με τη σωστή χρήση των

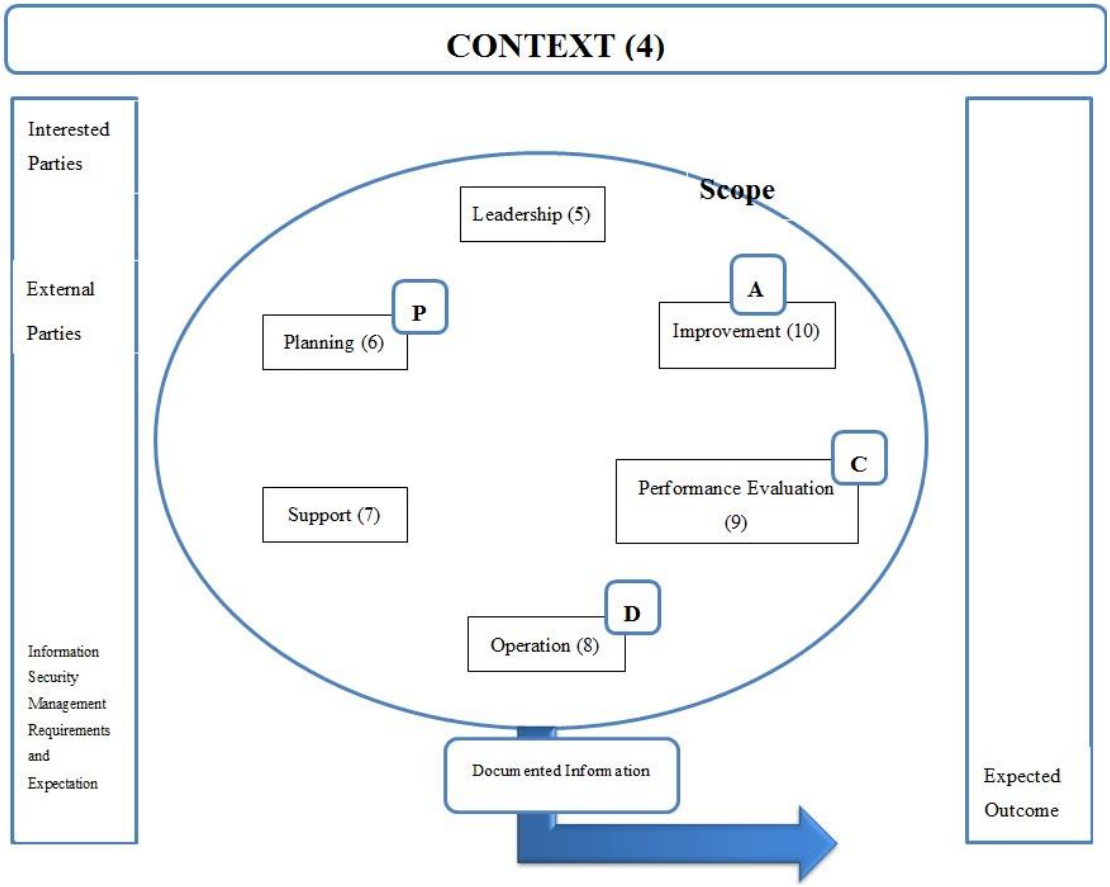
διαδικασιών βέβαια, το κατάλληλο πλαίσιο για την ασφάλεια των αγαθών (assets) του οργανισμού.

Ένα ακόμα πλεονέκτημα είναι η συμμόρφωση με τις νομικές απαιτήσεις στις οποίες υπόκειται η κάθε εταιρεία/οργανισμός ανάλογα βέβαια με τη χώρα στην οποία είναι. Το πρότυπο προβλέπει μέσω των διαδικασιών του το τι πρέπει να ακολουθείται προκειμένου να μην υπάρχουν νομικές ατέλειες.

Όπως γίνεται αντιληπτό, υπάρχει πληθώρα πλεονεκτημάτων, την οποία προσφέρει το ISO 27001 και αυτό είναι που το κάνει περιζήτητο στους οργανισμούς για να το αποκτήσουν και συνάμα να γίνουν και αυτοί ανταγωνιστικοί στην αγορά εργασίας.

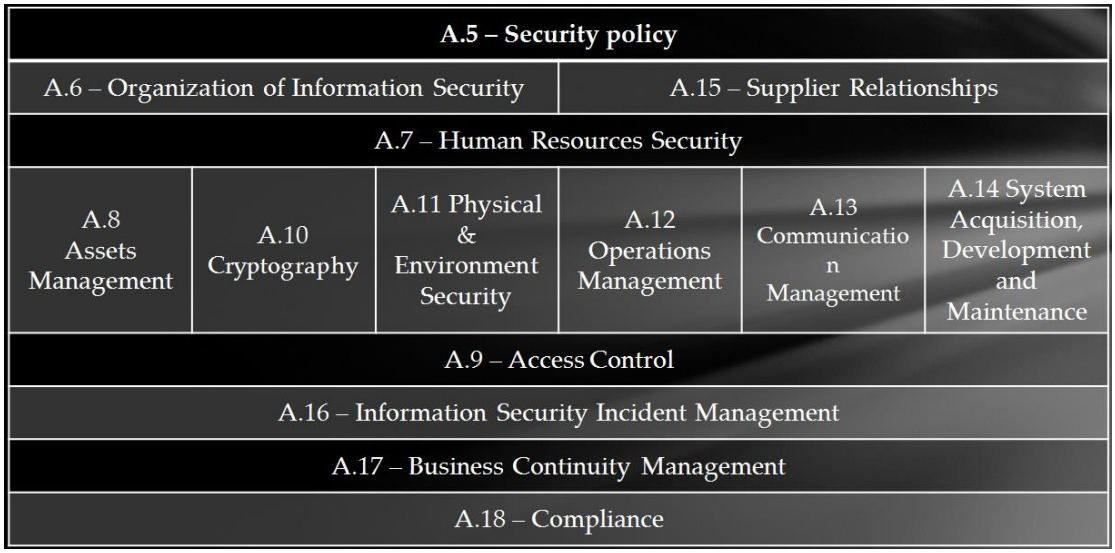
## 2.3 Σύγκριση ISO/IEC 27001:2005 & 27001:2013

Το ISO 27001:2013 σε σχέση με τον προκάτοχό του διαφοροποιείται σε αρκετά σημεία. Πρώτα απ' όλα, το βασικότερο είναι να γίνει κατανοητή η δομή του προτύπου όπως αυτό έχει διαμορφωθεί στη νέα του έκδοση. Αρχικά, στην επόμενη εικόνα φαίνεται τόσο η δομή του προτύπου στο κυρίως μέρος του καθώς και πώς διαμορφώνεται το μοντέλο PDCA.




Εικόνα 2 - Δομή του ISO

Επιπλέον, στη νέα έκδοση του προτύπου έχει διαφοροποιηθεί και το Annex A το οποίο περιέχει τα controls του ISO. Έχει αλλάξει τόσο η δομή του Annex καθώς επίσης έχει γίνει και η προσθήκη νέων control, τα οποία καλύπτουν επιπλέον περιοχές του ΣΔΑΠ.




Εικόνα 3 - Annex A, Controls of ISO 27001:2013

Για την καλύτερη δυνατή κατανόηση των αλλαγών, οι οποίες έχουν γίνει με την έκδοση του ISO/IEC 27001:2013 παρατίθενται ακολούθως πίνακες οι οποίοι περιγράφουν τις αλλαγές.

| **Main Body (Clauses) of ISO/ IEC 27001:2013** | |
|---|---|
| ***ISO/IEC 27001:2013*** | ***ISO/IEC 27001:2005*** |
| 0 Introduction | 0 Introduction |
| 1 Scope | 1 Scope |
| 2 Normative References | 2 Normative References |
| 3 Terms and Definition | 3 Terms and Definition |
| 4.1 Understanding the organization and its context | 8.3 Preventive Action |
| 4.2 Understanding the needs and expectations of interested parties | 5.2.1(c) Identify and address legal and regulatory requirements and contractual security obligations |
| 4.3 Determining the scope of the information security management system | 4.2.1(a) Define scope and boundaries<br>4.2.3(f) Ensure the scope remains adequate |
| 4.4 Information Security Management System | 4.1 General requirements |
| 5.1 Leadership and Commitment | 5.1 Management commitment |
| 5.2 Policy | 4.2.1(b) Define an ISMS Policy |
| 5.3 Organizational roles, responsibilities and authorities | 5.1(c) Establishing roles and responsibilities for information security |
| 6.1.1 actions to address risks and opportunities – general | 8.3 Preventive Action |

| | |
|---|---|
| 6.1.2 Information security risk assessment | 4.2.1(c) Define the risk assessment approach<br>4.2.1(d) Identify the risks<br>4.2.1(e) Analyze and evaluate the risks |
| 6.1.3 Information security risk treatment | 4.2.1(f) Identify and evaluate options for the treatment of risks<br>4.2.1(g) Select control objectives and controls for the treatment of risks<br>4.2.1(h) Obtain management approval of the proposed residual risks<br>4.2.1(j) Prepare a statement of Applicability<br>4.2.2(a) Formulate a risk treatment plan |
| 6.2 Information security objectives and planning to achieve them | 5.1(b) Ensuring that ISMS objectives and plans are established |
| 7.1 Resources | 4.2.2(g) Manage resources for the ISMS<br>5.2.1 Provision of resources |
| 7.2 Competence | 5.2.2 Training, awareness and competence |
| 7.3 Awareness | 4.2.2(e) Implement training and awareness programs<br>5.2.2 Training, awareness and competence |
| 7.4 Communication | 4.2.4(c) Communicate the actions and improvements<br>5.1(d) Communicating to the organization |
| 7.5 Documented Information | 4.3 Documentation requirements |
| 8.1 Operational planning and control | 4.2.2(f) Manage operations of the ISMS |
| 8.2 Information security risk assessment | 4.2.3(d) Review risk assessments at planned intervals |
| 8.3 Information security risk treatment | 4.2.2 b) Implement the risk treatment plan<br>4.2.2 c) Implement controls |
| 9.1 Monitoring, measurement, analysis and evaluation | 4.2.2(d) Define how to measure effectiveness<br>4.2.3(b) Undertake regular reviews of the effectiveness of the ISMS<br>4.2.3(c) Measure the effectiveness of controls |
| 9.2 Internal Audit | 4.2.3(e) Conduct internal ISMS audits<br>6 Internal ISMS audits |
| 9.3 Management review | 4.2.3(f) Undertake a management review of the ISMS<br>7 Management review of the ISMS |
| 10.1 Nonconformity and corrective action | 4.2.4 Maintain and improve the ISMS<br>8.2 Corrective action |
| 10.2 Continual improvement | 4.2.4 Maintain and improve the ISMS<br>8.1 Continual improvement |

**Πίνακας 1 - Mapping Clauses of ISO 27001**

| **Mapping ISO/IEC 27001:2013 Annex A Controls to ISO/IEC 27001:2005** | |
|---|---|
| **ISO 27001:2013 Annex A Controls** | **ISO 27001:2005 Annex A Controls** |
| **A.5 Information security policies** | **A.5 Security policy** |
| A.5.1.1 Policies for information security | A.5.1.1 Information security policy document |
| A.5.1.2 Review of policies for information security | A.5.1.2 Review of the information security policy |
| **A.6 Organization of information** | **A.6 Organization of information security** |
| A.6.1.1 Information security roles and responsibilities | A.6.1.3 Allocation of information security responsibilities |
| A.6.1.2 Segregation of duties | A.10.1.3 Segregation of duties |
| A.6.1.3 Contact with authorities | A.6.1.6 Contact with authorities |
| A.6.1.4 Contact with special interest groups | A.6.1.7 Contact with special interest groups |
| A.6.1.5 Information security in project management **(NEW)** | |
| A.6.2.1 Mobile device policy | A.11.7.1 Mobile computing and communications |
| A.6.2.2 Teleworking | A.11.7.2 Teleworking |
| **A.7 Human resource security** | **A.8 Human resource security** |
| A.7.1.1 Screening | A.8.1.2 Screening |
| A.7.1.2 Terms and conditions of employment | A.8.1.3 Terms and conditions of employment |
| A.7.2.1 Management responsibilities | A.8.2.1 Management responsibilities |
| A.7.2.2 Information security awareness, education and training | A.8.2.2 Information security awareness, education and training |
| A.7.2.3 Disciplinary process | A.8.2.3 Disciplinary process |
| A.7.3.1 Termination and change of employment responsibilities | A.8.3.1 Termination responsibilities |
| **A.8 Asset Management** | **A.7 Asset Management** |
| A.8.1.1 Inventory of assets | A.7.1.1 Inventory of assets |
| A.8.1.2 Ownership of assets | A.7.1.2 Ownership of assets |
| A.8.1.3 Acceptable use of assets | A.7.1.3 Acceptable use of assets |
| A.8.1.4 Return of assets | A.8.3.2 Return of assets |
| A.8.2.1 Classification of information | A.7.2.1 Classification guidelines |
| A.8.2.2 Labeling of information | A.7.2.2 Information labeling and handling |
| A.8.2.3 Handling of assets | A.10.7.3 Information handling procedures |
| A.8.3.1 Management of removable media | A.10.7.1 Management of removable media |
| A.8.3.2 Disposal of media | A.10.7.2 Disposal of media |
| A.8.3.3 Physical media transfer | A.10.8.3 Physical media in transit |
| **A.9 Access control** | **A.11 Access control** |
| A.9.1.1 Access control policy | A.11.1.1 Access control policy |
| A.9.1.2 Access to networks and network services | A.11.4.1 Policy on use of network services |
| A.9.2.1 User registration and de-registration | A.11.2.1 User registration |
| A.9.2.2 User access provisioning | A.11.5.2 User identification and |

| | |
|---|---|
| | authentication |
| A.9.2.3 Management of privileged access rights | A.11.2.2 Privilege management |
| A.9.2.4 Management of secret authentication information of users | A.11.2.3 User password management |
| A.9.2.5 Review of user access rights | A.11.2.4 Review of user access rights |
| A.9.2.6 Removal or adjustment of access rights | A.8.3.3 Removal of access rights |
| A.9.3.1 Use of secret authentication information | A.11.3.1 Password use |
| A.9.4.1 Information access restriction | A.11.6.1 Information access restriction |
| A.9.4.2 Secure log-on procedures | A.11.5.1 Secure logon procedures |
| A.9.4.3 Password management system | A.11.5.3 Password management system |
| A.9.4.4 Use of privileged utility programs | A.11.5.4 Use of system utilities |
| A.9.4.5 Access control to program source code | A.12.4.3 Access control to program source code |
| **A.10 Cryptography** | **A.12.3 Cryptographic controls** |
| A.10.1.1 Policy on the use of cryptographic controls | A.12.3.1 Policy on the use of cryptographic controls |
| A.10.1.2 Key management | A.10.1.2 Key management |
| **A.11 Physical and environmental security** | **A.9 Physical and environmental security** |
| A.11.1.1 Physical security perimeter | A.9.1.1 Physical security perimeter |
| A.11.1.2 Physical entry controls | A.9.1.2 Physical entry controls |
| A.11.1.3 Securing offices, rooms and facilities | A.9.1.3 Securing offices, rooms and facilities |
| A.11.1.4 Protecting against external and environmental threats | A.9.1.4 Protecting against external and environmental threats |
| A.11.1.5 Working in secure areas | A.9.1.5 Working in secure areas |
| A.11.1.6 Delivery and loading areas | A.9.1.6 Public access, delivery and loading areas |
| A.11.2.1 Equipment siting and protection | A.9.2.1 Equipment siting and protection |
| A.11.2.2 Supporting utilities | A.9.2.2 Supporting utilities |
| A.11.2.3 Cabling security | A.9.2.3 Cabling security |
| A.11.2.4 Equipment maintenance | A.9.2.4 Equipment maintenance |
| A.11.2.5 Removal of assets | A.9.2.7 Removal of property |
| A.11.2.6 Security of equipment and assets off-premises | A.9.2.5 Security of equipment off-premises |
| A.11.2.7 Secure disposal or re-use of equipment | A.9.2.6 Secure disposal and re-use of equipment |
| A.11.2.8 Unattended user equipment | A.11.3.2 Unattended user equipment |
| A.11.2.9 Clear desk and clear screen policy | A.11.3.3 Clear desk and clear screen policy |
| **A.12 Operations security** | **A.10 Communications and operations management** |
| A.12.1.1 Documented operating procedures | A.10.1.1 Documented operating procedures |

| | |
|---|---|
| A.12.1.2 Change management | A.10.1.2 Change management |
| A.12.1.3 Capacity management | A.10.3.1 Capacity Management |
| A.12.1.4 Separation of development, testing and operational environments | A.10.1.4 Separation of development, test and operational facilities |
| A.12.2.1 Controls against malware | A.10.4.1 Controls against malicious code |
| A.12.3.1 Information backup | A.10.5.1 Information backup |
| A.12.4.1 Event logging | A.10.10.1 Audit logging |
| A.12.4.2 Protection of log information | A.10.10.3 Protection of log information |
| A.12.4.3 Administrator and operator logs | A.10.10.4 Administrator and operator logs |
| A.12.4.4 Clock synchronization | A.10.10.6 Clock Synchronization |
| A.12.5.1 Installation of software on operational systems | A.12.4.1 Control of operational software |
| A.12.6.1 Management of technical vulnerabilities | A.12.6.1 Control of technical vulnerabilities |
| A.12.6.2 Restriction on software installation **(NEW)** | |
| A.12.7.1 Information systems audit controls | A.15.3.1 Information systems audit controls |
| **A.13 Communications security** | |
| A.13.1.1 Network controls | A.10.6.1 Network controls |
| A.13.1.2 Security of network services | A.10.6.2 Security of network services |
| A.13.1.3 Segregation in networks | A.11.4.5 Segregation in networks |
| A.13.2.1 Information transfer policies and procedures | A.10.8.1 Information exchange policies and procedures |
| A.13.2.2 Agreements on information transfer | A.10.8.2 Exchange Agreements |
| A.13.2.3 Electronic messaging | A.10.8.4 Electronic messaging |
| A.13.2.4 Confidentiality of non-disclosure agreements | A.6.1.5 Confidentiality agreements |
| **A.14 System acquisition, development and maintenance** | **A.12 Information systems acquisition, development and maintenance** |
| A.14.1.1 Information security requirements analysis and specification | A.12.1.1 Security requirements analysis and specification |
| A.14.1.2 Securing application services on public networks | A.10.9.1 Electronic commerce |
| A.14.1.3 Protecting application services transactions | A.10.9.2 On-line transactions |
| A.14.2.1 Secure development policy **(NEW)** | |
| A.14.2.2 System change control procedures | A.12.5.1 Change control procedures |
| A.14.2.3 Technical review of applications after operating platform changes | A.12.5.2 Technical review of applications after operating system changes |
| A.14.2.4 Restriction on changes to software packages | A.12.5.3 Restrictions on changes to software packages |
| A.14.2.5 Secure system engineering principles **(NEW)** | |

| | |
|---|---|
| A.14.2.6 Secure development environment **(NEW)** | |
| A.14.2.7 Outsourced development | A.12.5.5 Outsourced software development |
| A.14.2.8 System security testing **(NEW)** | |
| A.14.2.9 System acceptance testing | A.10.3.2 System Acceptance |
| A.14.3.1 Protection of test data | A.12.4.2 Protection of system test data |
| **A.15 Supplier relationships** | |
| A.15.1.1 Information security policy for supplier relationships **(NEW)** | |
| A.15.1.2 Addressing security within supplier agreements | A.6.2.3 Addressing security in third party agreements |
| A.15.1.3 Information and communication technology supply chain **(NEW)** | |
| A.15.2.1 Monitoring and review of supplier services | A.10.2.2 Monitoring and review of third party services |
| A.15.2.2 Managing changes to supplier services | A.10.2.3 Managing changes to third party services |
| **A.16 Information security incident management** | **A.13 Information security incident management** |
| A.16.1.1 Responsibilities and procedures | A.13.2.1 Responsibilities and procedures |
| A.16.1.2 Reporting information security events | A.13.1.1 Reporting information security events |
| A.16.1.3 Reporting information security weaknesses | A.13.1.2 Reporting information security weaknesses |
| A.16.1.4 Assessment of and decision on information security events **(NEW)** | |
| A.16.1.5 Response to information security incidents **(NEW)** | |
| A.16.1.6 Learning from information security incidents | A.13.2.2 Learning from information security incidents |
| A.16.1.7 Collection of evidence | A.13.2.3 Collection of evidence |
| **A.17 Information security aspects of business continuity management** | **A.14 Business continuity management** |
| A.17.1.1 Planning information security continuity | A.14.1.2 Business continuity and risk assessment |
| A.17.1 2 Implementing information security continuity | A.14.1.1 Including information security in the business continuity management process |
| A.17.1.3 Verify, review and evaluate information security continuity | A.14.1.5 Testing, maintaining and re-assessing business continuity plans |
| A.17.2.1 Availability of information processes facilities **(NEW)** | |
| **A.18 Compliance** | **A.15 Compliance** |
| A.18.1.1 Identification of applicable legislation and contractual requirements | A.15.1.1 Identification of applicable legislation |
| A.18.1.2 Intellectual property rights | A.15.1.2 Intellectual property rights |

| | |
|---|---|
| A.18.1.3 Protection of records | A.15.1.3 Protection of organizational records |
| A.18.1.4 Privacy and protection of personally identifiable information | A.15.1.4 Data protection and privacy of personal information |
| A.18.1.5 Regulation of cryptographic controls | A.15.1.6 Regulation of cryptographic controls |
| A.18.2.1 Independent review of information security | A.6.1.8 Independent review of information security |
| A.18.2.2 Compliance with security policies and standards | A.15.2.1 Compliance with security policies and standards |
| A.18.2.3 Technical compliance review | A.15.2.2 Technical compliance checking |

**Πίνακας 2 - Mapping Controls of ISO 27001**

| **Controls of ISO/IEC 27001:2005 No Longer Listed** | |
|---|---|
| A.6.1.1 Management commitment to information security | Covered by main requirements of standard – Leadership |
| A.6.1.2 Information security co-ordination | Covered by main requirements of standard |
| A.6.1.4 Authorization process for information processing facilities | Deleted |
| A.6.2.1 Identification of risks related to external parties | Covered by main requirements of standard – Risk Assessment |
| A.6.2.2 Addressing security when dealing with customers | Covered by main requirements of standard – Risk Assessment |
| A.8.1.1 Roles and responsibilities | Covered by main requirements of standard – (5.3) |
| A.10.2.1 Service delivery | Covered by other controls (A.15.2.1) |
| A.10.4.2 Controls against mobile code | Covered by other controls (A.12.2.1) |
| A.10.7.4 Security of system documentation | Covered by main requirements of standard - Risk Assessment |
| A.10.8.5 Business information systems | Deleted |
| A.10.9.3 Publicly available information | Covered by other controls (A.14.1.2) |
| A.10.10.2 Monitoring system use | Covered by other controls (A.12.4.1) |
| A.10.10.5 Fault logging | Covered by other controls (A.12.4.1) |
| A.11.4.2 User authentication for external connections | Covered by other controls (A.9.1.2, A.9.4.2) |
| A.11.4.3 Equipment identification in networks | subsumed into A.13.1 |
| A.11.4.4 Remote diagnostic and configuration port protection | subsumed into A.13.1 |
| A.11.4.6 Network connection control | subsumed into A.13.1 |
| A.11.4.7 Network routing control | subsumed into A.13.1 |
| A.11.5.5 Session time-out | subsumed into A.13.1 |
| A.11.5.6 Limitation of connection time | Covered by other controls (A.9.4.2) |
| A.11.6.2 Sensitive system isolation | subsumed into A.11.2.1 & A13.1.3 |
| A.12.2.1 Input data validation | subsumed into A.14.1.1 & A.14.2.5 |
| A.12.2.2 Control of internal processing | Covered by other controls (A.14.2.5) |
| A.12.2.3 Message integrity | subsumed into A.14.1.1 & A.14.2.5 |
| A.12.2.4 Output data validation | subsumed into A.14.1.1 & A.14.2.5 |
| A.12.5.4 Information leakage | subsumed into A 13.1 & A 13.2 |
| A.14.1.3 Developing and implementing continuity plans including information security | subsumed into A.17.1.2 |
| A.14.1.4 Business continuity planning framework | subsumed into A.17.1.2 |
| A.15.1.5 Prevention of misuse of information | Covered by main requirements of |

| | |
|---|---|
| processing facilities | standard - Risk Assessment |
| A.15.3.2 Protection of information systems audit tools | subsumed into 9.4 |

Πίνακας 3 - Controls of ISO 27001:2005 that no exist

| New Controls of Annex A in ISO 27001:2013 |
|---|
| A.6.1.5 Information security in project management |
| A.12.6.2 Restrictions on software installation |
| A.14.2.1 Secure development policy |
| A.14.2.5 Secure system engineering principles |
| A.14.2.6 Secure development environment |
| A.14.2.8 System security testing |
| A.15.1.1 Information security policy for supplier relationships |
| A.15.1.3 Information and communication technology supply chain |
| A.17.1.3 Verify, review and evaluate information security |
| A.17.2.1 Availability of information processing facilities |

Πίνακας 4 - New Controls in ISO 27001-2013

| New/updated Concept | Explanation |
|---|---|
| Context of the organization | The environment in which the organization operates |
| Issues, risks and opportunities | Replace preventive actions |
| Leadership | Requirements specific to top management |
| Communication | There are explicit requirements for both internal and external communications |
| Information security objectives | Information security objectives are now to be set at relevant functions and levels |
| Risk Assessment | Identification of assets, threats and vulnerabilities is no longer a prerequisite for the identification of information security risks |
| Risk owner | Replaces asset owner |
| Risk treatment plan | The effectiveness of the risk treatment plan is now regarded as being more important than the effectiveness of controls |
| Controls | Controls are now determined during the process of risk treatment, rather than being selected from Annex A |
| Documented Information | Replaces documents and records |
| Performance Evaluation | Covers the measurement of ISMS and risk treatment plan effectiveness |
| Continual Improvement | Methodologies other than (PDCA) may be used |

Εικόνα 4 - New Concept of ISO 27001:2013

Ένα πολύ σημαντικό μέρος κατά την προετοιμασία της πιστοποίησης για το ISO 27001:2013 είναι οι τεκμηριωμένες πληροφορίες (documented information) τις οποίες πρέπει να διατηρεί ο οργανισμός/εταιρία. Προκειμένου να προβεί στην πιστοποίηση κατά ISO 27001. Κάποιες από αυτές είναι απαραίτητες για την πιστοποίηση και παρατίθενται στον παρακάτω πίνακα.

| **Documented Information** |
|---|
| 4.3 Scope of the ISMS |
| 5.2 Information Security Policy |
| 6.1.2 Information security risk assessment process |
| 6.1.3 Information security risk treatment process |
| 6.1.3 d) Statement of Applicability |
| 6.2 Information security objectives |
| 7.2 d) Evidence of competence |
| 7.5.1 b) Documented information determined by the organization as being necessary for the effectiveness of the ISMS |
| 8.1 Operational planning and control |
| 9.2 g) Evidence of the audit program(s) and the audit results |
| 9.3 Evidence of the results of management reviews |
| 10.1 f) Evidence of the nature of the nonconformities and any subsequent actions taken |
| 10.1 g) Evidence of the results of any corrective action |
| A.14.2.1 Secure Development Policy |
| A.14.2.5 Secure Systems Engineering principles |
| A.15.1.1 Information Security Policy for Supplier Relationships |
| A.16.1.7 A procedure for evidence management |
| 8.2 Results of the information security risk assessments |
| 8.3 Results of the information security risk treatment |
| 9.1 Evidence of the monitoring and measurement results |

**Πίνακας 5 - Documented Information**

# Κεφάλαιο 3

## Ανάλυση Επικινδυνότητας

### 3.1 Γενικά Στοιχεία

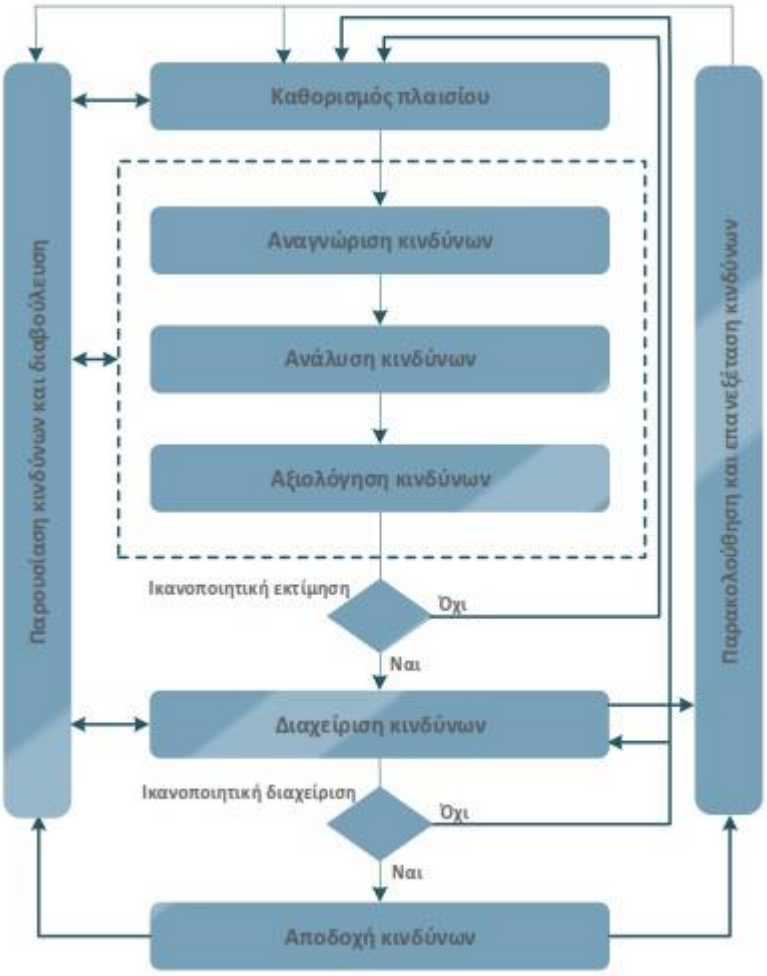
Η ενσωμάτωση αντιμέτρων ασφάλειας για ένα ΣΔΑΠ πολλές φορές καθίσταται δύσκολη υπόθεση ως προς την υλοποίηση αυτών. Οι δυσκολίες οι οποίες παρατηρούνται ως προς αυτή τη διαδικασία εστιάζονται σε διάφορα σημεία όπως, στην αδυναμία αιτιολόγησης του κόστους που αφορά τα μέτρα ασφαλείας ως προς τη διοίκηση. Αυτό είναι ένα σύνηθες φαινόμενο το οποίο παρατηρείται λόγω του ότι η διοίκηση της εκάστοτε εταιρείας δεν κατανοεί τους τεχνικούς όρους που χρησιμοποιεί το τεχνικό προσωπικό για να την πείσει ώστε να επενδύσει χρήματα στα μέτρα ασφαλείας του πληροφοριακού συστήματος. Επιπλέον, ένας ακόμα ανασταλτικός παράγοντας είναι η έλλειψη επαρκούς ενημέρωσης του προσωπικού αλλά και της διοίκησης σε θέματα ασφάλειας πληροφοριών.

Όπως γίνεται αντιληπτό, το πρόβλημα δεν είναι μόνο τεχνικό, δηλαδή αγορά εξοπλισμού (Hardware / Software) για την αντιμετώπιση των κινδύνων, αλλά και διοικητικό καθώς πέρα από τα τεχνικά θέματα πρέπει να εξασφαλιστεί και η συμμετοχή του ανθρώπινου παράγοντα στην προσπάθεια αυτή. Για να γίνει αυτό όμως χρειάζονται επιπλέον χρήματα για εκπαιδεύσεις του προσωπικού αλλά και για τη συνεχή ενημέρωση αυτού.

Επίσης, μία ακόμα σοβαρή δυσκολία είναι η σωστή αποτίμηση των αγαθών (assets) της εταιρίας. Είναι εύκολο να υπολογιστεί η αξία ενός αγαθού, το οποίο ανήκει στα Hardware συστήματα του ΣΔΑΠ καθώς έχει μια αγοραστική αξία και κατ' επέκταση έχει και αξία ως αγαθό, η οποία μεταφράζεται σε χρήματα. Το πρόβλημα έγκειται κυρίως σε αγαθά τα οποία είναι άυλα, δηλαδή πληροφορίες – δεδομένα. Σε αυτήν την περίπτωση η εκτίμηση της αξίας είναι σε κάθε περίπτωση υποκειμενική και αφορά ουσιαστικά την αξία που έχει μια πληροφορία για την εκάστοτε εταιρία.

Για την αντιμετώπιση των προαναφερθέντων έχουν δημιουργηθεί πολλές μέθοδοι ανάλυσης επικινδυνότητας, οι οποίες προσφέρουν συγκεκριμένη μεθοδολογία, (κάποιες απ' αυτές με τη συνοδεία βοηθητικού λογισμικού), για την αποτελεσματική ανάλυση της επικινδυνότητας σε πληροφοριακά συστήματα. Οι πιο γνώστες μέθοδοι ανάλυσης κινδύνου είναι, η CRAMM, η NIST 800, OCTAVE, SBA, EBIOS κ.ά.

Για την καλύτερη δυνατή κατανόηση του τρόπου λειτουργίας μιας τέτοιας μεθόδου αξίζει να γίνει αναφορά στη μέτρηση του κινδύνου. Ο κίνδυνος (D) μπορεί να εκφραστεί από το γινόμενο της πιθανότητας (P) να συμβεί ένα περιστατικό ασφάλειας, επί την επίπτωση (I) που θα έχει αυτό στην εταιρία, **D = P * I**.



[1]

**Εικόνα 5 - Μεθοδολογία διαχείρισης κινδύνων**

[1] Πηγή: Σημειώσεις μαθήματος «Διαχείριση Ασφάλειας», καθ. Κάτσικας Σωκράτης

## 3.2 CCTA Risk Analysis and Management Method (CRAMM)

Όπως έχει προαναφερθεί, η μέθοδος η οποία χρησιμοποιήθηκε για τις ανάγκες της εφαρμογής είναι η CRAMM. Η αιτία επιλογής της συγκεκριμένης μεθόδου προκύπτει από το ότι πρόκειται για μία μέθοδο η οποία έχει χαρακτηριστεί ως μια από τις πιο αποδοτικές μεθόδους για την ανάλυση επικινδυνότητας.

Η CRAMM αναπτύχθηκε από την Κεντρική Υπηρεσία Υπολογιστών και Τηλεπικοινωνιών (Central Computers and Telecommunications Agency – CCTA) της Βρετανικής κυβέρνησης. Η πρώτη έκδοση της CRAMM κυκλοφόρησε το 1985. Η τελευταία έκδοση (V5.0) κυκλοφόρησε το 2003. Κυκλοφόρησε επίσης μία έκδοση το 2009 (V5.2). Πρόκειται για ένα εμπορικό προϊόν.

Η CRAMM είναι παγκοσμίως αναγνωρισμένη καθώς έχει χρησιμοποιηθεί σε πάρα πολλές μελέτες και θεωρείται κατάλληλη για εταιρίες / οργανισμούς μεγάλου μεγέθους.

Η μέθοδος δομείται σε τρία στάδια προκειμένου να υλοποιηθεί η μελέτη επικινδυνότητας. Αρχικά γίνεται αναγνώριση και εκτίμηση αξίας των αγαθών (assets) της εταιρίας / οργανισμού. Στη δεύτερη φάση πραγματοποιείται εκτίμηση των απειλών (threats) και των ευπαθειών (vulnerabilities) που υπάρχουν στο ΣΔΑΠ και τέλος συντελείται η επιλογή των κατάλληλων αντιμέτρων (countermeasures) για την αντιμετώπιση των προαναφερθέντων.

Τα τρία προηγούμενα στάδια ακολουθούνται και κατά τη διαδικασία υπολογισμού κινδύνου στην εφαρμογή. Η εφαρμογή χρησιμοποιεί ένα μέρος των χαρακτηριστικών της CRAMM καθώς πρόκειται για εμπορικό προϊόν και δεν είναι πλήρως διαθέσιμη. Ωστόσο, μέσα από τον οδηγό χρήσης της CRAMM χρησιμοποιείται τόσο ο πίνακας υπολογισμού ρίσκου (risk matrix) όσο και ο κατάλογος απειλών και ευπαθειών, ο οποίος είναι διαθέσιμος. Παρόλα αυτά η CRAMM έχει ένα τεράστιο κατάλογο αντιμέτρων, πάνω από 3000, τα οποία όμως είναι διαθέσιμα μόνο μέσα από την εφαρμογή. Για το λόγο αυτό στην εφαρμογή χρησιμοποιήθηκε ο κατάλογος αντιμέτρων από το πρότυπο BSI Standard 100-3 “Risk Analysis Based on IT – Grundschutz”.

# Κεφάλαιο 4

## Ανάπτυξη Web Εφαρμογής

### 4.1 Σκοπός Εφαρμογής

Η διαδικασία πιστοποίησης κατά ISO 27001:2013 για έναν οργανισμό είναι μία αρκετά χρονοβόρα διαδικασία κατά την προετοιμασία καθώς επίσης απαιτεί αρκετή γραφειοκρατία. Η δημιουργία μίας εφαρμογής, η οποία λειτουργεί ως web application έχει ως στόχο να βοηθήσει στην προετοιμασία ενός οργανισμού για την πιστοποίηση, καθώς επίσης και να εμπλέξει και ένα μέρος του προσωπικού της εταιρίας με τη φιλοσοφία του ISO 27001:2013.

Αυτό μπορεί να συμβεί μέσα από την εφαρμογή, καθώς υπάρχει δυνατότητα σύνδεσης διάφορων χρηστών με διαφορετικό επίπεδο πρόσβασης (access level) ανάλογα με το ρόλο τον οποίο έχουν μέσα στον οργανισμό. Δηλαδή, ο κάθε υπεύθυνος ενός τμήματος μπορεί να συνδεθεί στην εφαρμογή και να καταχωρήσει τους πόρους (assets) του συστήματος καθώς επίσης και να προχωρήσει σε ανάλυση επικινδυνότητας ως προς τους πόρους τους οποίους διαχειρίζεται.

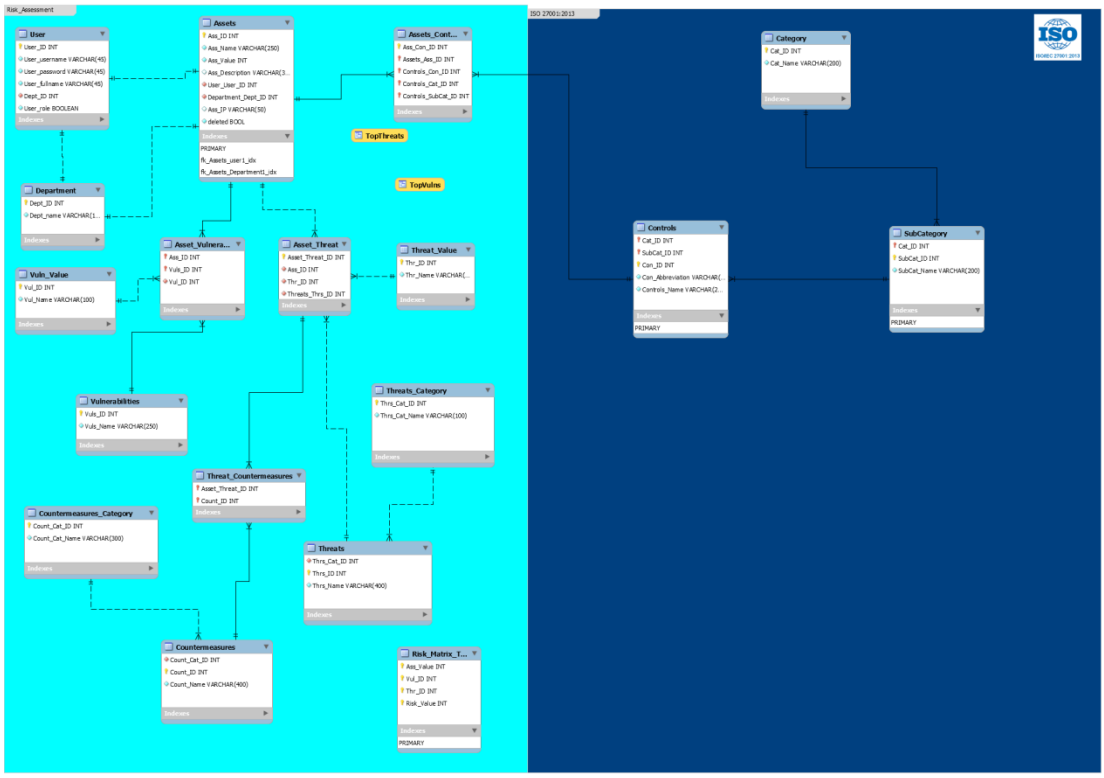
Όσον αφορά τον Information Security Officer παρέχει τη δυνατότητα της πλήρους ανασκόπησης του ΣΔΑΠ. Μπορεί να διαχειρίζεται τη βάση δεδομένων μέσα από το γραφικό περιβάλλον της εφαρμογής προσθέτοντας νέα threats, vulnerabilities, countermeasures καθώς επίσης και να παρακολουθεί τους πόρους του συστήματος, αλλά και να υλοποιεί την ανάλυση επικινδυνότητας. Του παρέχεται επίσης η δυνατότητα να έχει τη διαχείριση ενός directory, το οποίο περιέχει όλα τα απαιτούμενα έγγραφα για το ISO 27001:2013.

Βλέποντας την εφαρμογή σε ένα γενικότερο πλαίσιο, μπορούμε να πούμε πως αυτοματοποιεί τις περισσότερες από τις διαδικασίες του ISO και διευκολύνει κατά πολύ στην προετοιμασία αυτού. Παρακάτω θα γίνει λεπτομερής ανάλυση του τρόπου χρήσης της εφαρμογής.

### 4.2 Ανάπτυξη Εφαρμογής

Η εφαρμογή αναπτύχθηκε με τη γλώσσα προγραμματισμού C# σε framework .NET 4 με χρήση της αρχιτεκτονικής MVC (Model View Controller). Η επιλογή αυτή έγινε προκειμένου να υπάρχει η καλύτερη απόδοση συμπεριφοράς της εφαρμογής σε web περιβάλλον. Επίσης για τη διαχείριση και αποθήκευση των δεδομένων, τα οποία

διαχειρίζεται η εφαρμογή, αναπτύχθηκε Βάση Δεδομένων με χρήση της γλώσσας MySQL. Το διάγραμμα της Βάσης Δεδομένων φαίνεται στην παρακάτω εικόνα.




**Εικόνα 6 - EER Diagram**

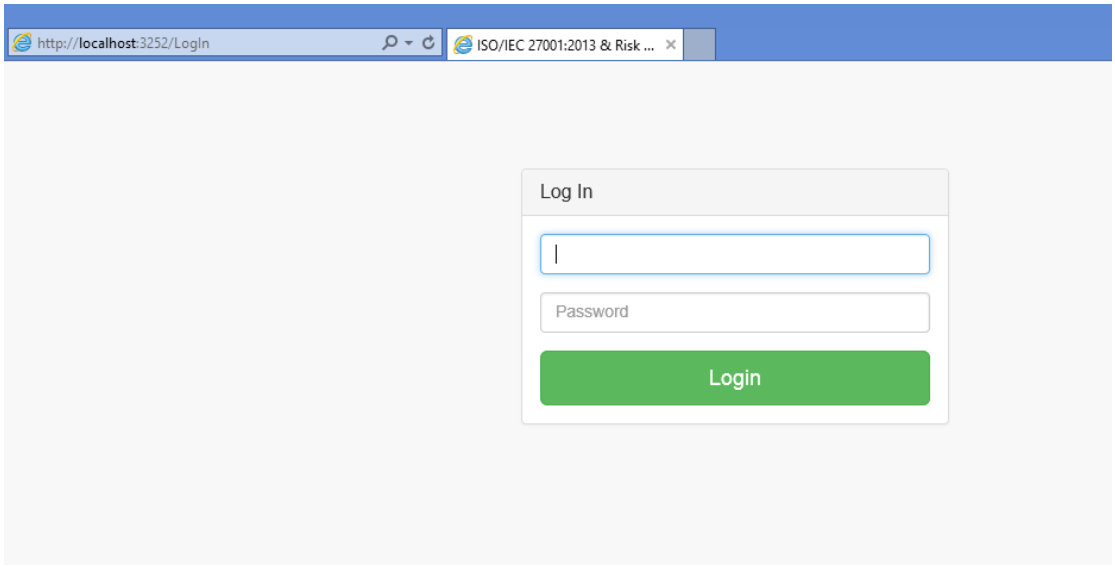
## 4.3 Οδηγός Χρήσης της Εφαρμογής

Η εφαρμογή, όπως έχει ήδη αναφερθεί, λειτουργεί με role based σύστημα σύνδεσης (login) των χρηστών σε αυτήν. Βάσει αυτού λοιπόν, ο κάθε χρήστης, ανάλογα το ρόλο τον οποίο έχει, του δίνονται και διαφορετικές δυνατότητες αξιοποίησης της εφαρμογής. Υπάρχουν δύο βασικοί ρόλοι για τους χρήστες: ο πρώτος είναι αυτός του administrator και ο δεύτερος αυτός του normal user.

Η βασικότερη διαφορά τους έγκειται στο ότι ο administrator έχει πλήρη πρόσβαση σε όλες τις δυνατότητες της εφαρμογής, σε αντίθεση με τον normal user, ο οποίος έχει πρόσβαση μόνο σε ορισμένα πεδία και κυρίως στη διαχείριση των assets, τα οποία ανήκουν στο τμήμα του. Στη συνέχεια θα γίνει αναλυτική παρουσίαση των δυνατοτήτων της εφαρμογής.

### 4.3.1 Login Page & Dashboard

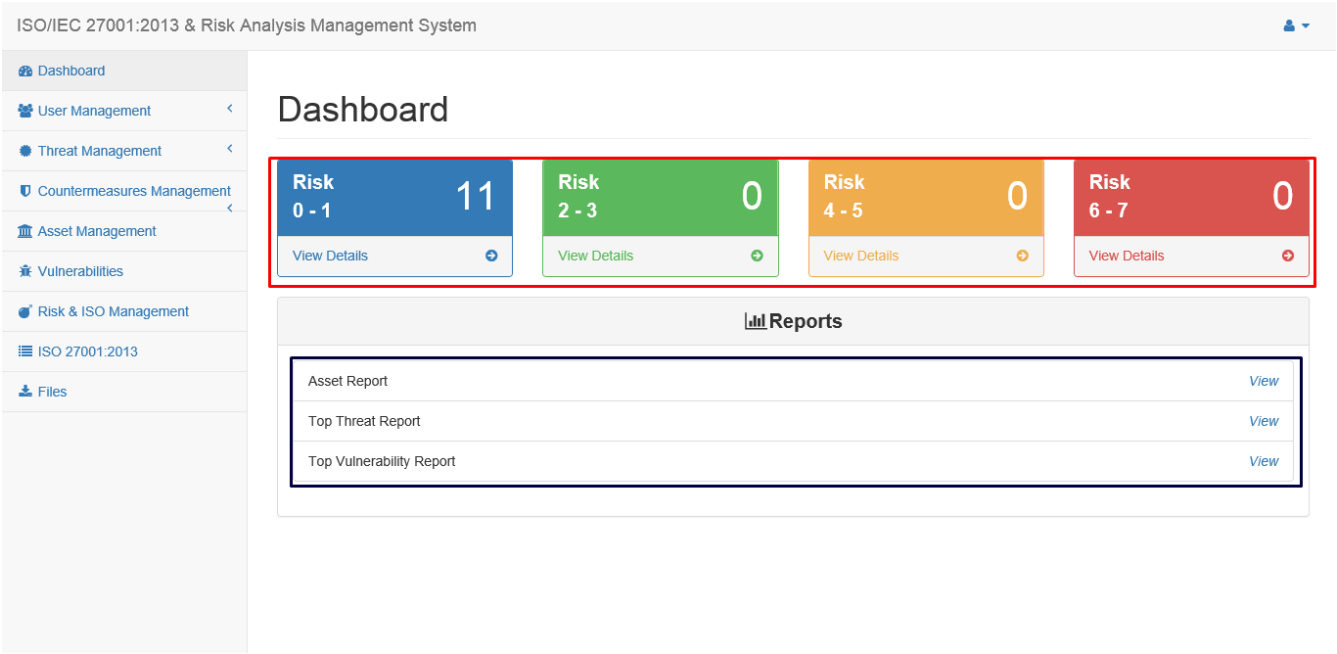
Αρχικά, ο χρήστης όταν πατήσει το URL της εφαρμογής παραπέμπεται στη login σελίδα, όπως φαίνεται παρακάτω.




Εικόνα 6 - Login Page

Ο χρήστης με τα credentials, τα οποία έχει λάβει από το Information Security Officer, μπορεί να συνδεθεί στην εφαρμογή. Αρχικά θα γίνει σύνδεση με δικαιώματα Διαχειριστή.

Η πρώτη εικόνα που βλέπει ο χρήστης είναι το Dashboard της εφαρμογής.

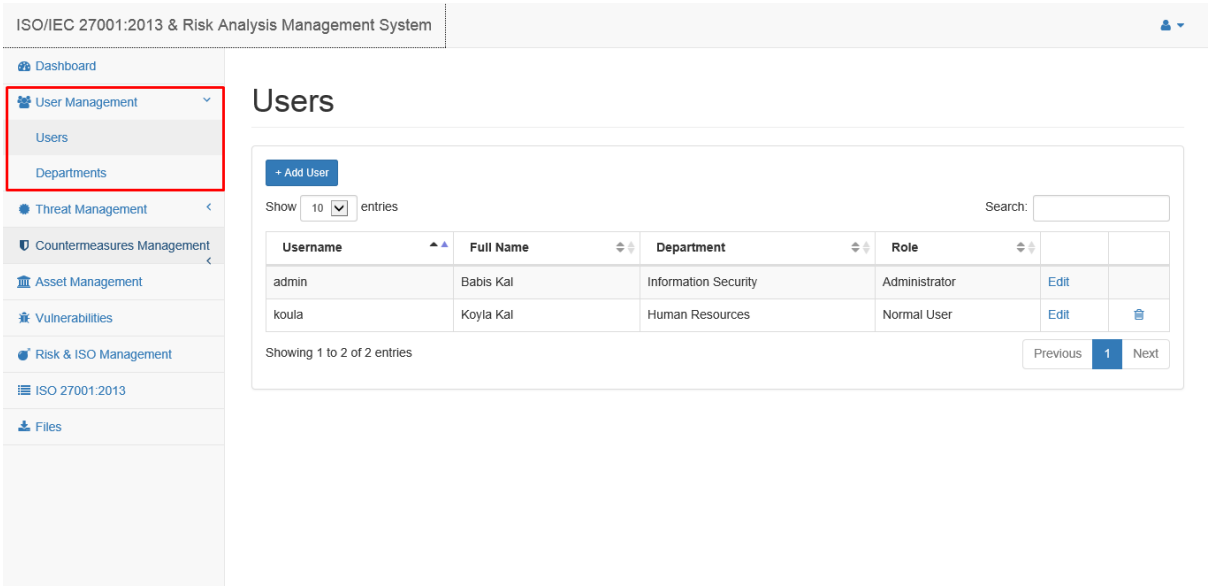



Εικόνα 7 - Dashboard

Στο κόκκινο πλαίσιο φαίνεται ότι ο χρήστης μπορεί να έχει μια πρώτη εικόνα για το πόσα asset έχουν το αντίστοιχο ρίσκο. Όπως φαίνεται υπάρχουν 11 assets τα οποία έχουν ρίσκο 0-1, δηλαδή μηδενικό. Ακολούθως στο μπλε πλαίσιο υπάρχει η δυνατότητα εξαγωγής report τα οποία θα αναλυθούν στη συνέχεια. Αριστερά υπάρχει το κεντρικό μενού.

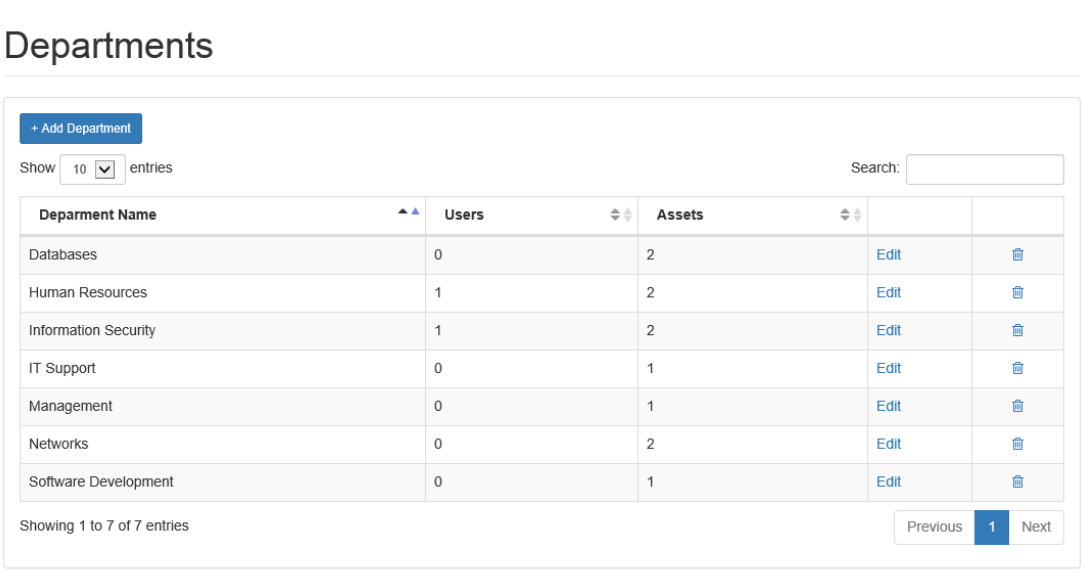
### 4.3.2 User Management

Το πρώτο μενού είναι το user management από το οποίο ο Administrator της εφαρμογής έχει τη δυνατότητα τόσο να δημιουργήσει ένα νέο χρήστη όσο και να επεξεργαστεί κάποιον ήδη υπάρχοντα.



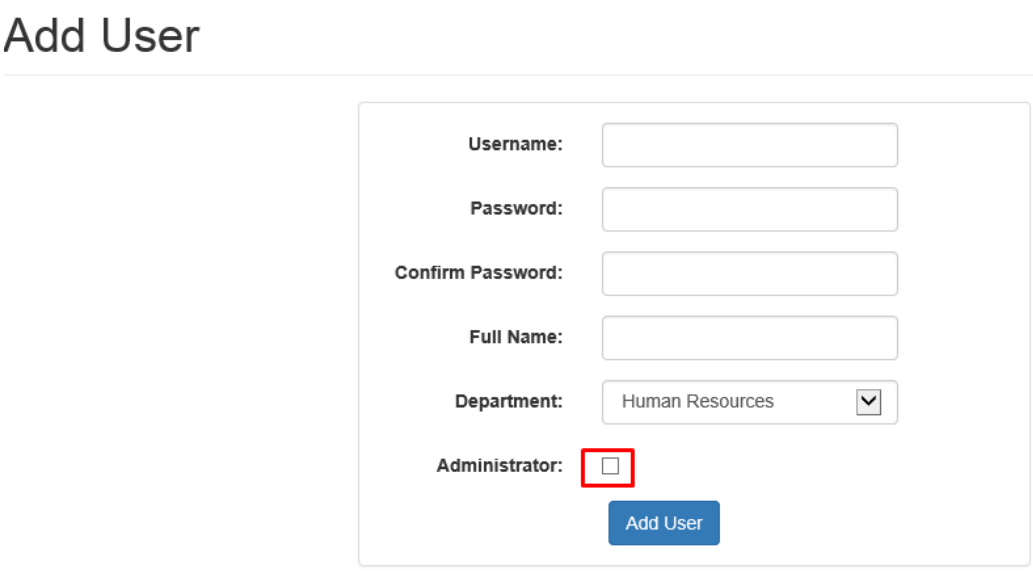

Εικόνα 8 – User Management

Επίσης στο User Management υπάρχει η δυνατότητα προσθήκης – επεξεργασίας των Departments του εκάστοτε οργανισμού.




Εικόνα 9 – Department Management

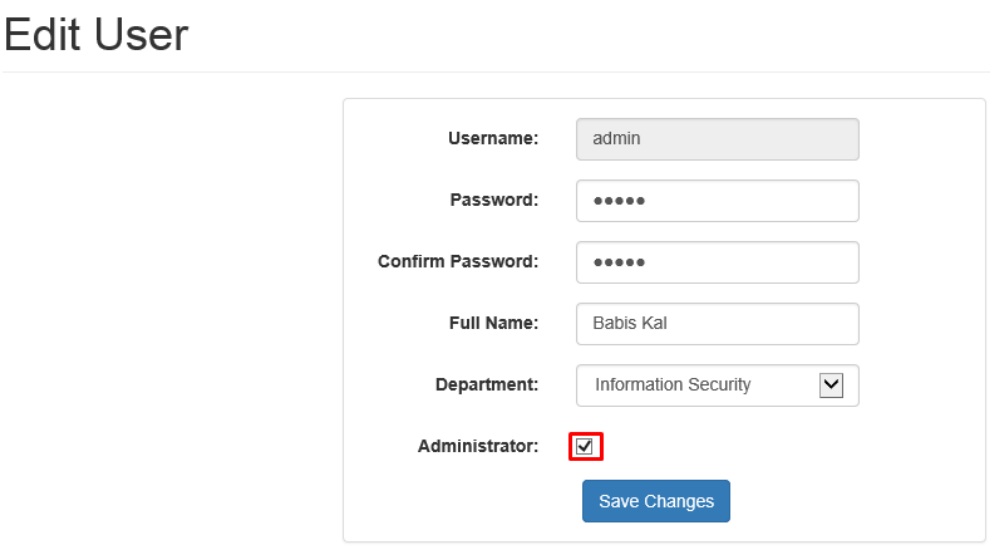
Όπως προαναφέρθηκε, ο Διαχειριστής έχει τη δυνατότητα να κάνει τόσο προσθήκη ενός χρήστη καθώς και να επεξεργαστεί κάποιον που υπάρχει ήδη.




Εικόνα 10 - Add User

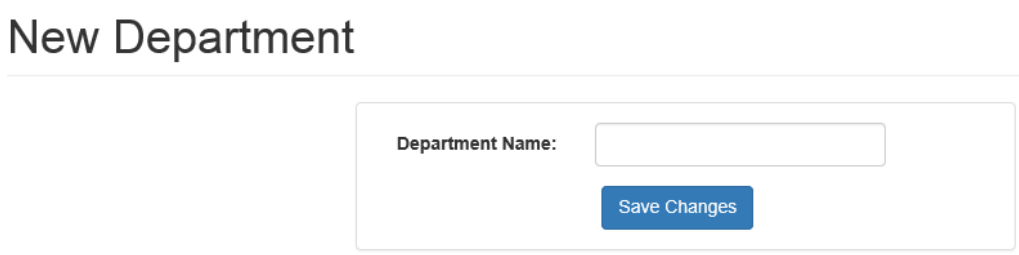
Όπως φαίνεται στην εικόνα παραπάνω, ο administrator έχει τη δυνατότητα να ορίσει το Username του χρήστη καθώς και το password αυτού. Επίσης πρέπει να δίνεται και το πλήρες όνομα του χρήστη καθώς και σε ποιο Department ανήκει. Τέλος, όπως φαίνεται στο κόκκινο πλαίσιο με το checkbox, μπορεί να ορίσει κάποιον χρήστη ως διαχειριστή ή απλό χρήστη.

Βέβαια υπάρχει η δυνατότητα αλλαγής δικαιωμάτων ενός χρήστη, όπως επίσης και όλων των στοιχείων του από το menu “edit”. Όπως διακρίνεται παρακάτω, ο διαχειριστής μπορεί να επέμβει σε οποιοδήποτε πεδίο πέραν του username, το οποίο μένει αμετάβλητο λόγω περιορισμών, οι οποίοι έχουν τεθεί στη Βάση Δεδομένων.

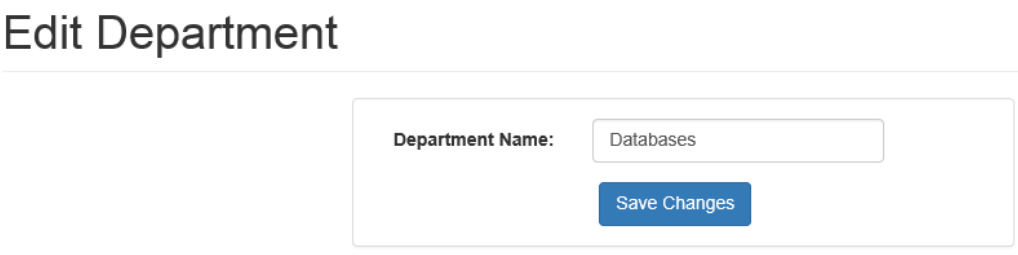



Εικόνα 11 – Edit User

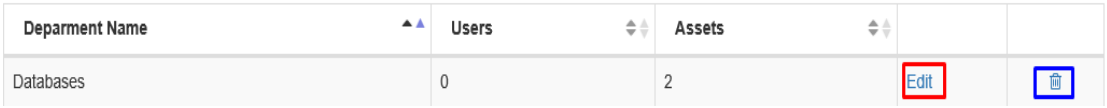
Όπως έχει ήδη σημειωθεί ο χρήστης έχει τη δυνατότητα μέσω του menu user management να διαχειριστεί και τα Departments του οργανισμού. Δίνεται λοιπόν η δυνατότητα τόσο της προσθήκης ενός νέου Department όσο και η δυνατότητα επεξεργασίας ή διαγραφής ενός ήδη υπάρχοντος.




Εικόνα 12 – Add Department



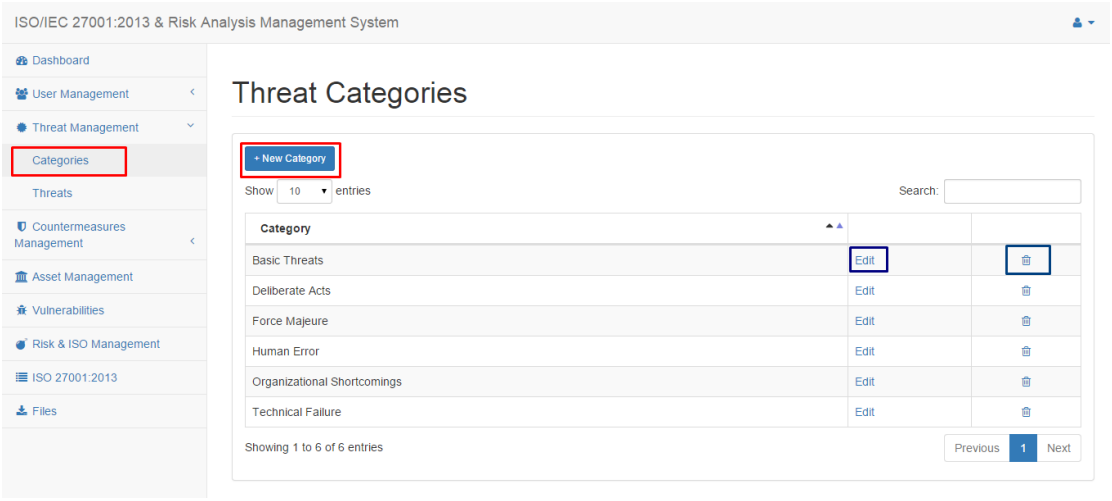

Εικόνα 13 – Edit Department



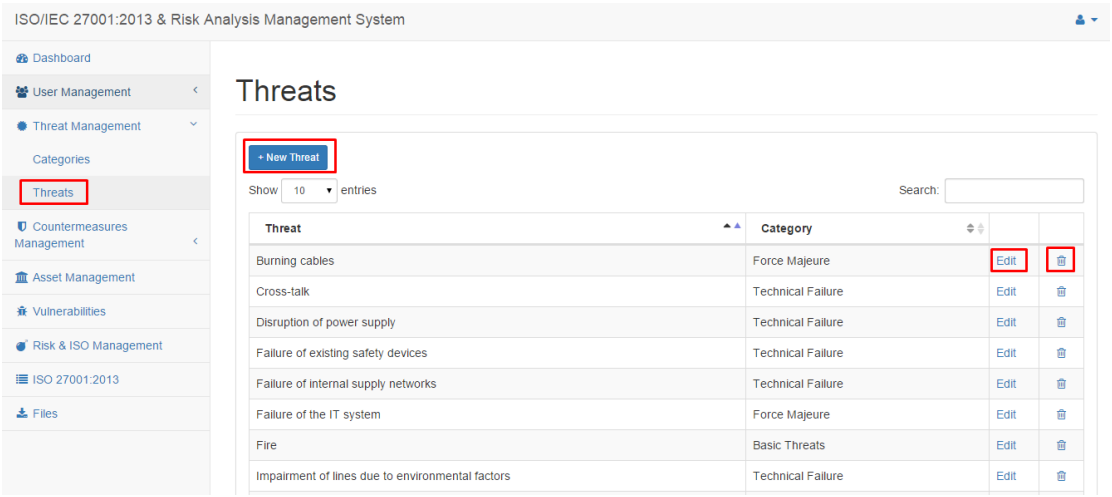

Εικόνα 14 – Delete Department

### 4.3.3 Threat Management

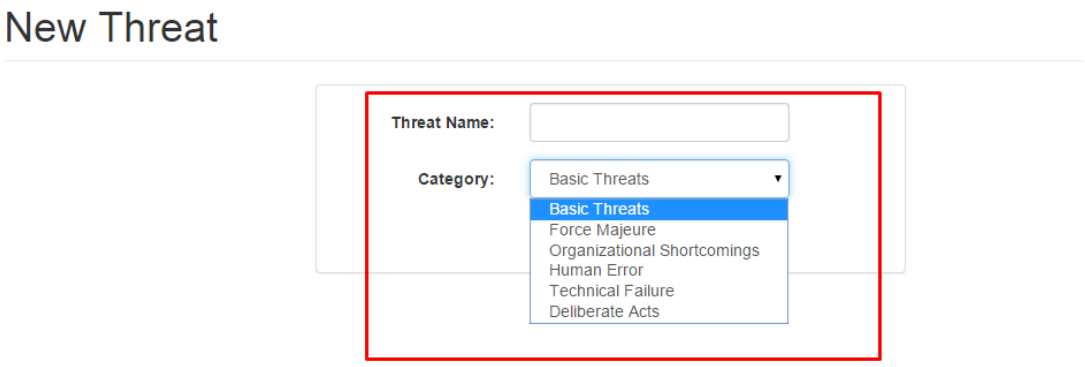
Στο αμέσως επόμενο menu υπάρχει η δυνατότητα διαχείρισης των **threats,** τα οποία υπάρχουν στη βάση δεδομένων της εφαρμογής. Η επιλογή των threats έχουν γίνει από το πρότυπο BSI καθώς επίσης και η κατηγοριοποίηση αυτών. Η δυνατότητα που δίνεται στο χρήστη είναι τόσο να επεξεργαστεί το όνομα ενός threat, αλλά και την κατηγοριοποίηση αυτού. Επίσης υπάρχει η δυνατότητα προσθήκης νέων threats στις ήδη υπάρχουσες κατηγορίες ή σε νέες, εάν προκύψει η ανάγκη ενός οργανισμού για αυτές, ή για τη διευκόλυνση των χρηστών.




Εικόνα 15 – Threat Category Management



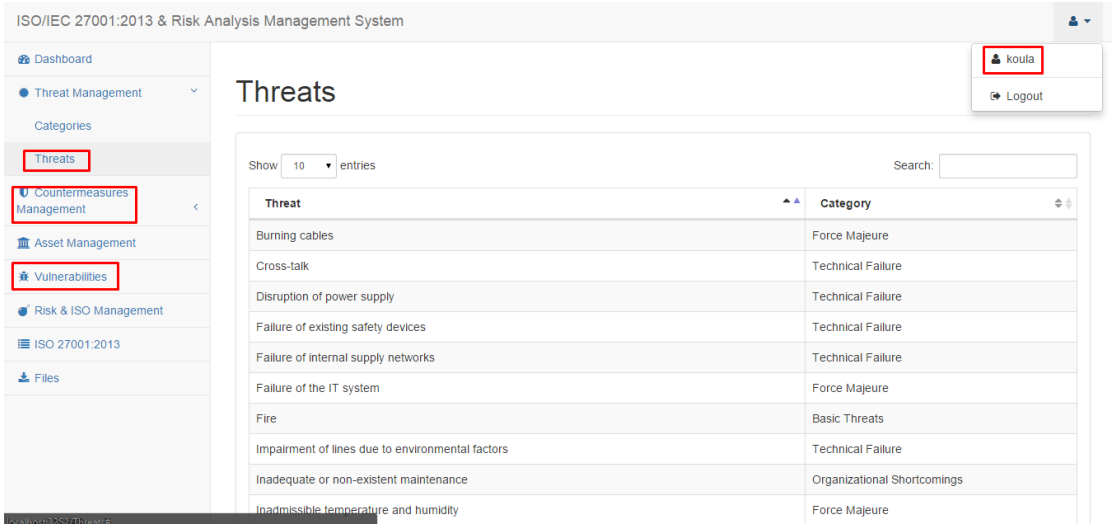

Εικόνα 16 – Threats Management




Εικόνα 17 – Εισαγωγή νέου threat

Όπως φαίνεται στο παραπάνω screenshot, ο χρήστης, κατά την εισαγωγή νέου threat, έχει τη δυνατότητα επιλογής ένταξης σε κατηγορία.

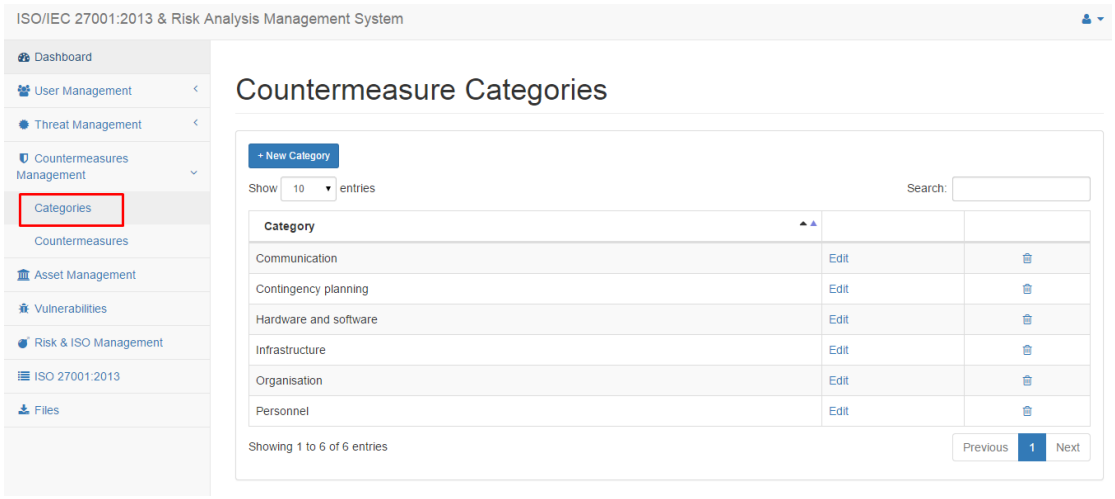
Σε αυτό το σημείο αξίζει να αναφερθεί πως δικαίωμα επεξεργασίας του συγκεκριμένου menu καθώς και των menu vulnerabilities και countermeasures έχει μόνο ο διαχειριστής. Ο απλός χρήστης έχει τη δυνατότητα προβολής. Χαρακτηριστικά παρατίθεται η παρακάτω εικόνα:



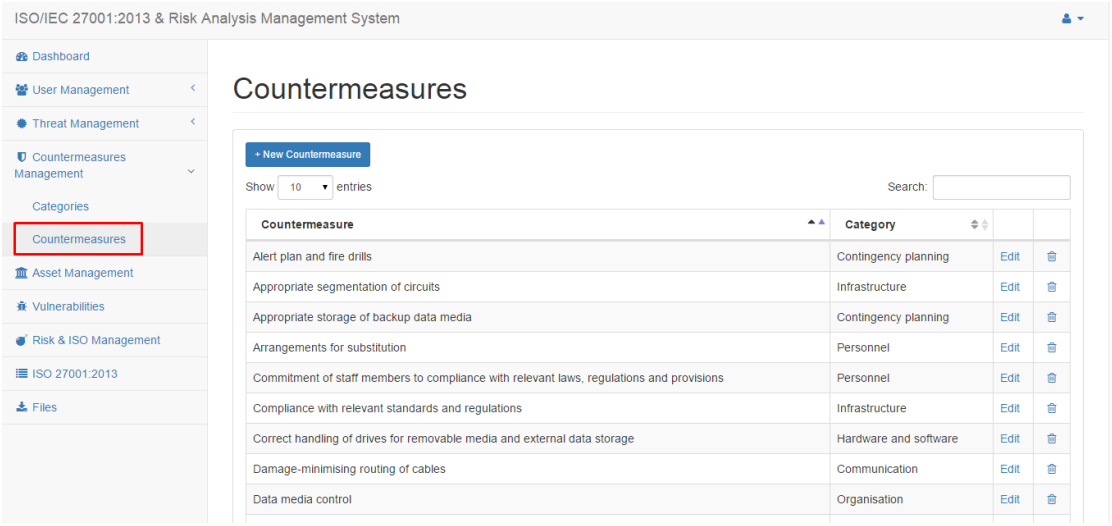

Εικόνα 18 – Normal User View

## 4.3.4 Vulnerabilities & Countermeasures Management

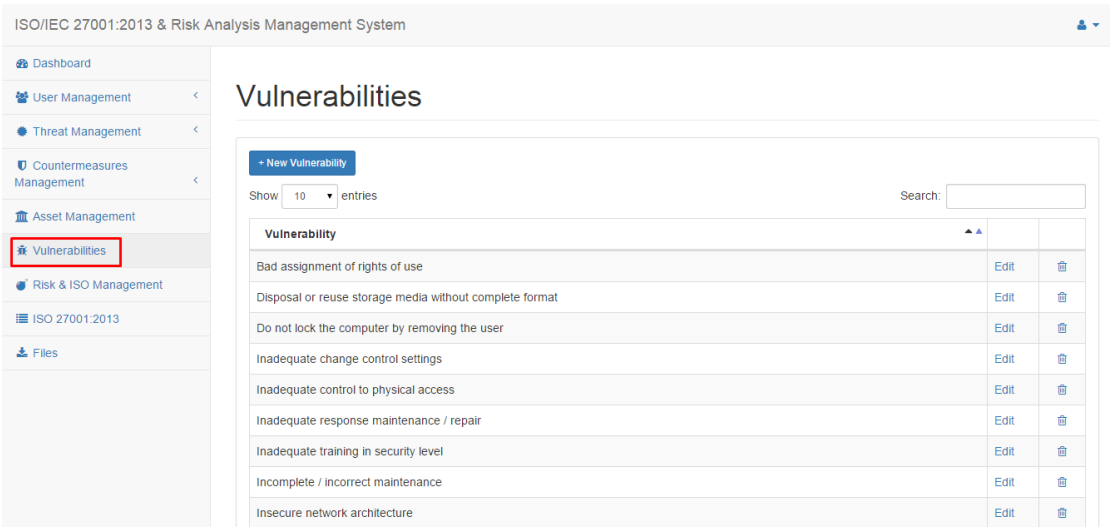
Κατ' αναλογία με το menu **Threats** λειτουργούν και τα menu **"Countermeasures Management"** και **"Vulnerabilities"**.




Εικόνα 19 – Countermeasures Categories Management




Εικόνα 20 – Countermeasures Management



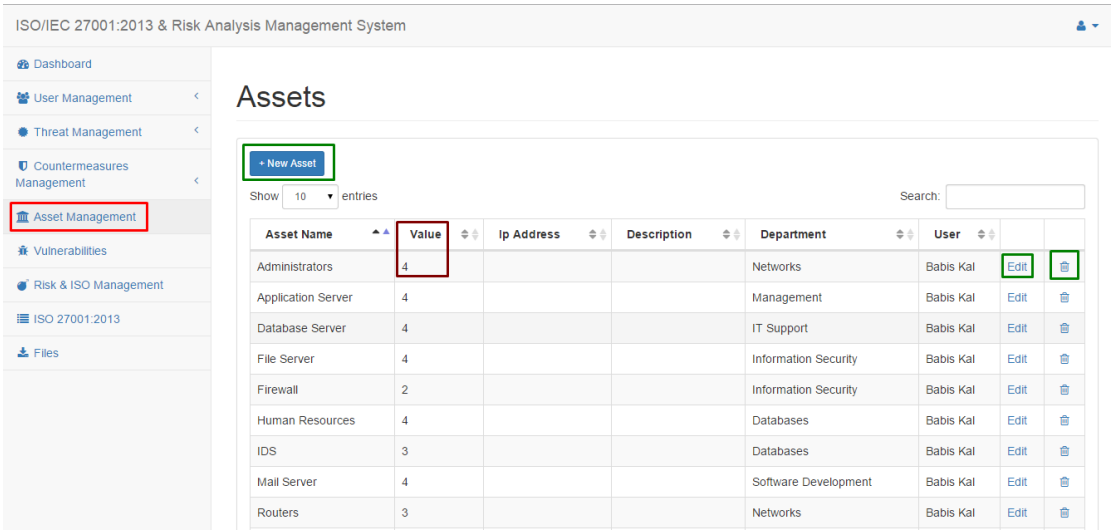

Εικόνα 21 – Vulnerabilities Management

Όσον αφορά τα vulnerabilities, πρέπει να σημειωθεί πως έχουν χρησιμοποιηθεί εκείνα τα οποία παρέχει η CRAMM καθώς δεν υπάρχει η κατηγοριοποίηση που υφίσταται στα threats και στα countermeasures.

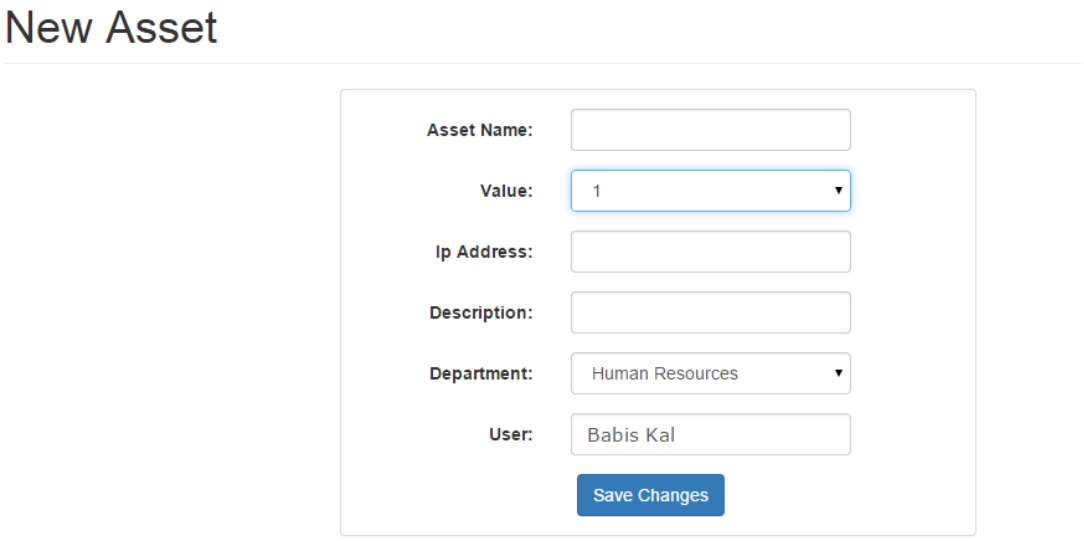
### 4.3.5 Asset Management

Στη συνέχεια, υπάρχει το menu "asset management", στο οποίο γίνεται η καταχώρηση των πόρων του συστήματος, καθώς επίσης και η ανάθεση κάποιων χαρακτηριστικών στους πόρους όπως η αξία τους, το τμήμα στο οποίο ανήκουν αλλά και ο χρήστης, ο οποίος είναι υπεύθυνος για τον κάθε πόρο και κατ' επέκταση και ο risk owner όπως ορίζει το ISO 27001:2013.

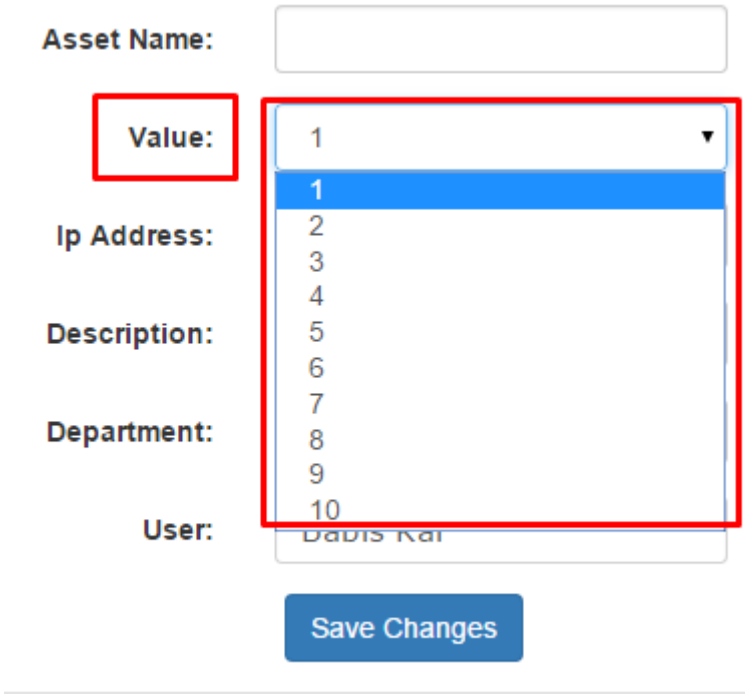
Η ανάθεση αξίας (value) στον κάθε πόρο (asset) είναι μία σημαντική διαδικασία η οποία γίνεται από τον Information Security Officer, αλλά και από κάποιον χρήστη, ο οποίος ανήκει στο Department, στο οποίο ανήκει το asset. Βέβαια, η ανάθεση της αξίας του πόρου γίνεται λαμβάνοντας υπόψη την αξία του πόρου είτε αυτή είναι οικονομική είτε είναι αξία πληροφοριών. Η αξία είναι υποκειμενική, καθώς καθορίζεται από πολλούς εξωγενείς και ενδογενείς παράγοντες. Η εφαρμογή δεν έχει σχεδιαστεί έτσι ώστε να λαμβάνει υπόψη την αξία του πόρου. Αυτό σημαίνει ότι πρέπει ο Information Security Officer να εκτιμήσει την αξία και βάσει αυτής της εκτίμησης να θέσει το κατάλληλο value στο asset προκειμένου να προχωρήσει η διαδικασία της ανάλυσης επικινδυνότητας.




**Εικόνα 22 – Asset Management**

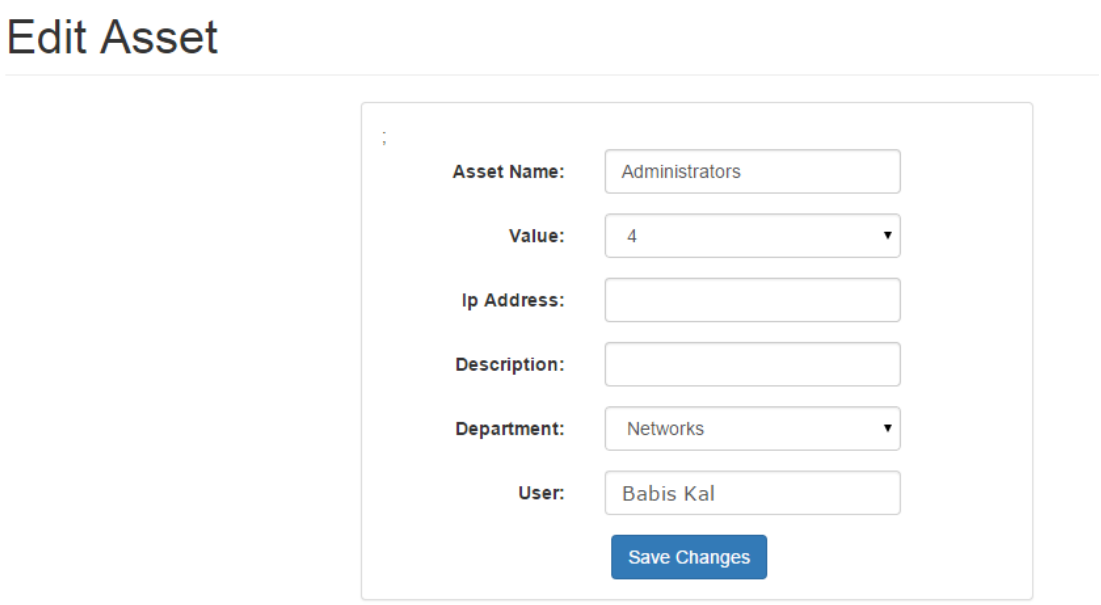



Εικόνα 23 – Εισαγωγή νέου Asset




Εικόνα 24 - Asset Value

Όπως φαίνεται στην εικόνα 24, το value ενός asset μπορεί να πάρει τιμές από 1 – 10. Αυτό συμβαίνει λόγω του ότι ακολουθείται η διαδικασία της CRAMM, όπως έχει ειπωθεί πρωτύτερα.

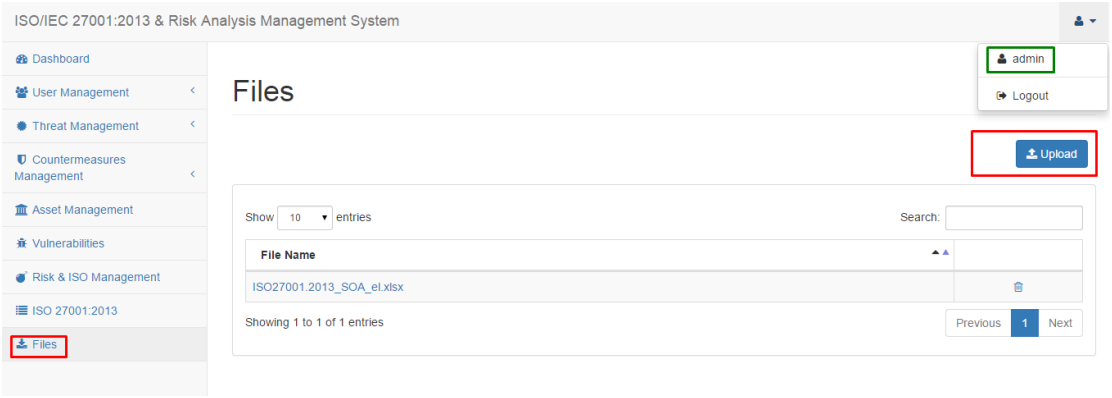



Εικόνα 25 – Edit Asset

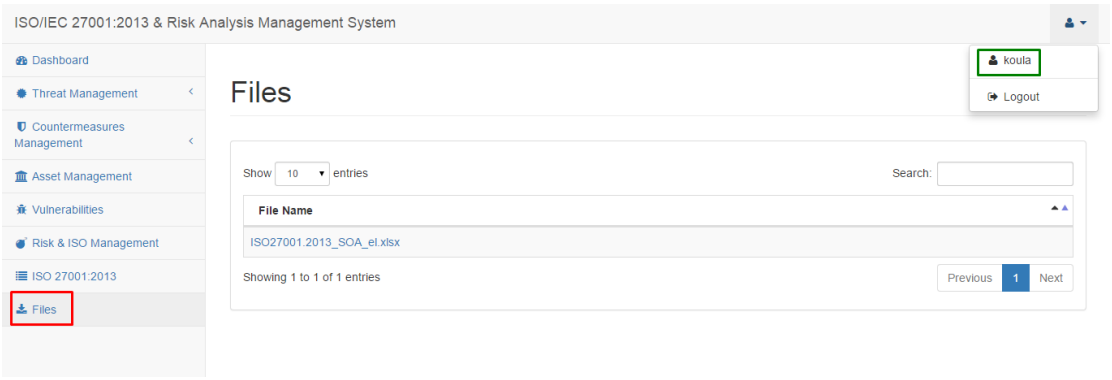
Όπως γίνεται κατανοητό, δίνεται η δυνατότητα για μια πλήρη καταγραφή των assets του πληροφοριακού συστήματος. Στο πεδίο **"Description"** ο χρήστης μπορεί να καταγράψει διάφορες παρατηρήσεις για το συγκεκριμένο πόρο. Μια απαραίτητη πληροφορία, η οποία χρειάζεται να καταγράφεται για την ανάλυση επικινδυνότητας έχει να κάνει με το, ποια είναι η αξία του asset που αφορά είτε αυτή είναι χρηματική είτε μεταφράζεται σε επιπτώσεις που αφορούν στη φήμη *(reputation)* του οργανισμού.

### 4.3.6 Files Menu & ISO 27001:2013

Άλλα δύο menu, τα οποία θα αναλυθούν πριν προχωρήσουμε στην ανάλυση επικινδυνότητας είναι το menu **"Files"** και το menu **"ISO 27001:2013".** Πρόκειται για δύο κατηγορίες της εφαρμογής, οι οποίες έχουν τόσο διαχειριστικό ρόλο όσο και ενημερωτικό. Στα **"Files"** ο administrator μπορεί να ανεβάσει *(upload)* και να κατεβάσει *(download)* αρχεία απαραίτητα για τις διαδικασίες του ISO 27001, αλλά και για την ανάλυση επικινδυνότητας. Ο απλός χρήστης έχει τη δυνατότητα μόνο να κατεβάσει αρχεία και όχι να ανεβάσει στο directory της εφαρμογής, για λόγους ασφαλείας και ακεραιότητας των διαχειρίσιμων από την εφαρμογή δεδομένων.

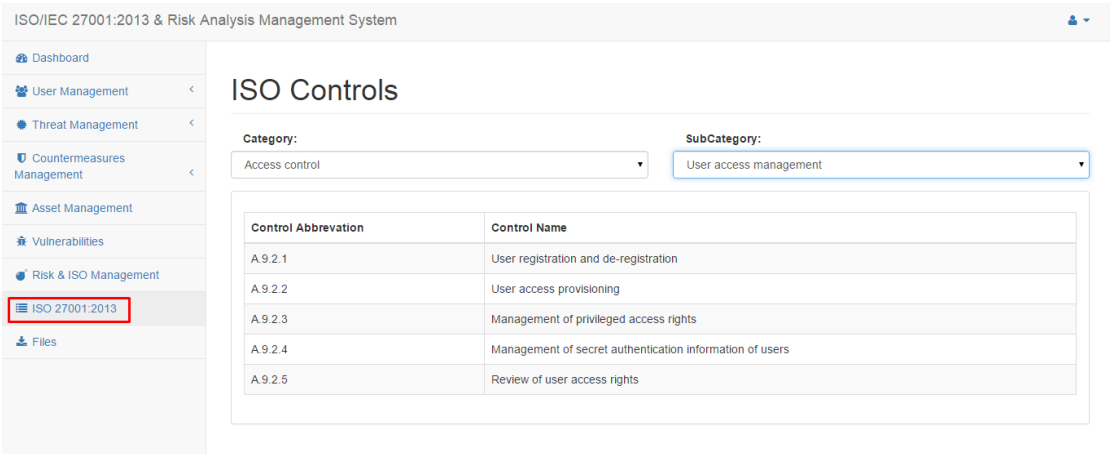



**Εικόνα 26 – Administrator view of "Files"**




**Εικόνα 27 – Normal User view of "Files"**

Το menu **"ISO 27001:2013"** διαδραματίζει ρόλο ενημέρωσης όλων των χρηστών της εφαρμογής. Παρέχεται η δυνατότητα στο χρήστη να δει όλη την πληροφορία, η οποία υπάρχει στο ANNEX A του προτύπου, στο οποίο συμπεριλαμβάνονται όλα τα controls του ISO 27001. Στο συγκεκριμένο σημείο της εφαρμογής τόσο ο administrator όσο και ο normal user έχουν τα ίδια δικαιώματα.



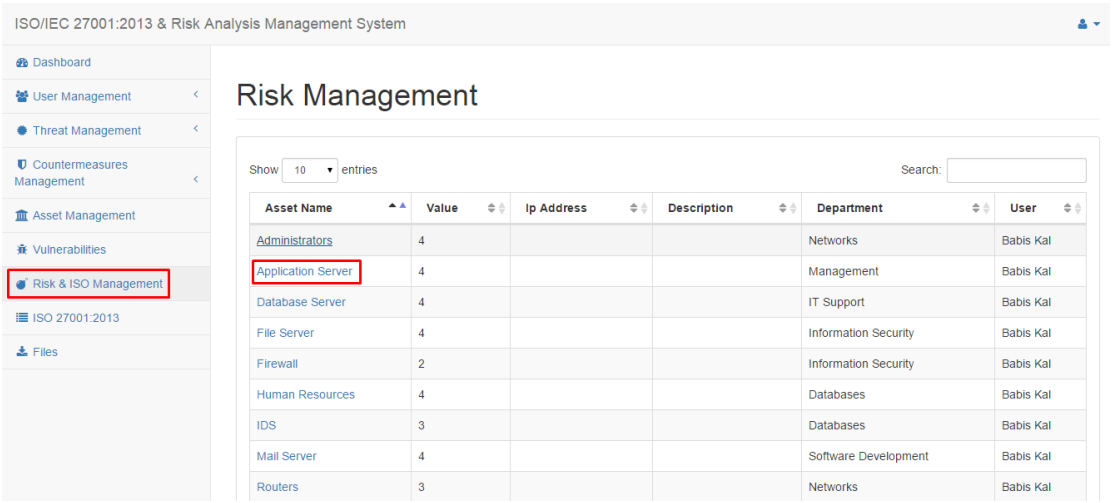

**Εικόνα 28 – ISO 27001:2013**

### 4.3.7 Risk & ISO Management

Τελευταίο menu, το οποίο θα αναλυθεί, είναι το **"Risk & ISO Management".** Πρόκειται για τη δυνατότητα της εφαρμογής να πραγματοποιεί αυτοματοποιημένους υπολογισμούς ανάλυσης ρίσκου για κάθε asset ξεχωριστά, αλλά και να συνδυάζει το ISO 27001 στο σημείο της πρόληψης των απειλών και των ευπαθειών που αντιμετωπίζει ένα asset.

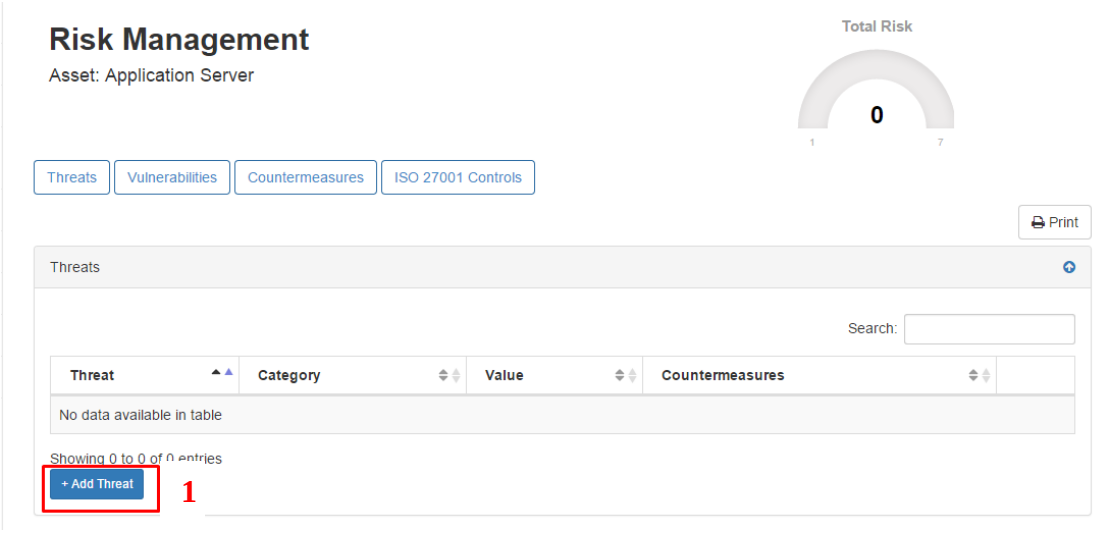
Αξιοσημείωτο είναι πως ο normal user έχει πρόσβαση μόνο σε assets τα οποία ανήκουν στο τμήμα στο οποίο ανήκει και αυτός, σε αντίθεση με τον administrator που έχει πρόσβαση σε όλα.

Σε πρώτο στάδιο ο χρήστης πρέπει να επιλέξει ένα asset από τα διαθέσιμα.

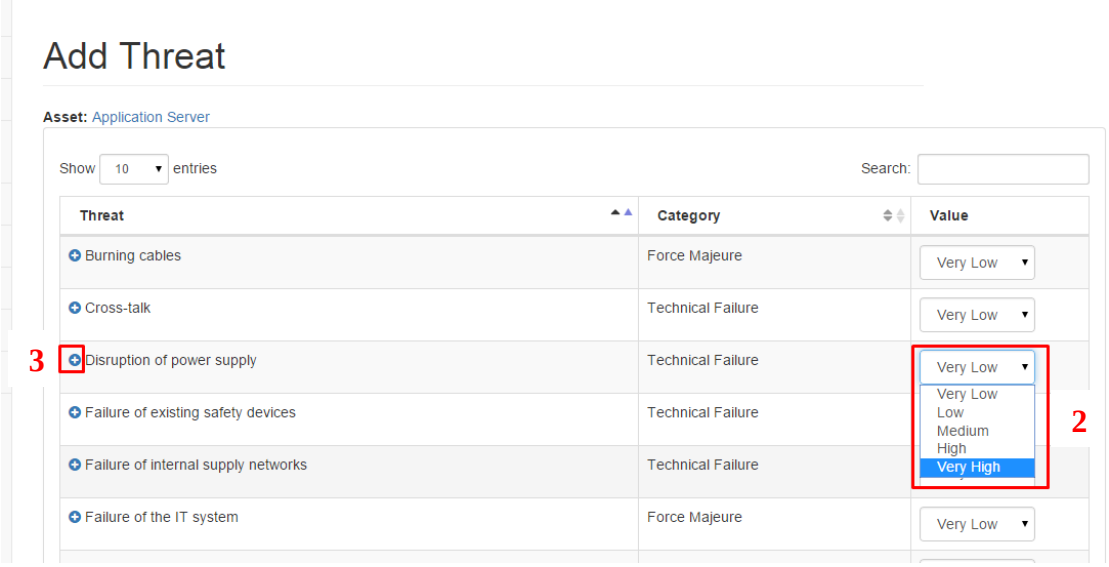



**Εικόνα 29 – Risk Management**

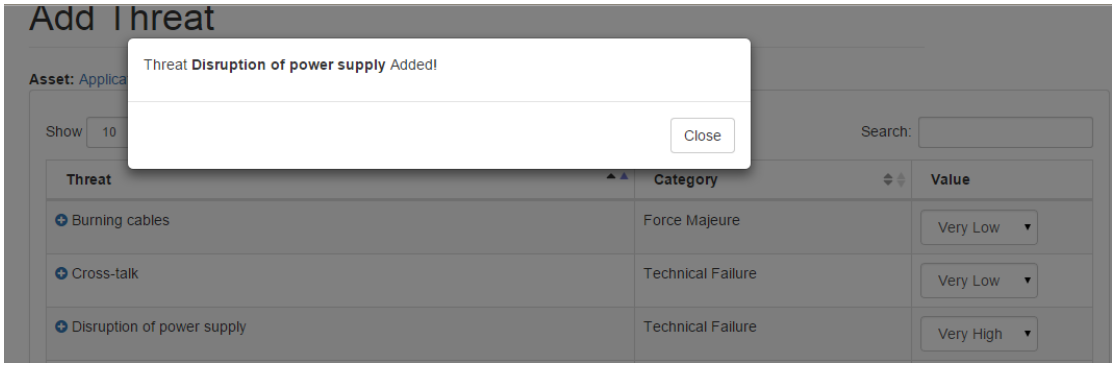
Έχοντας διαλέξει το asset "Application Server" ο χρήστης καλείται να αντιστοιχίσει τα threats και τα vulnerabilities, τα οποία έχουν εντοπιστεί για τον συγκεκριμένο πόρο, προκειμένου να υπολογιστεί από την εφαρμογή το ρίσκο.




Εικόνα 30 – Add Threat (1)

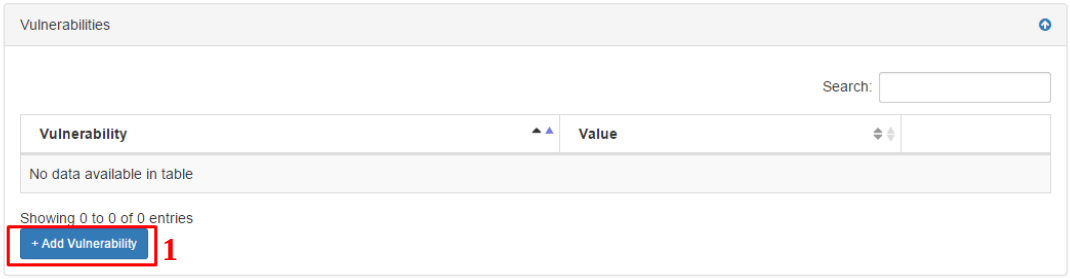



Εικόνα 31 – Add Threat (2)

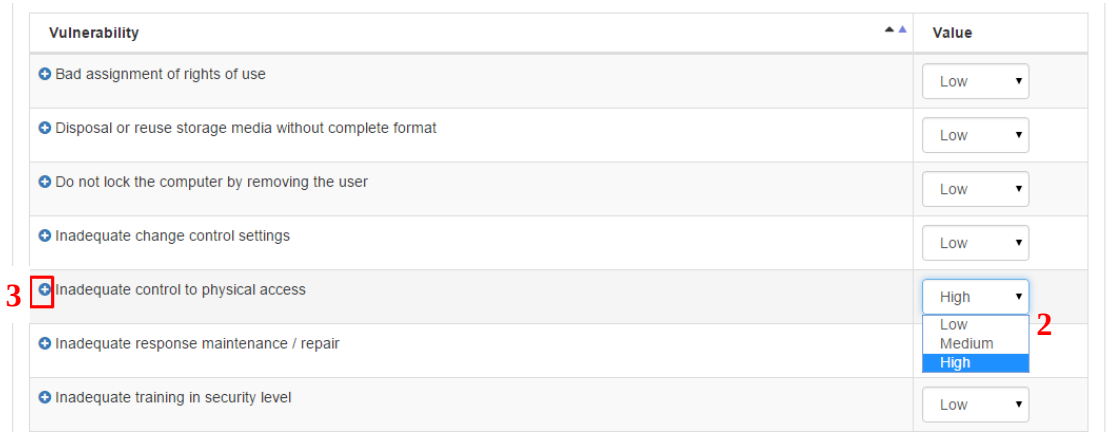



Εικόνα 32 – Add Threat (3)

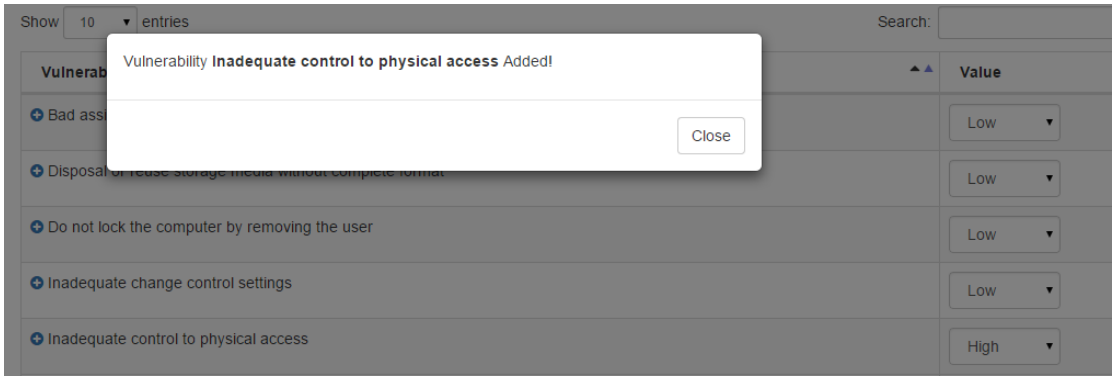
Κατά την εισαγωγή των threats ο χρήστης καλείται να δώσει μία τιμή στο value του threat σύμφωνα με τον πίνακα υπολογισμού ρίσκου της CRAMM. Στη συνέχεια αντιστοιχίζονται τα vulnerabilities.




**Εικόνα 33 – Add Vulnerability (1)**

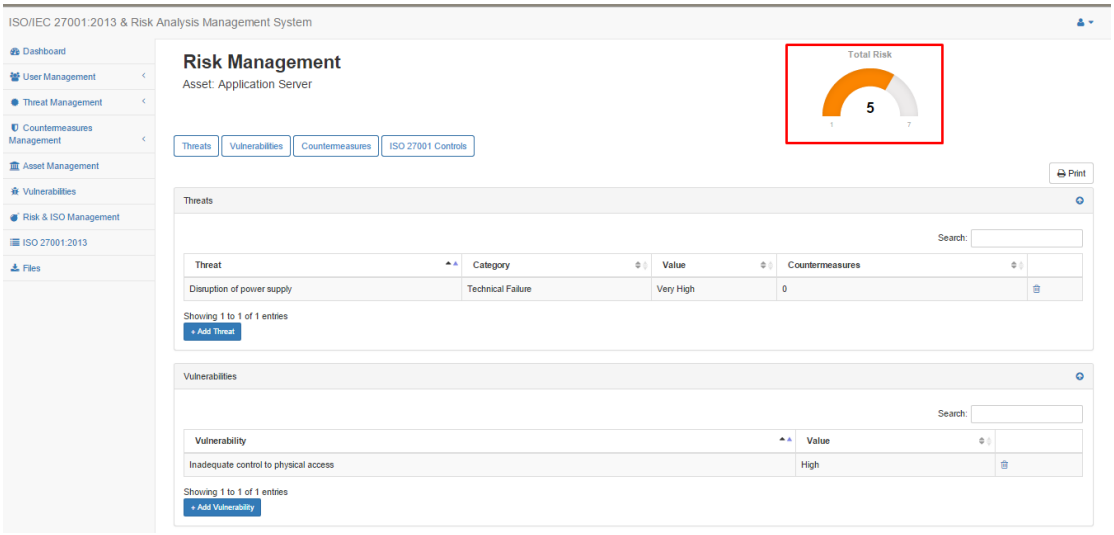



**Εικόνα 34 – Add Vulnerability (2)**




**Εικόνα 35 – Add Vulnerability (3)**

Αφού προστεθεί και το vulnerability η εφαρμογή υπολογίζει το ρίσκο όπως αυτό προκύπτει μέσω της CRAMM.




Εικόνα 36 – Risk Matrix

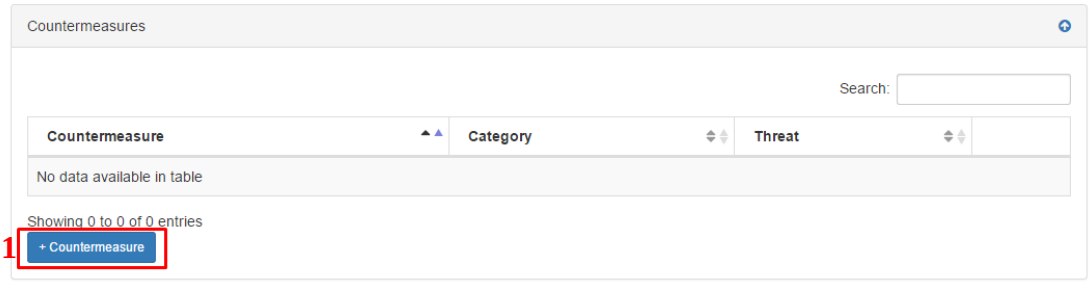
Το ρίσκο στο παραπάνω παράδειγμα προκύπτει και από τον πίνακα της CRAMM, όπως φαίνεται στην επόμενη εικόνα.

| Threat | Very Low | Very Low | Very Low | Low | Low | Low | Medium | Medium | Medium | High | High | High | Very High | Very High | Very High |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Vuln. / Asset Value | LOW | MEDIUM | HIGH | LOW | MEDIUM | HIGH | LOW | MEDIUM | HIGH | LOW | MEDIUM | HIGH | LOW | MEDIUM | HIGH |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 1 | 2 | 2 | 2 | 2 | 3 |
| 2 | 1 | 1 | 2 | 1 | 2 | 2 | 2 | 2 | 3 | 2 | 3 | 3 | 3 | 3 | 4 |
| 3 | 1 | 2 | 2 | 2 | 2 | 3 | 2 | 3 | 3 | 3 | 3 | 4 | 3 | 4 | 4 |
| 4 | 2 | 2 | 3 | 2 | 3 | 3 | 3 | 3 | 4 | 3 | 4 | 4 | 4 | 4 | 5 |
| 5 | 2 | 3 | 3 | 3 | 3 | 4 | 3 | 4 | 4 | 4 | 4 | 5 | 4 | 5 | 5 |
| 6 | 3 | 3 | 4 | 3 | 4 | 4 | 4 | 4 | 5 | 4 | 5 | 5 | 5 | 5 | 6 |
| 7 | 3 | 4 | 4 | 4 | 4 | 5 | 4 | 5 | 5 | 5 | 5 | 6 | 5 | 6 | 6 |
| 8 | 4 | 4 | 5 | 4 | 5 | 5 | 5 | 5 | 6 | 5 | 6 | 6 | 6 | 6 | 7 |
| 9 | 4 | 5 | 5 | 5 | 5 | 6 | 5 | 6 | 6 | 6 | 6 | 7 | 7 | 7 | 7 |
| 10 | 5 | 5 | 6 | 5 | 6 | 6 | 6 | 6 | 6 | 6 | 7 | 7 | 7 | 7 | 7 |

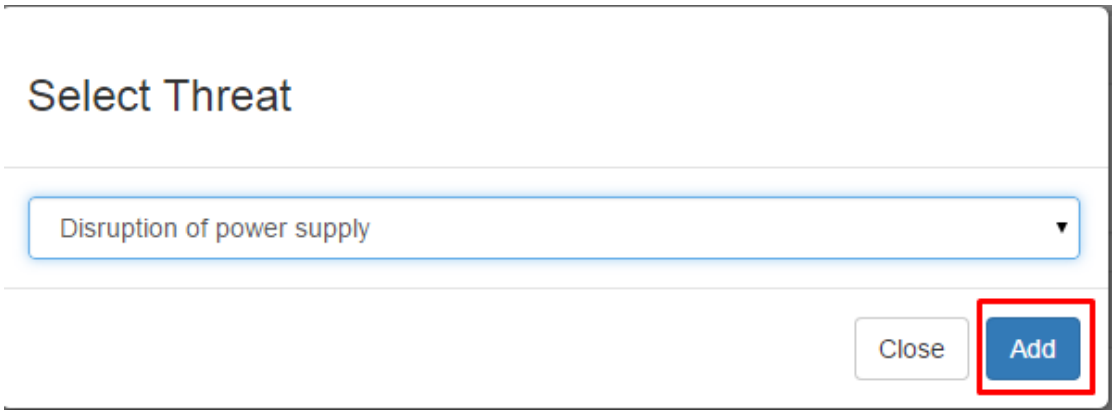
1 2 3 4

Εικόνα 37 – CRAMM Risk Matrix Table

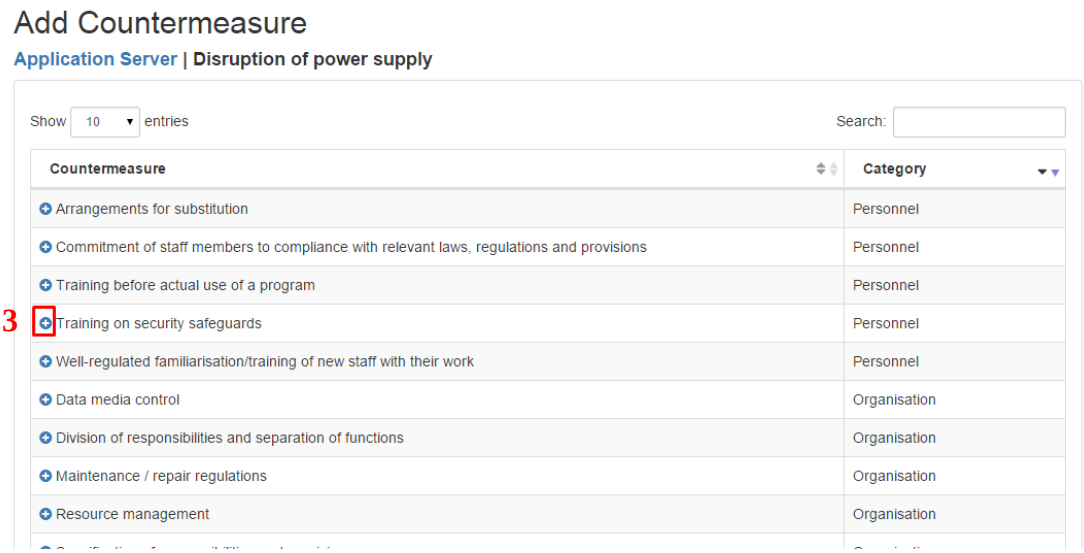
Αφού γίνει ο υπολογισμός του ρίσκου, ο administrator έχει τη δυνατότητα να προσθέσει στο asset τόσο countermeasures, τα οποία αφορούν ένα συγκεκριμένο asset, όσο και controls του ISO 27001.



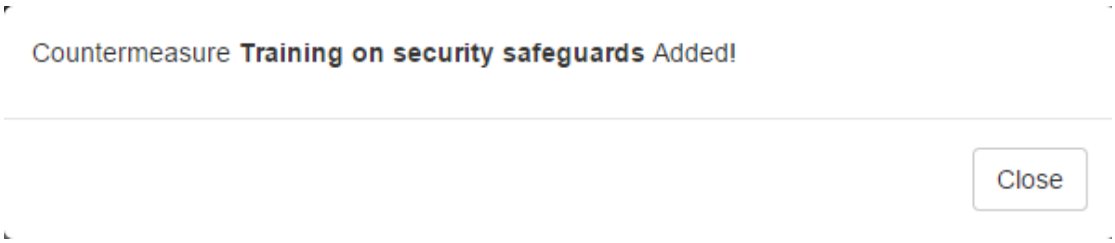

Εικόνα 38 – Εισαγωγή Countermeasures (1)



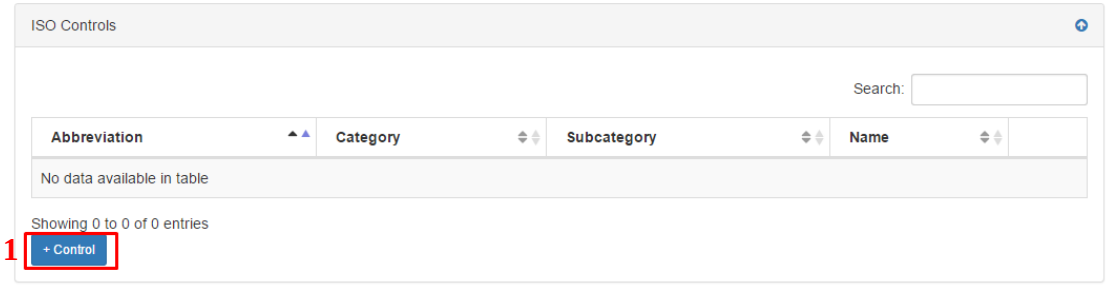

Εικόνα 39 – Εισαγωγή Countermeasures (2)



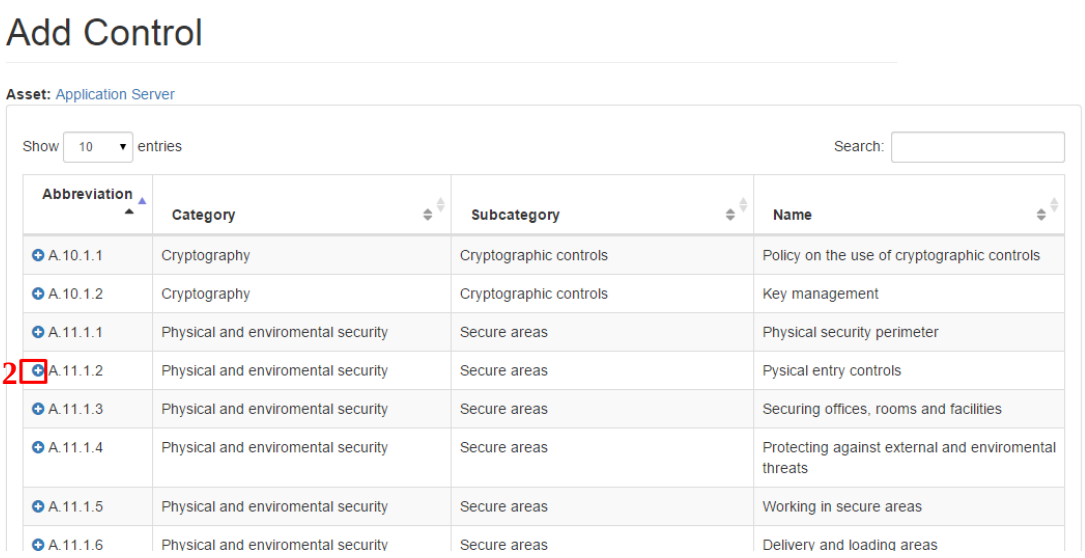

Εικόνα 40 – Εισαγωγή Countermeasures (3)



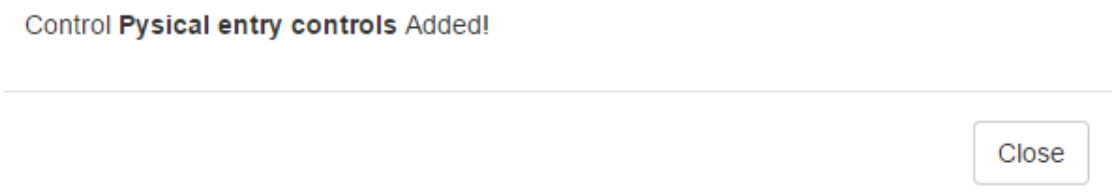

Εικόνα 41 – Εισαγωγή Countermeasures (4)




Εικόνα 42 – Εισαγωγή Controls of ISO 27001 (1)

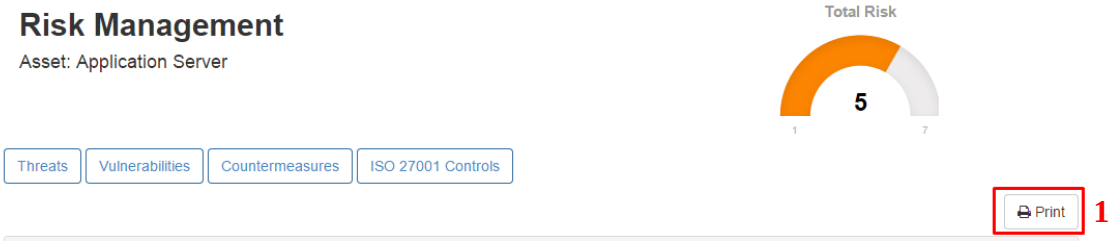



Εικόνα 43 – Εισαγωγή Controls of ISO 27001 (2)




Εικόνα 44 – Εισαγωγή Controls of ISO 27001 (3)

Αφού ο administrator ολοκληρώσει και αυτή τη διαδικασία έχει τη δυνατότητα να εξάγει μια συνολική αναφορά *(report)* για το συγκεκριμένο asset.



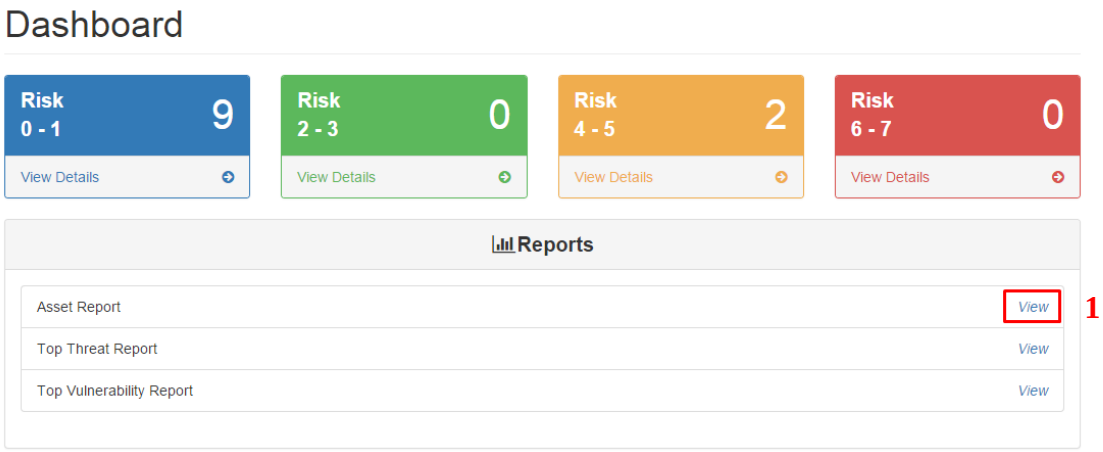

**Εικόνα 45 – Asset Report (1)**

2

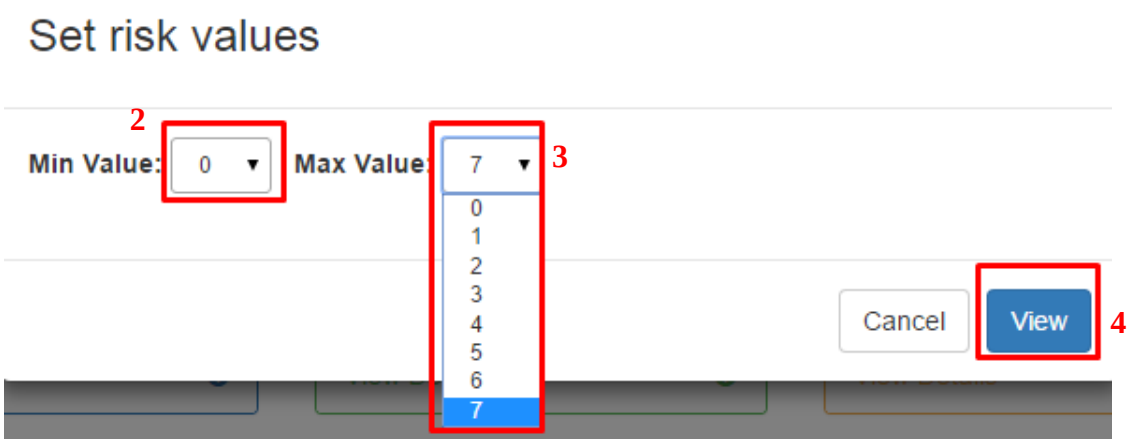

Εικόνα 46 – Asset Report (2)

### 4.3.8 Reports

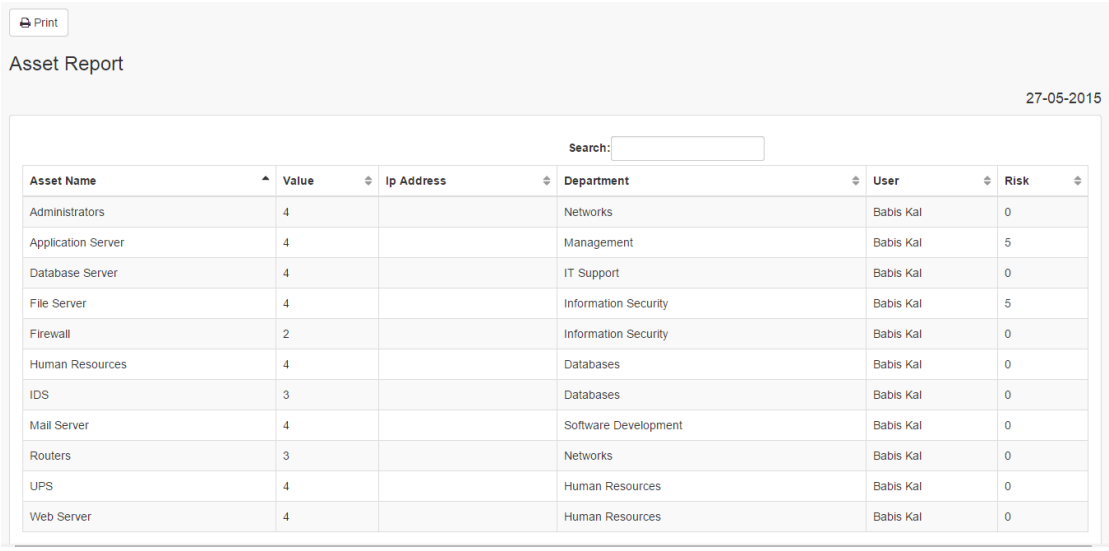
Επιπλέον, όσον αφορά το θέμα των αναφορών *(reports,)* ο administrator έχει τη δυνατότητα να εξάγει άλλα τρία reports. Το πρώτο παρέχει συγκεντρωτική πληροφορία για τους πόρους του συστήματος, σύμφωνα με το ρίσκο το οποίο έχουν. Τα άλλα δύο δίνουν πιο γενική πληροφορία η οποία αφορά τα threats και τα vulnerabilities με την υψηλότερη αξία *(value)* στο πληροφοριακό σύστημα.




Εικόνα 48 – Asset Report according to Risk (1)



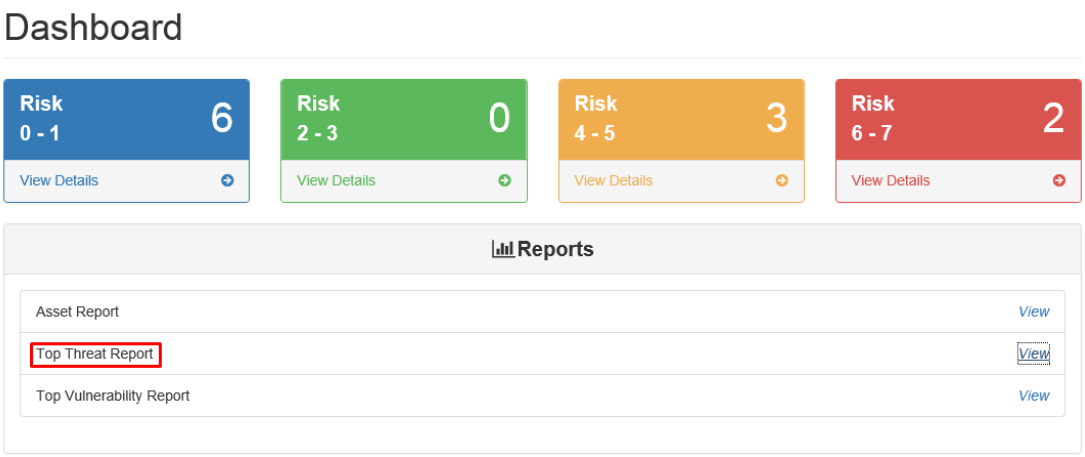

Εικόνα 59 – Asset Report according to Risk (2)



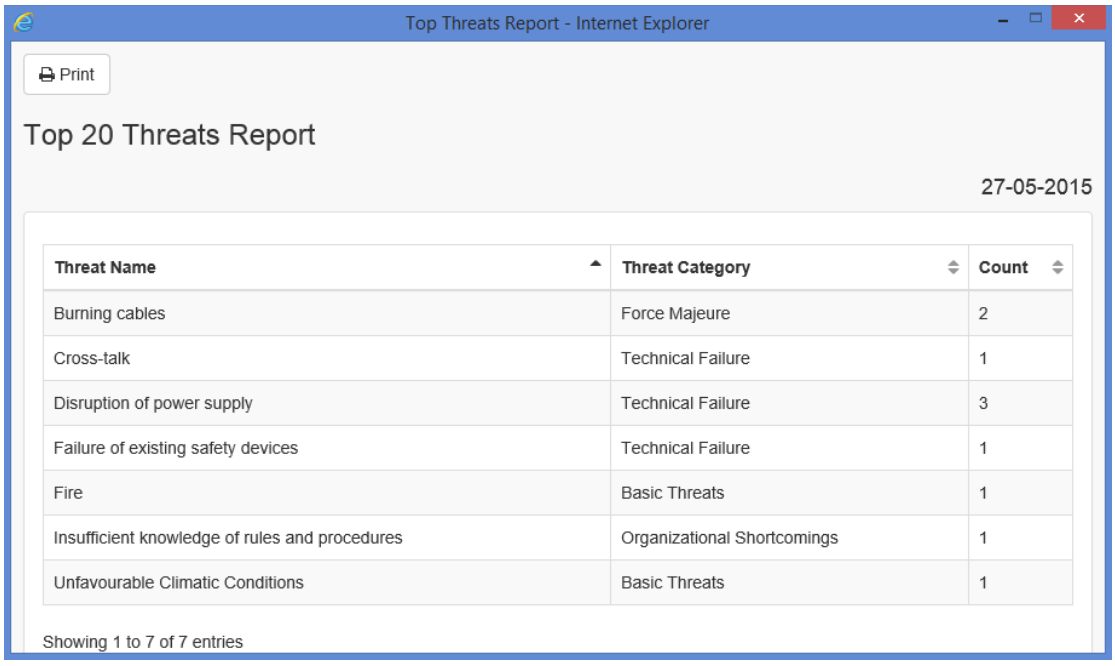

| Asset Name | Value | Ip Address | Department | User | Risk |
|---|---|---|---|---|---|
| Administrators | 4 | | Networks | Babis Kal | 0 |
| Application Server | 4 | | Management | Babis Kal | 5 |
| Database Server | 4 | | IT Support | Babis Kal | 0 |
| File Server | 4 | | Information Security | Babis Kal | 5 |
| Firewall | 2 | | Information Security | Babis Kal | 0 |
| Human Resources | 4 | | Databases | Babis Kal | 0 |
| IDS | 3 | | Databases | Babis Kal | 0 |
| Mail Server | 4 | | Software Development | Babis Kal | 0 |
| Routers | 3 | | Networks | Babis Kal | 0 |
| UPS | 4 | | Human Resources | Babis Kal | 0 |
| Web Server | 4 | | Human Resources | Babis Kal | 0 |

Εικόνα 60 – Asset Report according to Risk (3)

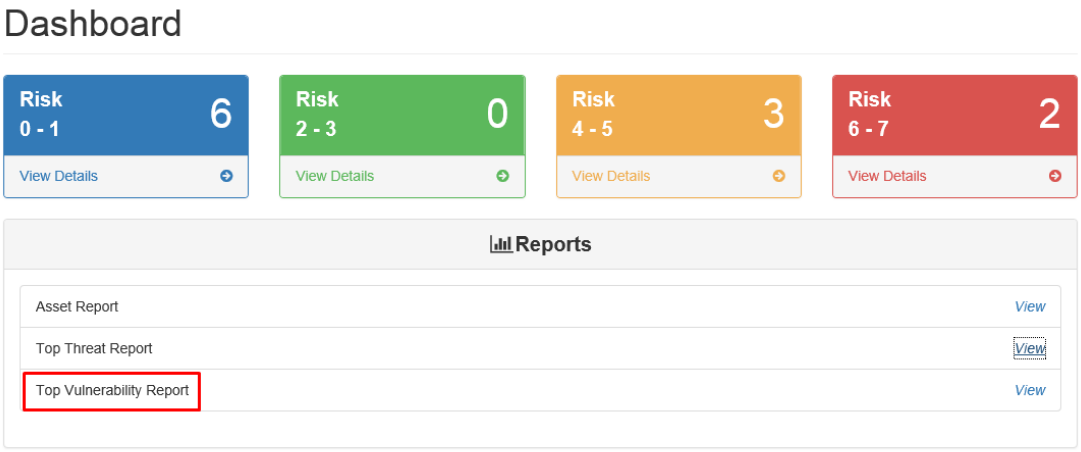
Τα report τα οποία αφορούν τα threats και τα vulnerabilities είναι μια γενική εικόνα για το ποια είναι τα κυριότερα threats και vulnerabilities, τα οποία αντιμετωπίζει το πληροφοριακό σύστημα. Επιπροσθέτως, και στα δύο report υπάρχει ένδειξη που δηλώνει πόσες φορές απαντά κάποιο threat ή vulnerability, ώστε ο Information Security Officer να έχει μία πλήρη εικόνα για τις κυριότερες ευπάθειες και απειλές του συστήματος.



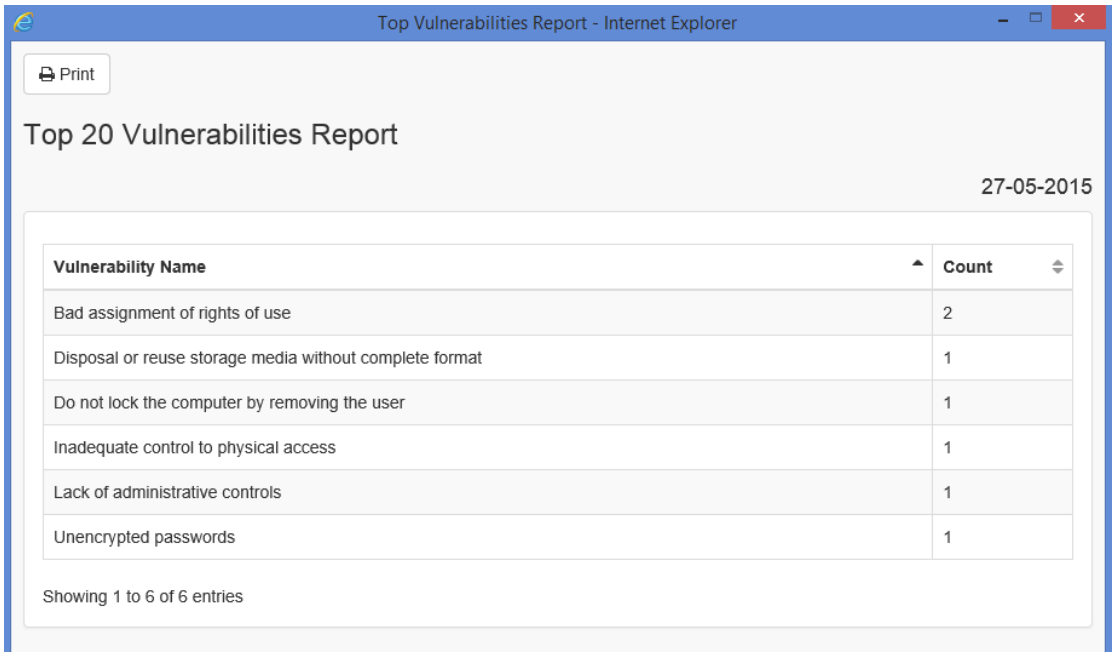

Εικόνα 61 – Top Threat Report




Εικόνα 62 – Top Threat Report Outcome




Εικόνα 61 – Top Vulnerability Report




Εικόνα 62 – Top Vulnerability Report Outcome

# Κεφάλαιο 5

## Επίλογος

### 5.1 Συμπεράσματα

Είναι σαφές ότι η Ασφάλεια Πληροφοριών είναι αναπόσπαστο κομμάτι της Πληροφορικής. Μέσω της συγκεκριμένης διπλωματικής εργασίας δόθηκε η δυνατότητα τόσο της μελέτης του προτύπου ISO 27001:2013 όσο και μεθόδων ανάλυσης επικινδυνότητας όπως είναι η CRAMM, η NIST 800, ISO 31000 κ.τ.λ.

Βέβαια, αξιοσημείωτο είναι το γεγονός ότι από τη μελέτη για την εκπόνηση της διπλωματικής, παρατηρήθηκε η αυξανόμενη απειλή για threats και vulnerabilities, η οποία ελλοχεύει. Ο ψηφιακός κόσμος είναι συνεχώς μεταβαλλόμενος και οι απειλές αυξάνονται εκθετικά.

Προκύπτει λοιπόν ότι η φιλοσοφία της ασφάλειας πληροφοριών και των συστημάτων που φιλοξενούν αυτές τις πληροφορίες πρέπει να είναι αναπόσπαστο τμήμα της πληροφοριακής κουλτούρας, καθότι, σε κάθε νέα επίθεση που διενεργείται, διακυβεύονται σημαντικές πληροφορίες, αλλά και τίθενται σοβαρά οικονομικά ζητήματα.

Συμπληρωματικά προς τα έως τώρα διατυπωμένα, αξίζει να αναφερθεί ότι η ανάπτυξη της εφαρμογής, η οποία αναλύθηκε σε προηγούμενο κεφάλαιο, ανέδειξε την ανάγκη δημιουργίας ενός πλήρως αυτοματοποιημένου εργαλείου, το οποίο θα πραγματοποιεί τόσο τις γραφειοκρατικές διαδικασίες του ISO 27001:2013 όσο και την ανάλυση επικινδυνότητας.

### 5.2 Future Work

Η εφαρμογή, η οποία αναπτύχθηκε για τις ανάγκες της διπλωματικής εργασίας, είναι μία πρώτη προσέγγιση στην αυτοματοποίηση των διαδικασιών του ISO 27001:2013 αλλά και της ανάλυσης επικινδυνότητας. Σαφώς και υπάρχουν περιθώρια βελτιστοποίησης για την εφαρμογή.

Η εξέλιξη της εφαρμογής με την πλήρη αυτοματοποίηση του ISO, δημιουργώντας τις πολιτικές που χρειάζονται μέσα από έτοιμες φόρμες που θα συμπληρώνει ο χρήστης θα ήταν μείζονος σημασίας. Επίσης, η εξέλιξη της ανάλυσης επικινδυνότητας με εμπλουτισμό της εφαρμογής και με άλλες μεθόδους, και τη δυνατότητα επιλογής μεθόδου από τον χρήστη, θα ήταν δύο πολύ σημαντικά στοιχεία που θα κερδίσουν την προσοχή μας στο άμεσο μέλλον.

Η επιλογή μεθόδου είναι σημαντική γιατί η κάθε μέθοδος προσφέρει διαφορετικά αποτελέσματα και ανταποκρίνεται στις διαφορετικές ανάγκες του εκάστοτε

οργανισμού. Αυτό θα μπορούσε να θεωρηθεί μια καινοτομία, καθώς θα υπάρχουν σε μία εφαρμογή όλες οι μέθοδοι ανάλυσης επικινδυνότητας με δυνατότητα επιλογής μεθόδου.

Ως σημείο έρευνας και ανάπτυξης ο χώρος της ασφάλειας είναι ένα πεδίο το οποίο απαιτεί συνεχή έρευνα καθώς είναι βέβαιο ότι στο πλαίσιο της εξέλιξης, η οποία απαντά σε κάθε τομέα τη σημερινή εποχή, και πόσο μάλλον στον τεχνολογικό, είναι φυσικό επακόλουθο να προκύπτουν νέα δεδομένα που χρήζουν ενδελεχούς διερεύνησης και αφοσίωσης.

# Παράρτημα Α

## Αποτελέσματα PENETRATION TEST του Συστήματος «ISO/IEC 27001:2013»

ΚΕΝΤΡΟ ΠΛΗΡΟΦΟΡΙΚΗΣ ΥΠΟΣΤΗΡΙΞΗΣ ΕΛΛΗΝΙΚΟΥ ΣΤΡΑΤΟΥ (ΚΕΠΥΕΣ)
ΛΟΧΟΣ ΚΥΒΕΡΝΟΑΜΥΝΑΣ
Αθήνα, 15/6/2015

### Περιορισμοί στην αποκάλυψη και χρήση της παρούσας Έκθεσης

Η Έκθεση αυτή περιέχει πληροφορίες σχετικά με δυνητικά υψηλού επιπέδου τρωτά σημεία του συστήματος στόχου (ISO/IEC 27001:2013), καθώς και μεθόδων για την αξιοποίηση τους. Ο Λόχος Κυβερνοάμυνας συνιστά να λαμβάνονται ειδικές προφυλάξεις για την προστασία αυτού του εγγράφου και των πληροφοριών που εμπεριέχονται στο παρόν.

Το Penetration Test είναι μία αβέβαιη διαδικασία, βασισμένη σε εμπειρίες του παρελθόντος, πληροφορίες που είναι διαθέσιμες σήμερα και γνωστές απειλές. Πρέπει να τονιστεί ότι όλα τα συστήματα ασφάλειας πληροφοριών τα οποία εκ φύσεως εξαρτώνται από ανθρώπινα όντα, είναι ευπαθή σε ένα βαθμό. Ο Λόχος Κυβερνοάμυνας θεωρεί ότι οι κύριες αδυναμίες των συστημάτων που αναλύθηκαν έχουν προσδιοριστεί, παρόλα αυτά, δεν μπορεί να παρέχει διαβεβαίωση ότι θα προσδιορισθούν όλα τα πιθανά σημεία αδυναμιών.

Τα συμπεράσματα της παρακάτω διαδικασίας αφορούν τη συγκεκριμένη έκδοση του συστήματος, καθώς οποιαδήποτε αλλαγή μπορεί να προκαλέσει τη δημιουργία νέων ευπαθειών.

### Περίληψη

Κατά την περίοδο μεταξύ 8/6/2015 και 10/6/2015, ο Λόχος Κυβερνοάμυνας διετάχθη να εκτελέσει ένα Penetration Test στο σύστημα "*ISO/IEC 27001:2013*".

Ο συγκεκριμένος έλεγχος έγινε από εσωτερική γραμμή ως ένας οποιοσδήποτε χρήστης που έχει να αντιμετωπίσει και τις διατάξεις ασφαλείας του υπολογιστή.

Ο στόχος του Penetration Test είναι να ανακαλύψει τυχόν αδυναμίες ασφαλείας στο εν λόγω σύστημα, να προσδιορίσει το επίπεδο του κινδύνου σύμφωνα με την αντίστοιχη αδυναμία και να προτείνει αντίμετρα, ώστε να

μετριασθεί ο δυνητικός αντίκτυπος σε ένα αποδεκτό επίπεδο.

Το αποτέλεσμα της δοκιμής δεν ήταν επιτυχές και το σύστημα στόχος δεν βρέθηκε ευάλωτο.

Καθ' όλη τη διάρκεια αυτής της διαδικασίας έχει εκτελεστεί μια εκτενή σειρά επιθέσεων εναντίον του συστήματος στόχου, προκειμένου να προσδιορισθούν τρωτά σημεία που θα μπορούσαν να βλάψουν την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των πληροφοριών.

Ο έλεγχος έγινε σε δύο(2) φάσεις:

A. Black Box σαν κάποιος χρήστης που δεν έχει δικαιώματα στην εφαρμογή (εξωτερική πρόσβαση).

B. Grey Box σαν χρήστης (εξουσιοδοτημένη πρόσβαση).

## Εισαγωγή

Κατά τη διάρκεια προγραμματισμένου ελέγχου για ύπαρξη τυχόν αδυναμιών, ο Λόχος Κυβερνοάμυνας του ΚΕΠΥΕΣ προέβη στη διαδικασία του Penetration Test στο σύστημα *"ISO/IEC 27001:2013"*.

Στην αρχή, οι συνθήκες διεξαγωγής του Penetration Test περιλάμβαναν μηδενικό επίπεδο πρόσβασης, δηλαδή ο επιτιθέμενος δεν γνώριζε τίποτα για το σύστημα και δεν είχε τα απαραίτητα διαπιστευτήρια (credentials). Στη συνέχεια έγινε έλεγχος με πρόσβαση απλού χρήστη.

Κατά την διάρκεια του Penetration Test, ο Λόχος Κυβερνοάμυνας υπέθεσε ότι το σύστημα στόχος ανήκει σε περιβάλλον παραγωγής χρησιμοποιώντας πραγματικά δεδομένα και ότι όλοι οι ιδιοκτήτες των συστημάτων έχουν ενημερωθεί για τις δραστηριότητες που θα λάβουν μέρος. Δεν δόθηκε καμία πληροφορία. Επομένως, οι φορείς της επίθεσης ήταν μη εξουσιοδοτημένοι χρήστες χωρίς καμία προηγούμενη γνώση της αρχιτεκτονικής υποδομής και διαμόρφωσης.

# 1. Μοντέλο ανάλυσης Ευπαθειών

Ενώ η ανακάλυψη ευπαθειών είναι ένα πολύ σημαντικό ορόσημο κατά την διάρκεια ενός Penetration Test, η αξιολόγηση κάθε αδυναμίας προκειμένου να εκτιμηθεί το παραγόμενο επίπεδο κινδύνου είναι η πιο σημαντική διαδικασία της εμπλοκής.

Επειδή κάθε εκμετάλλευση αδυναμίας είναι πιθανό να έχει τις δικές της συνέπειες, πιθανότητα επίθεσης, σενάριο επίθεσης, πιθανότητα επιτυχίας επίθεσης αντιπάλου, είναι απαραίτητο να προσδιορισθεί ο κίνδυνος για κάθε συνδυασμό των παραγόντων κινδύνου.

Η Ανάλυση Ευπάθειας είναι μια συστηματική προσέγγιση κατά την οποία ο κίνδυνος είναι συνάρτηση της

σοβαρότητας των συνεπειών ενός ανεπιθύμητου γεγονότος **(Δυνητικός Κίνδυνος)** και της πιθανότητας μιας επιτυχούς επίθεσης **(Πιθανότητα Εκμετάλλευσης).**

Αναπτύχθηκε ένα μοντέλο ανάλυσης τρωτών σημείων βασισμένο σε διεθνείς βέλτιστες πρακτικές ώστε να συμπεριληφθούν όλες οι διαφορετικές συνιστώσες που επηρεάζουν τον αντίκτυπο και την πιθανότητα πραγματοποίησης μιας συγκεκριμένης ευπάθειας.

## 1.1 Δυνητικός Αντίκτυπος (ΔΑ)

**Ο Δυνητικός Αντίκτυπος μπορεί να υπολογισθεί σε τρεις ποιοτικές μετρήσεις που αποτιμώνται σύμφωνα με το αποτέλεσμα που έχει η ευπάθεια στις παρακάτω συνιστώσες (Αξίες: 1 – 5):**

**Απώλεια Εμπιστευτικότητας:** Η αξία αυτής της μέτρησης εξαρτάται από τον όγκο και την ευαισθησία των δεδομένων που αποκαλύπτονται.

**Απώλεια της Ακεραιότητας:** Η αξία αυτής της μέτρησης εξαρτάται από τον όγκο των δεδομένων που δύνανται να καταστραφούν καθώς και την επέκταση της διαφθοράς.

**Απώλεια Διαθεσιμότητας:** Η αξία αυτής της μέτρησης εξαρτάται από το χρονοδιάγραμμα της διακοπής υπηρεσιών και την κρισιμότητα των υπηρεσιών που διακόπτονται.

## 1.2 Πιθανότητα Εκμετάλλευσης (ΠΕ)

Μετά τον προσδιορισμό των τεχνικών επιπτώσεων μιας συγκεκριμένης ευπάθειας, η πιθανότητα επιτυχούς αξιοποίησης της τρωτότητας πρέπει να εντοπιστεί. Η πιθανότητα μπορεί να υπολογιστεί σε οκτώ ποιοτικές μετρήσεις, που

χωρίζονται σε δύο κατηγορίες: Παράγοντες κινδύνου και παράγοντες ευπάθειας.

Παρακάτω αναφέρονται οι παράγοντες που αφορούν το προφίλ και τις ικανότητες που πρέπει να έχουν οι επιτιθέμενοι (hackers) ώστε να επιτευχθεί εκμετάλλευση της κάθε ευπάθειας (Ο κάθε παράγοντας μπορεί να βαθμολογηθεί σε κλίμακα από1 έως 5):

- **Επίπεδο γνώσεων:** Αυτός ο παράγοντας δείχνει τις τεχνικές ικανότητες του επιτιθέμενου.

- **Κίνητρο**: Αυτός ο παράγοντας δείχνει το κίνητρο του επιτιθέμενου.

- **Ευκαιρία**: Αυτός ο παράγοντας δείχνει το απαιτούμενο επίπεδο πρόσβασης του επιτιθέμενου.

- **Πηγή επίθεσης**: Αυτός ο παράγοντας δείχνει τους φορείς επίθεσης από την οποία είναι προσβάσιμη η ευπάθεια.

Οι παράγοντες ευπάθειας που σχετίζονται με την πιθανότητα ανακάλυψης και εκμετάλλευσης από έναν πράκτορα (Κλίμακα για κάθε παράγοντα από 0 έως 4):

- **Ευκολία Ανακάλυψης:** Αυτός ο παράγοντας δείχνει πόσο εύκολο είναι για έναν επιτιθέμενο να προσδιορίσει την ευπάθεια.

- **Ευκολία Εκμετάλλευσης:** Αυτός ο παράγοντας δείχνει πόσο εύκολο είναι για έναν επιτιθέμενο να εκμεταλλευτεί την ευπάθεια.

- **Δημοσιότητα:** Αυτός ο παράγοντας δείχνει πόσο διαδεδομένη είναι η ευπάθεια.

- **Ευκολία εντοπισμού των ενεργειών του πράκτορα:** Η αξία αυτής της μέτρησης εξαρτάται από την ιχνηλασιμότητα των ενεργειών των επιτιθέμενων.

## 2. Επίπεδο Κινδύνου (ΕΚ)

Για τον υπολογισμό του Επίπεδου Κινδύνου (ΕΚ) κάθε αδυναμίας πολλαπλασιάζονται οι αξίες του Δυνητικού Αντίκτυπου (ΔΑ) και της Πιθανότητας Εκμετάλλευσης (ΠΕ), βασισμένες στην ακόλουθη εξίσωση:

**ΕΚ = ΔΑ x ΠΕ**

## Δείκτες Επικινδυνότητας

**Critical**

Αυτά τα τρωτά σημεία είναι κρίσιμα για το σύστημα και θα πρέπει να αντιμετωπίζονται αμέσως.

**High**

Ευρήματα υψηλού κινδύνου. Θα πρέπει να αντιμετωπιστούν το συντομότερο δυνατόν, καθώς μπορεί να θέτουν σε άμεσο κίνδυνο τα συστήματα, ή τα δεδομένα που εμπλέκονται.

**Medium**

Ευρήματα μέτριου κινδύνου, θα πρέπει να αντιμετωπιστούν γρήγορα, αλλά με δευτερεύουσα προτεραιότητα.

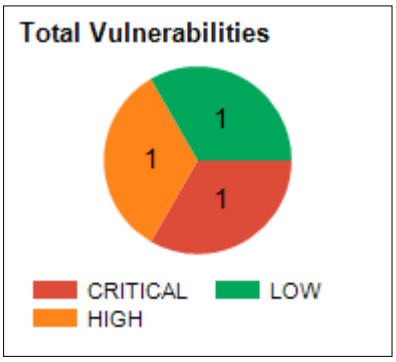
**Low**

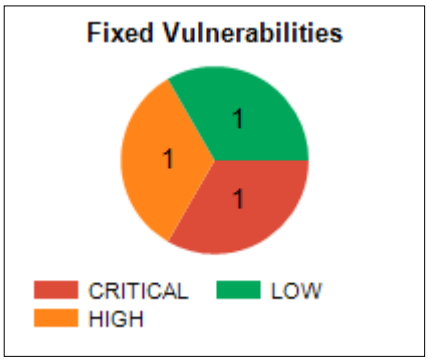
Ευρήματα χαμηλού κινδύνου, θα πρέπει να αντιμετωπιστούν εν ευθέτω χρόνο.

**Info**

Ευρήματα χαμηλού κινδύνου, θα πρέπει να αντιμετωπιστούν εν ευθέτω χρόνο.

## 3. Ανάλυση τρωτοτήτων που εντοπίστηκαν κατά τον έλεγχο.




**Vulnerability:** Sensitive Data Exposure **Fixed:** ☑

**Critical**

**Summary:** Στην φόρμα διαχείρισης χρήστη ("/Users/EditUser") αλλά και στο προφίλ του κάθε χρήστη ("/Profile") ο επιτιθέμενος μπορεί να δει στον πηγαίο κώδικα της φόρμας τον κωδικό του χρήστη σε μορφή κειμένου (plaintext).

**Solution:** Ο διακομιστής δεν θα πρέπει να αποκαλύπτει στον χρήστη (Client) ευαίσθητες πληροφορίες.

**Vulnerability:** Failure to Restrict URL Access **Fixed:** ☑

**High**

**Summary:** Παρατηρήθηκε ότι στην καρτέλα διαχείρισης αρχείων ("/Files") δεν εκτελείται ο απαιτούμενος έλεγχος πρόσβασης με αποτέλεσμα κάποιος να έχει πρόσβαση σε αυτήν χωρίς όμως να έχει αυθεντικοποιηθεί.

**Vulnerability:** Remote File Inclusion (RFI) **Fixed:** ✓

**Low**

**Summary:** Στην καρτέλα διαχείρισης αρχείων ("/Files"). Ο διαχειριστής του συστήματος μπορεί να ανεβάσει αρχεία κακόβουλου χαρακτήρα. Η εφαρμογή, δεν εκτελεί έλεγχους των τύπων των αρχείων κάτι το οποίο επιτρέπει το ανέβασμα και την εκτέλεση κακόβουλων αρχείων (webshell).

**Solution:** Η εφαρμογή θα πρέπει να ελέγχει από την μεριά του διακομιστή, τους τύπους των αρχείων και να επιτρέπει μόνο συγκεκριμένους (π.χ. doc, docx, pfd, xls, xlsx).

# 4. Συμπεράσματα και Συστάσεις

## 4.1 Συμπεράσματα

Ο τρόπος εκμετάλλευσης των αδυναμιών που βρέθηκαν στο σύστημα στόχος είναι γνωστός στο κοινό και παρουσιάζει κρίσιμο επίπεδο τεχνικού κινδύνου. Τα ακόλουθα τονίζουν θέματα ασφαλείας και πρέπει να εξεταστούν σε βάθος:

- Είναι δυνατό για έναν ήδη εξουσιοδοτημένο χρήστη της εφαρμογής να αποκτήσει πλήρη πρόσβαση στον εξυπηρετητή ανεβάζοντας αρχεία κακόβουλου χαρακτήρα.
- Αποκαλύπτεται κρίσιμη πληροφορία στον διαχειριστή της εφαρμογής Στην φόρμα διαχείρισης χρήστη ("/Users/EditUser") αλλά και στο προφίλ του κάθε χρήστη ("/Profile") ο επιτιθέμενος μπορεί να δει στον πηγαίο κώδικα της φόρμας τον κωδικό του χρήστη σε μορφή κειμένου (plaintext).
- Στο μενού *Files* παρατηρήθηκε η δυνατότητα upload κακόβουλου αρχείου (web shell) καθώς η εφαρμογή δεν πραγματοποιεί ελέγχους για τον τύπο των αρχείων τα οποία έχουν δικαίωμα να γίνουν upload στην εφαρμογή.

## 4.2 Συστάσεις

Το σύστημα στόχος έχει βρεθεί ότι είναι ευάλωτο σε μικρό αριθμό και είδος επιθέσεων, οι οποίες όμως θα πρέπει να μετριαστούν όσο το δυνατόν συντομότερα στο περιβάλλον παραγωγής. Οι επιθέσεις που πραγματοποιηθήκαν κατά τη διάρκεια του Penetration Test είναι γνωστές στην hacking κοινότητα και σε περίπτωση που ένας κακόβουλος χρήστης αποφασίσει να ξεκινήσει μια επίθεση, υπάρχει δυνατότητας επιτυχίας.

Συνεπώς, η σύσταση του Λόχου Κυβερνοάμυνας είναι να πραγματοποιηθούν οι διορθωτικές ενέργειες που περιγράφονται στο κεφάλαιο 3 όσο το δυνατόν συντομότερα.

Το επίπεδο ασφαλείας που περιγράφεται καθώς και οι σχετικές συστάσεις αφορούν μόνο την web εφαρμογή. Κίνδυνοι για την ασφάλεια αυτής μπορούν να προέλθουν από μη ασφαλείς ρυθμίσεις των διακομιστών στους οποίους πρόκειται να φιλοξενηθεί.

# Βιβλιογραφία


- ISO/IEC 27000 — Information security management systems — Overview and vocabulary
- ISO/IEC 27001:2005/2013— Information technology - Security Techniques - Information security management systems — Requirements
- ISO/IEC 27002 — Code of practice for information security management
- ISO/IEC 27005 — Information security risk management
- ISO/IEC 31010:2009 - Risk Management - Risk Assessment Techniques
- CRAMM User Guide
- BSI IT-Grundschutz-Catalogues
- NIST SP 800-30 (csrc.nist.gov)
- www.iso27000.org
- www.iso27001standard.com
- msdn.microsoft.com
- www.asp.net/mvc
- www.mysql.com
- Ασφάλεια Πληροφοριακών Συστημάτων, Κάτσικας Σ. Γκρίτζαλης Δ., Γκρίτζαλης Σ, Εκδόσεις Νέων Τεχνολογιών (2004)
- The Hacker Playbook – Practical Guide to Penetration Testing, Peter Kim