



**ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ**

**ΜΕΤΑΠΤΥΧΙΑΚΟ ΔΙΠΛΩΜΑ ΕΙΔΙΚΕΥΣΗΣ (MSc)
στα ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ**

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

**«Μελέτη μεθόδων διαχείρισης επικινδυνότητας
πληροφοριακών συστημάτων και υλοποίηση μελέτης
περίπτωσης (case study) με τη μέθοδο Magerit και το
εργαλείο EAR/Pilar»**

**Σαραβάνου Μαρία-Χριστίνα
Μ310021**

ΑΘΗΝΑ, ΙΑΝΟΥΑΡΙΟΣ 2015

**ΜΕΤΑΠΤΥΧΙΑΚΟ ΔΙΠΛΩΜΑ ΕΙΔΙΚΕΥΣΗΣ (MSc)
στα ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ**

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

**«Μελέτη μεθόδων διαχείρισης επικινδυνότητας
πληροφοριακών συστημάτων και υλοποίηση μελέτης
περίπτωσης (case study) με τη μέθοδο Magerit και το
εργαλείο EAR/Pilar»**

**Σαραβάνου Μαρία-Χριστίνα
Μ310013**

**Επιβλέπων Καθηγητής: Δημήτρης Γκρίζαλης
Εξωτερικός Κριτής: Ονοματεπώνυμο**

**ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ**

ΑΘΗΝΑ, ΔΕΚΕΜΒΡΙΟΣ 2014

Πρόλογος και ευχαριστίες

Η παρούσα διατριβή πραγματοποιήθηκε στα πλαίσια της απόκτησης Μεταπτυχιακού Διπλώματος Ειδίκευσης (MSc) στα Πληροφοριακά Συστήματα, του τμήματος Πληροφορικής του Οικονομικού Πανεπιστημίου Αθηνών. Σκοπός είναι η πρόταση πλαισίου κριτηρίων για την επιλογή και την αξιολόγηση των υπαρχουσών μεθόδων μελέτης και διαχείρισης επικινδυνότητας και η σύγκριση των μεθόδων CRAMM και Magerit, καθώς και των εργαλείων που τις υποστηρίζουν.

Θα ήθελα να ευχαριστήσω τους γονείς μου για την αμέριστη και διαρκή υποστήριξή τους. Σας ευχαριστώ για όλα όσα κάνατε και συνεχίζετε να κάνετε για μένα. Η πίστη σας στις δυνατότητές μου αποτέλεσε αρωγό σε όλους τους στόχους και τα όνειρά μου. Επίσης θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή Δημήτρη Γκρίζαλη για τη δυνατότητα που μου πρόσφερε να εκπονήσω τη συγκεκριμένη πτυχιακή εργασία. Ιδιαίτερες ευχαριστίες στον υποψήφιο διδάκτορα Βασίλη Σταύρου για το χρόνο που διέθεσε, τη συνεχή υποστήριξη, την καθοδήγηση και τις πολύτιμες συμβουλές του.

Αθήνα, Ιανουάριος 2015

Μαρία-Χριστίνα Σαραβάνου

Περιεχόμενα

Περιεχόμενα.....	5
Ευρετήριο Εικόνων.....	11
Ευρετήριο Πινάκων	12
ΠΕΡΙΛΗΨΗ	13
Executive Summary	16
1. Εισαγωγή	18
1.1 Αντικείμενο διπλωματικής εργασίας	18
1.2 Αφορμή για την έρευνα	19
1.3 Σύντομη περιγραφή	21
2. Βασικοί ορισμοί.....	23
2.1 Αγαθό	23
2.2 Κίνδυνος και Επικινδυνότητα.....	24
2.3 Απειλή.....	26
2.4 Τρωτότητα	27
2.5 Αντίμετρο.....	28
2.6 Υποδομή	29
2.6.1 Κρίσιμες υποδομές.....	29
3. Διαχείριση επικινδυνότητας	32
3.1 Ανάλυση Επικινδυνότητας	33
3.1.1 Αναγνώριση Επικινδυνότητας.....	34
3.1.1.1 Μέθοδοι καταγραφής παραγόντων κινδύνου	35
3.1.2 Εκτίμηση Επικινδυνότητας	38
3.1.2.1 2.1 Ποσοτική αξιολόγηση.....	38
3.1.2.1.1 Εργαλεία ποσοτικού προσδιορισμού του κινδύνου	40
3.1.2.2 Ποιοτική αξιολόγηση.....	41
3.1.2.2.1 Μέθοδος Πιθανότητας - Επίπτωσης	42
3.1.2.2.2 Μέθοδος Βάρος-Σοβαρότητα.....	44
3.1.3 Αποτίμηση Επικινδυνότητας.....	45
3.2 Μεθοδολογία Διαχείρισης Επικινδυνότητας.....	47
4. Νομοθετικό πλαίσιο των πληροφοριακών συστημάτων	49
4.1 Πρότυπα	49
4.1.1 Πρότυπο Information Security Forum (ISF) Standard of Good Practice	49
4.1.2 Οικογένεια προτύπων 27000	51
4.1.2.1 ISO/IEC 27001:2005	52
4.1.2.2 ISO/IEC 27002:2005	55
4.1.2.3 Σύγκριση ISO/IEC 27001 και 27002.....	56
4.2 Πολιτικές προστασίας κρίσιμων υποδομών	57

4.2.1	Πολιτικές προστασίας κρίσιμων υποδομών στην Ευρωπαϊκή Ένωση	57
4.2.2	Πολιτικές προστασίας κρίσιμων υποδομών στις ΗΠΑ	60
4.2.3	Πολιτικές προστασίας κρίσιμων υποδομών στην Ελλάδα	61
4.2.4	Πρότυπα προστασίας κρίσιμων υποδομών.....	61
4.2.4.1	Διαχείριση Ασφάλειας στις ΗΠΑ.....	65
4.2.4.2	Διαχείριση Ασφάλειας στην Ευρώπη (τομέας ενέργειας).....	67
4.2.4.3	Προστασία κρίσιμων υποδομών Πληροφορικής και Επικοινωνιών	68
5.	Ολοκληρωμένες Προσεγγίσεις Εκτίμησης Επικινδυνότητας.....	69
5.1	Μέθοδος CRAMM	69
5.2	Μέθοδος Magerit – Εργαλείο EAR/Pilar	72
5.3	Μέθοδος NIST	72
5.4	Μέθοδος EBIOS	78
5.5	Μέθοδος/Εργαλείο OCTAVE	78
5.6	Μέθοδος MEHARI	79
5.7	Μέθοδος/Εργαλείο CORAS	79
5.8	Μέθοδος της Χάγης (DHM)	80
5.9	Μέθοδος PAS 55.....	81
5.10	Μέθοδος Handreiking Risico-analyse (Guide to Risk – Ολλανδική μέθοδος).....	82
5.11	Μέθοδος NRB	83
5.12	Μέθοδοι βάσει οργανισμού ISF.....	85
5.13	Εργαλείο CARVER2	87
5.14	Μητρώο κινδύνων ασφάλειας QinetiQ	88
5.15	Μέθοδος προγράμματος COUNTERACT (ενέργεια & μεταφορές – τρομοκρατία) 90	90
5.16	Μέθοδος RAM-CAP plus (κρίσιμες υποδομές)	91
5.17	Μέθοδος ES-ISAC (τομέας ενέργειας).....	92
6.	Η Μέθοδος Magerit και το εργαλείο EAR/PILAR	94
6.1	Μέθοδος Magerit	94
6.2	Περιγραφή Magerit	94
6.3	Βήματα Magerit.....	95
6.3.1.	Στάδιο 1: Προετοιμασία και Προγραμματισμός Έργου	96
6.3.2.	Στάδιο 2: Ανάλυση Επικινδυνότητας	98
6.3.3.	Στάδιο 3: Διαχείριση Επικινδυνότητας	101
6.4.	Το Εργαλείο EAR/Pilar	103
6.4.1.	Λειτουργικά Βήματα: Αναγνώριση αγαθών.....	105
6.4.1.1.	Κατηγοριοποίηση αγαθών	105
6.4.1.2.	Επεξεργασία Αγαθών	107
6.4.2.	Λειτουργικά Βήματα: Αποτίμηση αγαθών	109
6.4.3.	Λειτουργικά Βήματα: Εκτίμηση απειλών	110

6.4.3.1.	Αναγνώριση Απειλών.....	111
6.4.3.2.	Αποτίμηση Απειλών	111
6.4.4.	Λειτουργικά Βήματα: Εκτίμηση Επικινδυνότητας.....	113
6.4.5.	Λειτουργικά Βήματα: Προσδιορισμός προτεινόμενων αντιμέτρων.....	116
6.4.6.	Το Εργαλείο EAR/Pilar και η Διαδικασία Συνέχισης Λειτουργίας.....	120
6.4.6.1.	Αρχικοποίηση Έργου	122
6.4.6.2.	Στάδιο Ανάλυσης Επικινδυνότητας.....	123
6.4.6.3.	Στάδιο Πλάνου Ανάκαμψης Λειτουργίας.....	127
7.	Αξιολόγηση μεθόδων	129
7.1	Τεχνικές αξιολόγησης της ανάλυσης επικινδυνότητας	129
7.2	Βιβλιογραφική ανασκόπηση κριτηρίων αξιολόγησης μεθόδων και εργαλείων	134
7.3	Ομαδοποίηση κριτηρίων αξιολόγησης μεθόδων επικινδυνότητας.....	140
7.3.1	Λογική ορθότητα	141
7.3.2	Εγκυρότητα.....	141
7.3.3	Αποδοχή	142
7.3.4	Πόροι	142
7.3.5	Χρησιμότητα.....	143
7.3.6	Αξιοπιστία.....	144
7.3.7	Ευκολία Χρήσης.....	144
7.4	Συνοπτικός πίνακας κριτηρίων.....	145
7.5	Προτεινόμενα κριτήρια	145
7.6	Επιλογή μεθόδου βάσει AHP (Advanced Hierarchical Process)	148
7.6.1	Αρχές και αξιώματα της AHP	148
7.6.2	Μετρήσεις και Αναλογικές Κλίμακες στην AHP.....	150
7.6.3	Αναλογικές κλίμακες, αριθμητικές και γραφικές συγκρίσεις ανά ζεύγη	150
7.6.4	Φραστικές συγκρίσεις ανά ζεύγη	151
7.6.5	Στάθμιση κριτηρίων/ εναλλακτικών επιλογών.....	153
7.6.6	Αξιολόγηση κριτηρίων με AHP (παράδειγμα).....	153
8.	Σύγκριση CRAMM και MAGERIT	158
8.1	Χαρακτηριστικά Μεθόδου	158
8.1.1	Κόστος.....	158
8.1.1.1	Κόστος αγοράς και εφαρμογής.....	158
8.1.1.2	Χρόνος συλλογής δεδομένων	158
8.1.1.3	Χρόνος εκτίμησης επικινδυνότητας	159
8.1.2	Απαίτηση για συμφωνία διοίκησης και αναλυτών	159
8.1.3	Ευελιξία.....	159
8.1.3.1	Προσαρμογή ως προς τον οργανισμό και το πληροφοριακό σύστημα	160
8.1.3.2	Κάλυψη μελλοντικών αλλαγών.....	160

8.1.3.3	Επιλογή συνδυασμού αντιμέτρων	161
8.1.4	Πολυπλοκότητα, Εγκυρότητα, Αξιοπιστία.....	161
8.1.5	Πληρότητα.....	162
8.1.6	Συνέπεια	162
8.1.7	Ευκολία χρήσης.....	162
8.1.8	Αρχή κόστους-ωφέλειας.....	163
8.1.9	Υποστήριξη από το κατάλληλο λογισμικό	163
8.2	Χαρακτηριστικά οργανισμού	164
8.2.1	Επίπεδο επικινδυνότητας.....	164
8.2.2	Μέγεθος.....	164
8.2.3	Κουλτούρα ασφάλειας.....	164
8.2.4	Εξωτερικές απαιτήσεις	165
8.3	Διαδικασίες μεθόδων.....	165
8.3.1	Οριοθέτηση πλαισίου ανάλυσης.....	166
8.3.2	Συνεντεύξεις και ερωτηματολόγια	166
8.3.3	Αναγνώριση αγαθών	167
8.3.4	Αποτίμηση αγαθών.....	167
8.3.5	Εκτίμηση απειλών	168
8.3.6	Εκτίμηση Κινδύνου	168
8.3.7	Προσδιορισμός αντιμέτρων.....	169
9.	Επίλογος	172
9.1	Συμπεράσματα	172
Βιβλιογραφία	175	
ΠΑΡΑΡΤΗΜΑ.....	184	
Επιτελική Σύνοψη Παραδοτέου	184	
A1. ΕΙΣΑΓΩΓΗ	189	
A1.1 Ένθεση παραδοτέου	189	
A1.2 Το ζήτημα της ασφάλειας Πληροφοριακών Συστημάτων	189	
A1.3 Αντικείμενο, σκοπός και στόχοι Μελέτης Ασφάλειας	190	
A1.4 Δομή παραδοτέου.....	191	
A2. Πλαίσιο Μελέτης Ασφάλειας ΠΣ Χ.....	193	
A2.1 Εννοιολογικό πλαίσιο.....	193	
A2.2 Εξελίξεις, τάσεις και προβληματισμοί	195	
A3. Μεθοδολογία Μελέτης Ασφάλειας	200	
A3.1 Εισαγωγή.....	200	
A3.1.1 Περιγραφή Magerit.....	201	
A3.1.2 Βήματα Magerit	201	
A3.1.2.1 Στάδιο 1: Προετοιμασία και Προγραμματισμός Έργου	203	

A3.1.2.2 Στάδιο 2: Ανάλυση Επικινδυνότητας	205
A3.1.2.3 Στάδιο 3: Διαχείριση Επικινδυνότητας	208
A4 Ανάλυση Οργανισμού	210
A4.1 Εισαγωγή	210
A4.2 Ορισμός Πεδίου Εφαρμογής	210
A4.3 Ιστορικό Οργανισμού	210
A4.4 Προσφερόμενες υπηρεσίες	211
A4.5 Διοικητικό και οργανωτικό πλαίσιο	211
A4.6 Διαδικασίες	212
A4.6.1 Λειτουργικές Διαδικασίες	214
A4.7 Ανάλυση παρούσας κατάστασης	217
A4.8 Συμπεράσματα	218
A5 Οριοθέτηση έργου	219
A5.1 Μελέτη Ευκαιρίας	219
A5.2 Καθορισμός Πεδίου Εφαρμογής	219
A5.3 Προγραμματισμός και Σχεδιασμός Έργου	220
A6 Πληροφορικά Συστήματα και Εγκαταστάσεις Οργανισμού	222
A6.1 Εισαγωγή	222
A6.2 Περιγραφή ΠΣ	222
A6.3 Αποτίμηση ΠΣ και Εγκαταστάσεων Οργανισμού	224
A6.3.1 Εισαγωγή	224
A6.3.2 Μέθοδος αποτίμησης	224
A6.3.3 Αποτελέσματα Αποτίμησης	225
A7 Εκτίμηση επικινδυνότητας	228
A7.1 Εισαγωγή	228
A7.2 Απειλές και Ευπάθειες-Αδυναμίες	228
A8. Εκτίμηση Επιπτώσεων	237
A8.1 Δυνητική Επίπτωση	238
A8.2 Εναπομένουσα Αθροιστική Επίπτωση	240
A8.3 Εκτίμηση Δυνητικής Επικινδυνότητας	242
A8.4 Εκτίμηση Εναπομένουσας Επικινδυνότητας	244
A8.5 Συνολικά αποτελέσματα εκτίμησης επικινδυνότητας	246
A9. Διαχείριση επικινδυνότητας – Προτάσεις	248
A9.1 Εισαγωγή	248
A9.2 Περιοχές επικινδυνότητας	248
A9.3 Αξιολόγηση επικινδυνότητας	249
A9.4 Προτεινόμενο πλάνο ασφάλειας	253

A9.5 Πρότυπα Μέτρα Ασφάλειας	253
A10 Εκτίμηση αντιμέτρων	256
A10.1 Προσδιορισμός των αντιμέτρων.....	257
A10.2 Αξιολόγηση Αντιμέτρων.....	259

Ευρετήριο Εικόνων

Εικόνα 1: Πολιτικές προστασίας κρίσιμων υποδομών στην Ευρωπαϊκή Ένωση	60
Εικόνα 2: Διαδικασία διαχείρισης κινδύνων εντός οργανισμού	62
Εικόνα 3: Φάσεις εκτίμησης της ευπάθειας	66
Εικόνα 4: Βήματα Magerit (χωρίς safeguards)	95
Εικόνα 5: Βήματα Magerit (με safeguards).....	96
Εικόνα 6: Αρχική οθόνη εργαλείου.....	104
Εικόνα 7: Επιλογές στο επίπεδο του ειδικού.....	105
Εικόνα 8: Επιλογές στο βασικό επίπεδο.....	105
Εικόνα 9: Αναγνώριση Αγαθών	106
Εικόνα 10: Κατηγοριοποίηση αγαθών σε κλάσεις.....	106
Εικόνα 11: Αντιστοίχιση αγαθών με άλλα αγαθά για τη δημιουργία εξαρτήσεων	107
Εικόνα 12: Διάγραμμα συσχετίσεων αγαθών.....	108
Εικόνα 13: Χάρτης εξαρτήσεων.....	108
Εικόνα 14: Βαθμολόγηση αξίας αγαθών.....	109
Εικόνα 15: Σύνολο κριτηρίων αξιολόγησης αγαθών	110
Εικόνα 16: Κατηγοριοποίηση απειλών	111
Εικόνα 17: Αποτίμηση αγαθών	112
Εικόνα 18: Παράδειγμα συσσωρευμένης επίπτωσης.....	113
Εικόνα 19: Επεξήγηση χρωμάτων αποτελεσμάτων στους πίνακες αποτίμησης επιπτώσεων	114
Εικόνα 20: Παράδειγμα συσσωρευμένης επικινδυνότητας.....	114
Εικόνα 21: Παράδειγμα πίνακα επικινδυνότητας	115
Εικόνα 22: Επεξήγηση χρωματισμού ανάλογα με επίπεδο επικινδυνότητας.....	115
Εικόνα 23: Κλίμακα αξιολόγησης αντιμέτρων	116
Εικόνα 24: Σχετικό βάρος σημαντικότητας	118
Εικόνα 25: Πρόταση αντιμέτρων	118
Εικόνα 26: Προφίλ ασφάλειας	119
Εικόνα 27: Πρόσθετα μέτρα στη διοίκηση του οργανισμού	119
Εικόνα 28: Παράδειγμα αποτίμησης αντιμέτρων ασφαλείας.....	120
Εικόνα 29: Αρχικό μενού για Επιχειρησιακή Συνέχεια	122
Εικόνα 30: Interruption Steps.....	123
Εικόνα 31: Αποτίμηση αγαθών ανά επίπεδο	124
Εικόνα 32: Αποτίμηση απειλών	125
Εικόνα 33: Παθητικές εικόνες (Συσσωρευμένη επικινδυνότητα).....	125
Εικόνα 34: Παράδειγμα ορισμού εξόπλισμού.....	126
Εικόνα 35: Πλάνο Ανάκαμψης Λειτουργίας.....	127
Εικόνα 36: Προτεινόμενα κριτήρια.....	147
Εικόνα 37: Θεμελιώδης κλίμακα συγκρίσεων	152
Εικόνα 38: Ιεραρχία απόφασης	154

Ευρετήριο Πινάκων

Πίνακας 1: Παράγοντες κινδύνου και επιπτώσεις.....	35
Πίνακας 2 - Εκτίμηση Επικινδυνότητας με τη μέθοδο Πιθανότητας-Επίπτωσης.....	42
Πίνακας 3 - Εκτίμηση πιθανότητας.....	43
Πίνακας 4 - Εκτίμηση επιπτώσεων	44
Πίνακας 5 - Μήτρα Πιθανότητας / Επιπτώσεων	44
Πίνακας 6 – Εκτίμηση Επικινδυνότητας με τη μέθοδο Βάρος-Σοβαρότητα	45
Πίνακας 7 - Αποτίμηση Κινδύνου.....	46
Πίνακας 8: Θεματικές ενότητες ISO/IEC 27001	54
Πίνακας 9: Στάδια και βήματα της CRAMM.....	70
Πίνακας 10: Μήτρα υπολογισμού επικινδυνότητας.....	75
Πίνακας 11: Κατηγοριοποίηση αγαθών στη μέθοδο Magerit	98
Πίνακας 12: Κατηγοριοποίηση απειλών στη μέθοδο Magerit	100
Πίνακας 13: Στάδια και βήματα της EAR/Pilar	103
Πίνακας 14: Κριτήρια διαχωρισμού αντιμέτρων	116
Πίνακας 15: Κριτήρια διαχωρισμού αντιμέτρων	117
Πίνακας 16: Εμφάνιση κριτηρίων σε έρευνες.....	145

ΠΑΡΑΡΤΗΜΑ

Πίνακας 1: Στόχοι της μελέτης ασφάλειας των ΠΣ της Χ	190
Πίνακας 2: Βασικές έννοιες και ορισμοί	195
Πίνακας 3: Στάδια και βήματα της Magerit και του EAR/Pilar	201
Πίνακας 4: Κατηγοριοποίηση αγαθών στη μέθοδο Magerit	205
Πίνακας 5: Κατηγοριοποίηση απειλών στη μέθοδο Magerit	206
Πίνακας 6: Κριτήρια Αποτίμησης Αγαθών	225
Πίνακας 11: Πιθανότητα πραγματοποίησης απειλής.....	232
Πίνακας 14: Εναπομένουσα Αθροιστική Επίπτωση.....	242
Πίνακας 15: Εκτίμηση Δυνητικής Επικινδυνότητας	244
Πίνακας 17: Περιοχές με μεγάλο βαθμό επικινδυνότας	249
Πίνακας 18: Μείωση επικινδυνότητας	256

ΠΕΡΙΛΗΨΗ

Το πρόβλημα της ασφάλειας των πληροφοριακών συστημάτων ήταν - από γενέσεως πληροφορικής - πάντα κρίσιμο. Αναμφισβήτητα, σήμερα ο κίνδυνος είναι πιο συνειδητός, καθώς τα συστήματα εκτίθενται σε ευρύ φάσμα χρηστών και συνεπώς κινδύνων. Η πληροφορία, οποιαδήποτε κι αν είναι η μορφή της, εφόσον είναι σημαντική απαιτείται να διαφυλάσσεται κατάλληλα και να είναι σωστά προστατευμένη. Αυτός είναι ο απότερος σκοπός της ασφάλειας πληροφοριών : να προστατεύει την πληροφορία από ένα ευρύ φάσμα απειλών παρέχοντας εξασφάλιση στην επιχειρηματική κοινωνία, ελαχιστοποιώντας τη ζημία των επιχειρήσεων και αυξάνοντας το κέρδος από επενδύσεις και επιχειρηματικές ευκαιρίες. Η ασφάλεια των συστημάτων και των δεδομένων τους ορίζεται σε τρεις διαστάσεις: εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα.

Τα τελευταία χρόνια παρατηρείται ότι η αξία των περιουσιακών στοιχείων μιας εταιρείας προέρχεται κυρίως από άνλα στοιχεία. Αναπόφευκτα, η εξάρτηση πάνω στα πληροφοριακά συστήματα και υπηρεσίες σημαίνει ότι οι οργανισμοί είναι πιο ευάλωτοι στις απειλές ασφάλειας. Τα δεδομένα, οι πληροφορίες, οι υποστηρικτικές διαδικασίες, τα συστήματα και τα δίκτυα είναι σημαντικά επιχειρηματικά αγαθά, οπότε διαφυλάσσοντας τα μία εταιρεία μπορεί να αποφύγει ανυπολόγιστα προβλήματα τα οποία ενδέχεται να προκύψουν. Η αλματώδης ανάπτυξη και αύξηση των εταιρειών, έχει ως συνέπεια να γίνονται πιο "θελκτικός" στόχος άρα τα συστήματα πληροφοριών και τα δίκτυα τους να έχουν να αντιμετωπίσουν απειλές από ένα ευρύ φάσμα πηγών, περιλαμβάνοντας computer-assisted fraud, espionage, sabotage, βανδαλισμό, φωτιά ή πλημμύρα. Πηγές ζημιάς, όπως ιοί υπολογιστών και computer hacking έχουν γίνει ολοένα και πιο συχνοί, πιο φιλόδοξοι και εντυπωσιακά ειδικευμένοι. Αντιλαμβανόμαστε λοιπόν την σπουδαιότητα που πρέπει να έχει η ασφάλεια των πληροφοριών σε μία επιχείρηση.

Σε αυτό το σημείο εγείρεται το ερώτημα: τι διαδικασίες και τι μηχανισμούς πρέπει να ακολουθήσει μία επιχείρηση έτσι ώστε να εξασφαλίσει την ακεραιότητα της και να προστατέψει τα δεδομένα της; Σε θεωρητικό επίπεδο κατανοούμε ότι θα πρέπει να εφαρμοστούν έλεγχοι και διαδικασίες η οποίες θα διασφαλίσουν την συνοχή των

δεδομένων της επιχείρησης. Είναι απολύτως κατανοητό και αναμενόμενο πολλά πληροφοριακά συστήματα να μην έχουν σχεδιαστεί με τις σωστές προδιαγραφές ώστε να είναι ασφαλή. Η ασφάλεια που μπορεί να επιτευχθεί μέσα από τεχνικά μέσα είναι περιορισμένη, και θα πρέπει να υποστηρίζεται από κατάλληλη διαχείριση και διαδικασίες. Η διαχείριση της ασφάλειας πληροφοριών χρειάζεται συμμετοχή, όχι μόνο από τους εργαζομένους στην επιχείρηση, αλλά και όλους που συνεργάζονται με αυτήν, ενδεχομένως και με ειδικούς εμπειρογνώμονες έτσι ώστε να εξασφαλιστεί το καλύτερο δυνατό αποτέλεσμα. Αναγνωρίζοντας τι είδους έλεγχοι χρειάζονται, και ποιες είναι οι απαιτήσεις της επιχείρησης σε ασφάλεια προχωράμε με προσοχή στη λεπτομέρεια στον προσεχτικό σχεδιασμό της πολιτικής ασφάλειας. Είναι σαφές λοιπόν το ότι στις μέρες μας είναι απαραίτητο να ακολουθείται και να εφαρμόζεται μία πολιτική ασφάλειας εδραιώνοντας έτσι την ασφάλεια σε κάθε δυνατό επίπεδο και παρέχοντας την απαιτούμενη προστασία στην επιχείρηση.

Σκοπός της συγκεκριμένης διπλωματικής εργασίας, είναι η παρουσίαση μερικών από των πιο γνωστών και διεθνώς αποδεκτών μεθόδων μελέτης και διαχείρισης επικινδυνότητας και στη συνέχεια η πρόταση κριτηρίων αξιολόγησής τους. Από τη βιβλιογραφική έρευνα ανέκυψε ο προβληματισμός ότι δεν υπάρχει ένα ευρέως αποδεκτό πλαίσιο για την αξιολόγηση των μεθόδων και των χαρακτηριστικών τους. Το πλαίσιο των κριτηρίων που προτείνεται είναι προϊόν της βιβλιογραφικής ανασκόπησης για τη μελέτη επικινδυνότητας τόσο στην επιστήμη της πληροφορικής όσο και στις κοινωνικές και οικονομικές επιστήμες.

Ακόμα, όμως, και σε ένα πλαίσιο κριτηρίων αξιολόγησης γίνεται φανερό ότι κάποιο κριτήριο μπορεί να έχει διαφορετική βαρύτητα από κάποιο άλλο για τον αναλυτή ή για τον οργανισμό. Επομένως μπορεί να ληφθεί υπόψη σε μεγαλύτερο (ή μικρότερο) βαθμό. Για την επιλογή κριτηρίων (και εν συνεχείᾳ μεθόδων) βάσει βαρύτητας των κριτηρίων γίνεται παρουσίαση της μεθόδου Analytical Hierarchical Process (AHP), και δίνεται αναλυτικό παράδειγμα εφαρμογής της.

Τέλος, επιχειρείται μια αναλυτική σύγκριση των μεθόδων CRAMM (με το ομώνυμο εργαλείο) και MAGERIT (με το εργαλείο PILAR). Η σύγκριση αυτή κρίνεται ιδιαίτερα σκόπιμη, καθώς η μέθοδος MAGERIT αποτελεί μία από τις πιο αποτελεσματικές και ευέλικτες μεθόδους στον τομέα. Τέλος, παρουσιάζεται ενδεικτικά ένα υπόδειγμα (template), που θα μπορούσε να αποτελέσει μελλοντικά

πρότυπο για τις μελέτες που διεξάγονται με τη χρήση της μεθόδου MAGERIT και του εργαλείου της PILAR.

Συνοπτικά ο σκοπός της διπλωματικής κινήθηκε στους παρακάτω άξονες:

- Αναγκαιότητα και νομοθετικό πλαίσιο μελέτης επικινδυνότητας.
- Μέθοδοι μελέτης επικινδυνότητας.
- Πρόταση κριτηρίων για την αξιολόγηση των μεθόδων.
- Επιλογή κριτηρίων βάσει AHP.
- Σύγκριση μεθόδων CRAMM και MAGERIT (και εργαλείων CRAMM και PILAR αντίστοιχα).
- Υπόδειγμα μελέτης περίπτωσης με το εργαλείο PILAR.

Executive Summary

The problem of IT security was always critical. Undoubtedly, today the risk is more evident, as the systems are exposed to a wide range of users and, therefore, risk. The information, whatever its form, is required to maintain adequate and properly protected. This is the ultimate purpose of information security: to protect the information from a wide range of threats by providing assurance to the business community, minimizing the loss of business and increasing profit from investments and business opportunities. The security of their systems and their data is defined in three dimensions: confidentiality, integrity, availability.

The value of the assets of a company comes from data. Inevitably, the reliance on the information systems and services means organizations are more vulnerable to security threats. The data, the information, the supportive processes, the systems and the networks are important business assets, thus preserving them can help the companies avoid immense problems which may arise. The rapid development and growth of companies make them a more intriguing target so the information systems and networks have to face threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism or physical threats like fire. Sources of damage such as computer viruses and computer hacking have become more and more common and more ambitious while they require impressive skills. Consequently, information security is a necessity in the companies.

At this point the question arises: what procedures and what mechanisms should a company adopt in order to ensure its integrity and protect its data? Theoretically we understand that controls and procedures should be implemented in order to ensure the consistency of the company's data. It is quite understandable and that many information systems have not been designed with the correct specifications in order for them to be safe. The security which can be achieved through technical means is limited, and should be supported by appropriate management and procedures. The management of information security requires involvement not only by the employees concerned, but also from those who cooperate with it, including appropriate experts to ensure the best possible result. Recognizing what controls are needed, and what are the requirements of the operation to safely it is possible to proceed, with attention to detail, in careful security policy design. It is clear, therefore, that nowadays it is

necessary to follow and implement security policies at every level and providing the necessary protection to the business.

The purpose of this thesis is the presentation of some of the most famous and internationally acceptable methods of risk management and then the proposal of a framework with criteria for evaluation of these methods. From the literature review, it is obvious that there is not a widely accepted framework for the evaluation of methods and their special features. The framework of the criteria which is proposed is a product of the literature review in both computer science and the social and economic sciences.

However, it becomes obvious that a criterion may have a different weight than another to the analyst or the body. Therefore, it should be taken into account to a greater (or lesser) degree. For the selection of the criteria (and subsequent methods) the method Analytical Hierarchical Process (AHP) is presented, and a detailed example of application is given.

Finally, an in depth comparison of methods CRAMM (with the homonymous tool) and MAGERIT (with PILAR tool) is presented. This comparison is particularly important, as the MAGERIT method is one of the most effective and flexible methods in the field. Finally, a template is introduced, which could be a model for future studies which are conducted using the MAGERIT method and tool of PILAR.

In summary, the purpose of diplomatic focused on the following areas:

- Necessity and legislative framework of risk assessment and risk management.
- Methods of risk assessment and risk management.
- Suggested criteria for the evaluation of methods.
- Selection of criteria based on AHP.
- Comparison of methods CRAMM and MAGERIT (and CRAMM tools and PILAR respectively).
- Case study model with PILAR tool.

1. Εισαγωγή

1.1 Αντικείμενο διπλωματικής εργασίας

Ένας οργανισμός/υπηρεσία προκειμένου να έχει τη δυνατότητα να επιτυγχάνει τους στόχους του θα πρέπει, μεταξύ άλλων, να διασφαλίσει όσο το δυνατό καλύτερα την απαιτούμενη ασφάλεια της υπολογιστικής υποδομής του καθώς και των ευαίσθητων δεδομένων (βάσει νομικών υποχρεώσεων ή λόγω της φύσης του οργανισμού) που αποθηκεύονται ή διακινούνται σε αυτή. Το πρόβλημα της ασφάλειας των πληροφοριακών συστημάτων ήταν πάντα κρίσιμο. Αναμφισβήτητα, σήμερα ο κίνδυνος είναι πιο συνειδητός, καθώς τα συστήματα εκτίθενται σε ευρύ φάσμα χρηστών και συνεπώς κινδύνων.

Η πληροφορία, οποιαδήποτε και αν είναι η μορφή της, εφόσον είναι σημαντική απαιτείται να διαφυλάσσεται κατάλληλα και να είναι σωστά προστατευμένη. Αυτός είναι ο απότερος σκοπός της ασφάλειας πληροφοριών: να προστατεύει την πληροφορία από ένα ευρύ φάσμα απειλών παρέχοντας εξασφάλιση στην επιχειρηματική κοινωνία, ελαχιστοποιώντας τη ζημία των επιχειρήσεων και αυξάνοντας το κέρδος από επενδύσεις και επιχειρηματικές ευκαιρίες. Η εφαρμογή ενός σχεδίου ασφάλειας σήμερα, σύμφωνα με διεθνείς μεθόδους και πρακτικές, αντιμετωπίζεται σαν μία σημαντική διαχειριστική λειτουργία και όχι απλά ως μία τεχνική λειτουργία.

Για τη μελέτη και την εκπόνηση ενός αποτελεσματικού σχεδίου, απαιτείται η χρήση της κατάλληλης μεθόδου μελέτης επικινδυνότητας. Ωστόσο, υπάρχει πληθώρα μεθόδων, καθεμιά από τις οποίες έχει ιδιαίτερα χαρακτηριστικά τα οποία την καθιστούν πιο ικανή να ανταπεξέλθει στις εκάστοτε συνθήκες που επικρατούν σε ένα οργανισμό.

Σκοπός της συγκεκριμένης διπλωματικής εργασίας, είναι η παρουσίαση μερικών από των πιο γνωστών και διεθνώς αποδεκτών μεθόδων μελέτης και διαχείρισης επικινδυνότητας και στη συνέχεια η πρόταση κριτηρίων αξιολόγησής τους. Από τη βιβλιογραφική έρευνα ανέκυψε ο προβληματισμός ότι δεν υπάρχει ένα ευρέως αποδεκτό πλαίσιο για την αξιολόγηση των μεθόδων και των χαρακτηριστικών τους. Το πλαίσιο των κριτηρίων που προτείνεται είναι προϊόν της βιβλιογραφικής

ανασκόπησης για τη μελέτη επικινδυνότητας τόσο στην επιστήμη της πληροφορικής όσο και στις κοινωνικές και οικονομικές επιστήμες.

Ακόμα, όμως, και σε ένα πλαίσιο κριτηρίων αξιολόγησης γίνεται φανερό ότι κάποιο κριτήριο μπορεί να έχει διαφορετική βαρύτητα από κάποιο άλλο για τον αναλυτή ή για τον οργανισμό. Επομένως μπορεί να ληφθεί υπόψη σε μεγαλύτερο (ή μικρότερο) βαθμό. Για την επιλογή κριτηρίων (και εν συνεχείᾳ μεθόδων) βάσει βαρύτητας των κριτηρίων γίνεται παρουσίαση της μεθόδου Analytical Hierarchical Process (AHP), και δίνεται αναλυτικό παράδειγμα εφαρμογής της.

Τέλος, επιχειρείται μια αναλυτική σύγκριση των μεθόδων CRAMM (με το ομώνυμο εργαλείο) και MAGERIT (με το εργαλείο PILAR). Η σύγκριση αυτή κρίνεται ιδιαίτερα σκόπιμη, καθώς η μέθοδος MAGERIT αποτελεί μία από τις πιο αποτελεσματικές και ευέλικτες μεθόδους στον τομέα. Τέλος, παρουσιάζεται ενδεικτικά ένα υπόδειγμα (template), που θα μπορούσε να αποτελέσει μελλοντικά πρότυπο για τις μελέτες που διεξάγονται με τη χρήση της μεθόδου MAGERIT και του εργαλείου της PILAR.

Συνοπτικά ο σκοπός της διπλωματικής κινήθηκε στους παρακάτω άξονες:

- Αναγκαιότητα και νομοθετικό πλαίσιο μελέτης επικινδυνότητας.
- Μέθοδοι μελέτης επικινδυνότητας.
- Πρόταση κριτηρίων για την αξιολόγηση των μεθόδων.
- Επιλογή κριτηρίων βάσει AHP.
- Σύγκριση μεθόδων CRAMM και MAGERIT (και εργαλείων CRAMM και PILAR αντίστοιχα).
- Υπόδειγμα μελέτης περίπτωσης με το εργαλείο PILAR.

1.2 Αφορμή για την έρευνα

Τα τελευταία χρόνια παρατηρείται ότι η αξία των αγαθών μιας εταιρείας προέρχεται κυρίως από άνλα στοιχεία. Αναπόφευκτα, η εξάρτηση στα πληροφοριακά συστήματα και στις υπηρεσίες σημαίνει ότι οι οργανισμοί είναι πιο ευάλωτοι στις απειλές ασφάλειας. Τα δεδομένα, οι πληροφορίες, οι υποστηρικτικές διαδικασίες, τα συστήματα και τα δίκτυα είναι σημαντικά επιχειρηματικά αγαθά, οπότε διαφυλάσσοντάς τα, μια εταιρεία μπορεί να αποφύγει ανυπολόγιστα προβλήματα τα οποία ενδέχεται να προκύψουν. Η αλματώδης ανάπτυξη και αύξηση των εταιρειών συνετέλεσε στο να μετατραπούν σε πιο «θελκτικό» στόχος άρα τα συστήματα

πληροφοριών και τα δίκτυά τους να έχουν να αντιμετωπίσουν απειλές από ένα ευρύ φάσμα πηγών.

Σε αυτό το σημείο εγείρεται το ερώτημα σχετικά με το ποιες διαδικασίες και ποιους μηχανισμούς πρέπει να ακολουθήσει μια επιχείρηση έτσι ώστε να εξασφαλίσει την ακεραιότητά της και να προστατέψει τα δεδομένα της. Σε θεωρητικό επίπεδο είναι κατανοητό ότι θα πρέπει να εφαρμοστούν έλεγχοι και διαδικασίες οι οποίες θα διασφαλίσουν την συνοχή των δεδομένων της επιχείρησης. Είναι απολύτως κατανοητό και αναμενόμενο πολλά πληροφοριακά συστήματα να μην έχουν σχεδιαστεί με τις σωστές προδιαγραφές ώστε να είναι ασφαλή. Η ασφάλεια που μπορεί να επιτευχθεί μέσα από τεχνικά μέσα είναι περιορισμένη και θα πρέπει να υποστηρίζεται από κατάλληλη διαχείριση και διαδικασίες.

Η διαχείριση της ασφάλειας πληροφοριών χρειάζεται συμμετοχή, όχι μόνο από τους εργαζομένους στην επιχείρηση, αλλά και όλους όσους συνεργάζονται με αυτήν, ενδεχομένως και με ειδικούς εμπειρογνώμονες έτσι ώστε να εξασφαλιστεί το καλύτερο δυνατό αποτέλεσμα. Αναγνωρίζοντας τι είδους έλεγχοι χρειάζονται και ποιες είναι οι απαιτήσεις της επιχείρησης σε ασφάλεια προχωράμε με προσοχή στη λεπτομέρεια στον προσεχτικό σχεδιασμό της πολιτικής ασφάλειας. Είναι σαφές, λοιπόν, το ότι στις μέρες μας είναι απαραίτητο να ακολουθείται και να εφαρμόζεται πολιτική ασφάλειας εδραιώνοντας έτσι την ασφάλεια σε κάθε δυνατό επίπεδο και παρέχοντας την απαιτούμενη προστασία στην επιχείρηση.

Καθώς οι περισσότεροι οργανισμοί βασίζουν πλέον ένα μεγάλο μέρος της λειτουργίας τους σε πληροφοριακά συστήματα, η ανάγκη για κατάλληλη ασφάλεια αυξάνεται. Δυστυχώς, είναι δύσκολο να γίνει επιλογή των μέτρων ασφαλείας που χρειάζονται για να επιτευχθεί ικανοποιητική ασφάλεια. Μεγάλες ποσότητες πόρων ξοδεύονται με σκοπό την αποφυγή αποτυχιών. Παρόλα αυτά, τελικά είναι αδύνατο να υπάρξει η εγγύηση ότι το πληροφοριακό σύστημα (ΠΣ) είναι τέλειο, όπως είναι επίσης αδύνατο να προβλεφθεί και να εξαλειφθεί κάθε τι από τον εξωτερικό κόσμο που πιθανόν να απειλήσει το ΠΣ. Αυτό που όμως είναι δυνατό να επιτευχθεί, είναι η μείωση της πιθανότητας εμφάνισης κινδύνου, η οποία θα επιφέρει και ελάττωση της αβεβαιότητας.

Προϋπόθεση για την επίτευξη αυτής της ελάττωσης αποτελεί η εφαρμογή μιας κατάλληλης μεθόδου μελέτης επικινδυνότητας ώστε να επιτευχθεί επαρκής

αναγνώριση και αποτελεσματική αντιμετώπιση των διαφόρων κινδύνων που απειλούν το σύστημα. Όπως διαφαίνεται, η επιλογή της κατάλληλης μεθόδου μελέτης επικινδυνότητας, αποτέλεσε το έναυσμα για την εκπόνηση της παρούσας διπλωματικής εργασίας.

1.3 Σύντομη περιγραφή

Το **κεφάλαιο 1**, το οποίο είναι το τρέχον, παρουσιάζει μια εισαγωγή στο θέμα που μελετάται. Ακόμα, περιλαμβάνει την αφορμή για έρευνα στην παρούσα περιοχή και την οργάνωση της έρευνας σε κεφάλαια.

Στο **κεφάλαιο 2** περιλαμβάνονται έννοιες και ορολογίες που βοηθούν στην περαιτέρω κατανόηση του κειμένου της εργασίας.

Στο **κεφάλαιο 3** παρουσιάζονται τα κύρια χαρακτηριστικά της διαχείρισης επικινδυνότητας. Πιο συγκριμένα, περιλαμβάνονται τα στάδια ανάλυσης, εκτίμηση και αποτίμηση επικινδυνότητας καθώς και η γενική μεθοδολογία διεξαγωγής της διαχείρισης.

Στο **κεφάλαιο 4** παρατίθενται νομικές διατάξεις που σχετίζονται με την ασφάλεια των πληροφοριακών συστημάτων και είναι άρρηκτα συνδεδεμένες με τη διαχείριση της επικινδυνότητας. Επιπρόσθετα, παρουσιάζονται γενικά πρότυπα και γίνεται ιδιαίτερη αναφορά στις πολιτικές προστασίας κρίσιμων υποδομών.

Το **κεφάλαιο 5** επικεντρώνεται στη συνοπτική παρουσίαση μεθόδων μελέτης επικινδυνότητας και κάποιων χαρακτηριστικών τους.

Το **κεφάλαιο 6** περιλαμβάνει μια αναλυτική παρουσίαση της μεθόδου MAGERIT και του εργαλείου PILAR που την υποστηρίζει. Περιγράφονται αναλυτικά τα λειτουργικά βήματα σε κάθε στάδιο της μελέτης και ο τρόπος διεξαγωγής της μελέτης με το εργαλείο.

Στο **κεφάλαιο 7** παρουσιάζεται το πλαίσιο πρότασης κριτηρίων για την αξιολόγηση των μεθόδων. Περιλαμβάνεται η βιβλιογραφική ανασκόπηση και τα κριτήρια που επιλέχθηκαν βάσει της βιβλιογραφικής έρευνας. Παράλληλα, παρουσιάζεται και η μέθοδος AHP για την επιλογή κριτηρίων βάσει συγκεκριμένης στάθμισης.

Το **κεφάλαιο 8** επικεντρώνεται στη σύγκριση των μεθόδων CRAMM και MAGERIT βάσει συγκεκριμένων κριτηρίων.

Τέλος, στο **παράρτημα** περιλαμβάνεται ένα υπόδειγμα για την τεκμηρίωση της μελέτης επικινδυνότητας με τη μέθοδο MAGERIT και το εργαλείο PILAR.

2. Βασικοί ορισμοί

Η προστασία υποδομών βασικό σκοπό έχει να ενισχύσει την ανθεκτικότητα των υποδομών που θεωρούνται απαραίτητες για τη λειτουργία μιας κοινωνίας. Επομένως είναι εξαιρετικά σημαντικό να γνωρίζει κανείς πού και πώς μπορεί να διαταραχθεί η λειτουργία μιας υποδομής αλλά και τι μπορεί να γίνει για να αποφευχθεί αυτό. Ο εντοπισμός των αδύνατων σημείων και των πιθανών συνεπειών αλλά και η επακόλουθη μείωση των κινδύνων σε αποδεκτά επίπεδα αποτελούν τον πυρήνα της διαχείρισης επικινδυνότητας. Ως εκ τούτου, η προστασία υποδομών μπορεί να επωφεληθεί από τις προσπάθειες διαχείρισης επικινδυνότητας υπό την έννοια ότι καταγράφονται οι κίνδυνοι για τους οποίους έχουν ήδη ληφθεί μέτρα καθώς γίνεται η αναγνώριση νέων κίνδυνων στους οποίους συνεχίζει να είναι εκτεθειμένη η υποδομή. Επιπλέον, παρέχουν πληροφορίες για τη σχετική σπουδαιότητα των κινδύνων και πιθανά μέτρα για την αντιμετώπισή τους (αντίμετρα προστασίας).

Ο ορισμός των βασικών χαρακτηριστικών και εννοιών είναι θεμελιώδης για το πλαίσιο της διαδικασίας εκτίμησης κινδύνων στις υποδομές. Οι ορισμοί των επόμενων υποκεφαλαίων βασίζονται σε εκείνους που δόθηκαν από τους Peltier (2005), Whitmann και Mattord (2011), Theoharidou et al. (2009), Γκρίτζαλης κ.ά. (2003), Κάτσικας κ.ά. (2004) και Tohidi (2011).

2.1 Αγαθό

Ένας από τους θεμελιώδεις ορισμούς είναι αυτός του αγαθού (asset). Γενικά, το αγαθό μιας υποδομής είναι εκείνο το στοιχείο που παρουσιάζει κρισιμότητα για την ομαλή λειτουργία της και μπορεί να υποστεί ζημία, βλάβη ή να απειληθεί από κάποιον κίνδυνο. Από πλευράς ασφάλειας, τα αγαθά ορίζονται και κατηγοριοποιούνται με την ευρεία έννοια του όρου, δηλαδή ως ανθρώπινο δυναμικό, πληροφορίες ακόμα και η ίδια η υποδομή. Στις δημόσιες συγκοινωνίες, «άνθρωποι» είναι οι επιβάτες, οι υπάλληλοι, οι επισκέπτες, οι εργολάβοι, οι προμηθευτές, τα μέλη της τοπικής κοινωνίας και άλλα άτομα ή φορείς που έρχονται σε επαφή με το σύστημα. «Πληροφορίες» είναι οι διαδικασίες λειτουργίας και συντήρησης, τα συστήματα ελέγχου και τροφοδοσίας, οι παράμετροι και οι κωδικοί πρόσβασης του δικτύου υπολογιστών καθώς και άλλες αποκλειστικές/ευαίσθητες πληροφορίες.

Η εξέταση των πόρων ενός συστήματος θα πρέπει να καταλήγει σε ιεράρχηση με βάση το ποιος πόρος επιφέρει τις σοβαρότερες συνέπειες για τους ανθρώπους και τη

δυνατότητα του συστήματος να εκτελεί αδιάλειπτα την λειτουργία του. Αυτοί οι πόροι ενδέχεται να απαιτούν μεγαλύτερη ή ειδική προστασία από επιθέσεις. Για τη λήψη απόφασης, το σύστημα πρέπει να λαμβάνει υπόψη τα κάτωθι:

- Την αξία του πόρου περιλαμβανομένης της τρέχουσας αξίας και της αξίας αντικατάστασης.
- Την αξία του πόρου για έναν ενδεχόμενο δολιοφθορέα.
- Τη στρατηγική θέση των πόρων στο σύστημα.
- Πώς, το πότε και το ποιος έχει πρόσβαση και χρησιμοποιεί έναν πόρο.
- Ποιες είναι οι επιπτώσεις για τους πελάτες, τους υπαλλήλους, τους οργανισμούς δημόσιας ασφάλειας και το γενικό κοινό σε περίπτωση απώλειας πόρων.

2.2 Κίνδυνος και Επικινδυνότητα

Κίνδυνος είναι η δυνητική ζημία που μπορεί να προκύψει από κάποια υφιστάμενη διαδικασία ή από κάποιο μελλοντικό γεγονός. Ο κίνδυνος είναι παρών σε κάθε πτυχή της ζωής μας και πολλοί διαφορετικοί κλάδοι επικεντρώνονται σε αυτόν, δεδομένου ότι εφαρμόζεται σε αυτούς. Εναλλακτικά ο κίνδυνος, ο οποίος εκφράζει το ενδεχόμενο για απώλεια, μπορεί να εκφραστεί καλύτερα με την απάντηση των τεσσάρων παρακάτω ερωτήσεων:

1. Τι θα μπορούσε να συμβεί; (Απειλή)
2. Πόσο κακό θα μπορούσε να είναι; (Συνέπειες)
3. Πόσο συχνά μπορεί να συμβαίνει; (Συχνότητα)
4. Τι σιγουριά υπάρχει για τις απαντήσεις στις τρεις παραπάνω ερωτήσεις; (Βαθμός αβεβαιότητας)

Επικινδυνότητα είναι η πιθανότητα μια συγκεκριμένη απειλή να εκμεταλλευτεί μια συγκεκριμένη ευπάθεια. Στον τομέα της ασφάλειας, ο βασικός τύπος που αποτελεί την ανάλυση της Επικινδυνότητα (E) ορίζεται ως το γινόμενο της Πιθανότητας (Π) πραγματοποίησης ενός επεισοδίου ασφάλειας επί το (οικονομικό ή άλλο) Κόστος (K) που θα επιφέρει, δηλαδή

$$E = \Pi * K \text{ ή αλλιώς } B > P * L$$

όπου B = Το κόστος για την πρόληψη μιας απώλειας,

P = Η πιθανότητα να συμβεί μια απώλεια και

L = Το συνολικό κόστος μιας απώλειας.

Το νόημα του τύπου είναι ότι όταν το κόστος της πρόληψης μιας απώλειας είναι μεγαλύτερο από το γινόμενο του κόστους της απώλειας επί την πιθανότητα να συμβεί αυτή τότε η υλοποίηση του μέτρου πρόληψης κρίνεται ως υπερβολική. Στην αντίθετη περίπτωση το μέτρο πρόληψης συμφέρει να υλοποιηθεί. Συνήθως τα μεγέθη υπολογίζονται σε ετήσιες απώλειες και ετήσια πιθανότητα να συμβεί ένα γεγονός. Ο τύπος αυτός αντικατοπτρίζει την κεντρική ιδέα πίσω από κάθε ανάλυση κινδύνων, όχι μόνο για πληροφοριακά συστήματα: την ιδέα του υπολογισμού της πιο συμφέρουσας λύσης.

Ωστόσο ο υπολογισμός του τύπου και η πρακτική του εφαρμογή βρίσκει σημαντικές δυσκολίες. Συγκεκριμένα, ο ακριβής υπολογισμός των τιμών των πιθανοτήτων και του κόστους πρόληψης ή απώλειας δεν είναι πάντα εύκολος ή δυνατός. Για παράδειγμα η αντιστοίχηση των απωλειών με οικονομικά νούμερα δεν είναι πάντα δυνατή διότι πολλές φορές στην ανάλυση κινδύνων αξιολογούνται απώλειες απροσδιόριστες όπως η εικόνα ενός οργανισμού και η εμπιστοσύνη που έχουν οι «πελάτες» του σε αυτόν. Ακόμα και αν δεν χρησιμοποιείται όμως άμεσα, όλες οι μέθοδοι της ανάλυσης κινδύνων βασίζονται πάνω στην λογική του τύπου BPL.

Από άποψη ασφάλειας των πληροφοριακών συστημάτων, η διαχείριση του κινδύνου είναι η διαδικασία κατανόησης και αντιμετώπισης των παραγόντων που μπορεί να οδηγήσουν σε αστοχία της εμπιστευτικότητας, της ακεραιότητας ή/και της διαθεσιμότητας ενός πληροφοριακού συστήματος. Κίνδυνος για την ασφάλεια ενός πληροφοριακού συστήματος είναι η βλάβη σε μια διαδικασία ή οι σχετικές πληροφορίες που προκύπτουν από κάποιο σκόπιμο ή ακούσιο γεγονός που επιδρά αρνητικά στη διαδικασία ή τις σχετικές πληροφορίες.

Ο κίνδυνος στον οποίο εκτίθεται ένα πληροφοριακό σύστημα είναι συνάρτηση της αξίας των περιουσιακών στοιχείων, των ευπαθειών του, των πιθανών απειλών και της φύσης τους, και των επιπτώσεων που μπορεί να προκύψουν.

2.3 Απειλή

Η απειλή (threat) είναι ένας βασικός ορισμός καθώς αποτελεί τον πυρήνα οποιασδήποτε διαδικασίας εκτίμησης κινδύνου. Μια απειλή μπορεί να είναι ένα οποιοδήποτε συμβάν ή περιστατικό που ενδέχεται να προκαλέσει πρόβλημα ή ακόμα και ολοσχερή καταστροφή σε ένα αγαθό ή σύνολο αγαθών.

Ένα μη επιθυμητό γεγονός που μπορεί να προκαλέσει μη διαθεσιμότητα του συστήματος και των υπηρεσιών, τυχαία ή με πρόθεση τη μετατροπή των δεδομένων, την καταστροφή των δεδομένων ή του συστήματος και τέλος μη εξουσιοδοτημένη αποκάλυψη ευαίσθητων πληροφοριών είναι απειλή. Πιο απλά, απειλή είναι το ενδεχόμενο μια πηγή απειλής να ασκήσει (να ενεργοποιηθεί κατά λάθος ή σκόπιμα) μια συγκεκριμένη ευπάθεια. Κάποιες (αλλά όχι όλες) από τις πιθανές απειλές για τα πληροφοριακά συστήματα είναι οι εξής:

- Η Τυχαία Γνωστοποίηση (Accidental Disclosure): Η άνευ αδείας ή τυχαία ελευθέρωση των διαβαθμισμένων, προσωπικών ή ευαίσθητων πληροφοριών.
- Οι πράξεις της Φύσης (Acts of Nature): Όλα τα είδη φυσικών φαινομένων (π.χ. σεισμοί, τυφώνες, ανεμοστρόβιλοι) που μπορούν να βλάψουν ή να επηρεάσουν το σύστημα / εφαρμογή. Οποιαδήποτε από αυτές τις πιθανές απειλές θα μπορούσε να οδηγήσει σε μερική ή ολική διακοπή λειτουργίας, επηρεάζοντας έτσι τη διαθεσιμότητα.
- Η Τροποποίηση του Λογισμικού (Alteration of Software): Μία εκ προθέσεως τροποποίηση, προσθήκη, διαγραφή του λειτουργικού συστήματος ή των προγραμμάτων του συστήματος εφαρμογής, από εξουσιοδοτημένο χρήστη ή μη, που θέτει σε κίνδυνο το απόρρητο, τη διαθεσιμότητα, ή την ακεραιότητα των δεδομένων, τα προγράμματα, το σύστημα και τους πόρους που ελέγχονται από το σύστημα. Αυτό περιλαμβάνει ιομορφικό λογισμικό, όπως είναι οι λογικές βόμβες, οι δούρειοι ίπποι, οι κερκόπορτες, και οι ιοί.
- Η Χρήση εύρους ζώνης (Bandwidth Usage): Η τυχαία ή εσκεμμένη χρήση του εύρους ζώνης των επικοινωνιών για άλλους σκοπούς εκτός αυτών για τους οποίους προορίζεται.
- Οι Ηλεκτρικές παρεμβολές/Διακοπές (Electrical Interference/Disruption): Μια παρέμβαση ή διακύμανση μπορεί να προκύψει ως αποτέλεσμα μιας διακοπής ρεύματος. Αυτό μπορεί να προκαλέσει άρνηση εξυπηρέτησης στους

εξουσιοδοτημένους χρήστες (ανεπάρκεια) ή τροποποίηση των δεδομένων (διακυμάνσεις).

- Η Σκόπιμη αλλοίωση των δεδομένων (Intentional Alteration of Data): Μια σκόπιμη τροποποίηση, προσθήκη, ή διαγραφή των δεδομένων, από εξουσιοδοτημένο χρήστη ή μη, θέτει σε κίνδυνο την εμπιστευτικότητα, τη διαθεσιμότητα ή την ακεραιότητα των δεδομένων που παράγονται, τροποποιούνται, ελέγχονται, ή αποθηκεύονται από συστήματα επεξεργασίας δεδομένων.
- Το Σφάλμα Ρυθμίσεων του Συστήματος (τυχαία) (System Configuration Error (Accidental)): Μια τυχαία λανθασμένη ρύθμιση παραμέτρων κατά την αρχική εγκατάσταση ή αναβάθμιση του υλικού, του λογισμικού, του εξοπλισμού επικοινωνίας ή/και του λειτουργικού περιβάλλοντος.
- Η Δυσλειτουργία/Διακοπή Τηλεπικοινωνιών (Telecommunication Malfunction/Interruption): Κάθε σύνδεση επικοινωνίας, μονάδα ή βλάβη στοιχείου αρκεί για να προκαλέσει διακοπές στη μεταφορά δεδομένων μέσω τηλεπικοινωνιών μεταξύ τερματικών ηλεκτρονικών υπολογιστών, απομακρυσμένων ή κατανεμημένων επεξεργαστών και των τοπικών εγκαταστάσεων υπολογιστών.

2.4 Τρωτότητα

Δεδομένης της ύπαρξης απειλών, η έννοια της ευπάθειας ή τρωτότητας (vulnerability) εισάγεται ως όρος για να περιγράψει την αδυναμία ενός συγκεκριμένου αγαθού καθώς και την ευκολία με την οποία μπορεί να επηρεαστεί από μια συγκεκριμένη απειλή. Όταν ένα αγαθό μπορεί να επηρεαστεί εύκολα από μια απειλή, λέμε ότι αυτός το αγαθό είναι τρωτό σε αυτήν την απειλή. Η εκτίμηση της τρωτότητας αποτελεί αναπόσπαστο τμήμα κάθε πλαισίου εκτίμησης κινδύνων. Στην πραγματικότητα, η κατανόηση των αδύνατων σημείων/ζωνών ενός συστήματος ή ενός δικτύου αποτελεί το πρώτο βήμα για τη βελτίωση της γενικότερης ασφάλειάς του.

Ευπάθεια είναι ένα ελάττωμα ή μια αδυναμία στις διαδικασίες ασφάλειας του συστήματος, το σχεδιασμό, την υλοποίηση, ή τους εσωτερικούς ελέγχους που θα μπορούσαν να ασκηθούν (κατά λάθος ή εσκεμμένα) και έχουν ως αποτέλεσμα την

παραβίαση της ασφάλειας ή την παραβίαση της πολιτικής ασφάλειας του συστήματος. Άλλος ορισμός για την τρωτότητα είναι αδυναμία ή σχεδιαστική ατέλεια σε ένα σύστημα, εφαρμογή ή υποδομή που μπορεί να γίνει αιτία για την παραβίαση της ασφάλειας και της ακεραιότητας του συστήματος.

Ευπάθεια μπορεί να είναι ένα ελάττωμα ή μια αδυναμία, σε κάθε πτυχή του συστήματος. Οι αδυναμίες δεν είναι απλώς λάθη στην τεχνική προστασία που παρέχει το σύστημα. Σημαντικές αδυναμίες συχνά περιέχονται στις τυποποιημένες διαδικασίες λειτουργίας που οι διαχειριστές των συστημάτων εκτελούν, στη διαδικασία που το γραφείο εξυπηρέτησης χρησιμοποιεί για να επαναφέρει κωδικούς πρόσβασης ή για να επανεξετάσει ανεπαρκείς συνδέσεις. Ένας άλλος τομέας όπου τρωτά σημεία μπορούν να εντοπιστούν είναι σε επίπεδο πολιτικής. Για παράδειγμα, η έλλειψη σαφώς καθορισμένης πολιτικής ελέγχου ασφαλείας μπορεί να είναι άμεσα υπεύθυνη για την ύπαρξη ευπάθειας.

Μερικά παραδείγματα των τρωτών σημείων που σχετίζονται με τον σχεδιασμό της έκτακτης ανάγκης/ανάκτησης από καταστροφή είναι τα εξής:

- Να μην έχουν οριστεί με σαφήνεια οδηγίες και διαδικασίες έκτακτης ανάγκης.
- Η έλλειψη ενός δοκιμασμένου, σαφούς, σχεδίου έκτακτης ανάγκης.
- Η απουσία επαρκούς τυπικής εκπαίδευσης έκτακτης ανάγκης.
- Η έλλειψη αντιγράφων ασφαλείας των πληροφοριών (δεδομένων και λειτουργικού συστήματος).
- Οι ανεπαρκείς διαδικασίες ανάκτησης πληροφοριών του συστήματος, για όλους τους χώρους επεξεργασίας (συμπεριλαμβανομένων των δικτύων).
- Η έλλειψη εναλλακτικών τοποθεσιών επεξεργασίας ή αποθήκευσης.
- Η έλλειψη εναλλακτικών υπηρεσιών επικοινωνίας.

2.5 Αντίμετρο

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

2.6 Υποδομή

Ο όρος υποδομή ορίζεται ως «το θεμελιώδες ή το βασικό πλαίσιο λειτουργίας ενός συστήματος ή οργανισμού». Αυτός ο ορισμός προέκυψε ως αποτέλεσμα του έργου της Επιτροπής Προστασίας Κρίσιμων Υποδομών του Προέδρου των Η.Π.Α. Στην έκθεσή της προς τον αμερικανό πρόεδρο τον Οκτώβριο του 1997 (Ellis et al., 1997), η Επιτροπή όρισε την υποδομή ως ένα δίκτυο ανεξάρτητων, κυρίως ιδιόκτητων, τεχνητών και τεχνολογικών συστημάτων και διαδικασιών που λειτουργούν συλλογικά και συνεργατικά με σκοπό να παράγουν και να διανείμουν με συνεχή ροή ουσιώδη αγαθά και υπηρεσίες.

2.6.1 Κρίσιμες υποδομές

Στη μελέτη της, η Επιτροπή Προστασίας Κρίσιμων Υποδομών του Προέδρου των Η.Π.Α (Ellis et al., 1997) επικεντρώθηκε αυστηρά σε οκτώ κρίσιμες υποδομές «των οποίων η μη διαθεσιμότητα ή η καταστροφή θα επέφερε αρνητικές επιπτώσεις στην άμυνα και την οικονομική ασφάλεια». Αυτές οι οκτώ υποδομές είναι οι εξής: τηλεπικοινωνίες, συστήματα παραγωγής ηλεκτρικής ενέργειας, φυσικό αέριο και πετρέλαιο, τράπεζες και χρηματοοικονομικά, μεταφορές, συστήματα ύδρευσης, κυβερνητικές υπηρεσίες και υπηρεσίες έκτακτης ανάγκης.

Η κρίσιμη υποδομή ορίστηκε ως το πλαίσιο ανεξάρτητων δικτύων και συστημάτων που αποτελείται από αναγνωρίσιμους τομείς, θεσμούς (περιλαμβανομένων των ανθρώπων και των διαδικασιών) και δίκτυα διανομής, τα οποία παρέχουν μια αξιόπιστη ροή προϊόντων και υπηρεσιών και είναι απαραίτητα για την άμυνα και την οικονομική ασφάλεια των ΗΠΑ, την ομαλή λειτουργία των κυβερνήσεων σε όλα τα επίπεδα και την κοινωνία στο σύνολό της. Υπό αυτήν την ευρύτερη προοπτική, άλλα παραδείγματα υποδομών (εκτός των οκτώ κρίσιμων υποδομών της Επιτροπής) είναι η γεωργία/τρόφιμα (παραγωγή, αποθήκευση και διάθεση), το διάστημα, πολλά αγαθά (σίδηρος και χάλυβας, αλουμίνιο, τελικά προϊόντα, κ.λπ.), ο τομέας της υγείας και το εκπαιδευτικό σύστημα.

Η εναλλακτική προσέγγιση (Kröger, 2008) του American Heritage Dictionary ορίζει τον όρο «κρίσιμη υποδομή» ως «τα βασικά μέσα, οι υπηρεσίες και οι εγκαταστάσεις που απαιτούνται για τη λειτουργία μιας κοινότητας ή της κοινωνίας, όπως συστήματα μεταφορών και επικοινωνίας, φορείς ηλεκτροδότησης και ύδρευσης και δημόσια

ιδρύματα όπως σχολεία, ταχυδρομεία και φυλακές». Ωστόσο, αυτός ο ορισμός και άλλοι παρόμοιοι ορισμοί είναι αρκετά γενικοί και υπόκεινται σε διαφορετικές ερμηνείες. Στην πράξη, αυτό που θεωρείται υποδομή εξαρτάται κατά πολύ από το πλαίσιο εντός του οποίου χρησιμοποιείται ο όρος. Σε μια έκθεση του 1983, το U.S. Congressional Budget Office όρισε ως «κρίσιμη υποδομή» τις εγκαταστάσεις που έχουν «κοινά χαρακτηριστικά υψηλά επίπεδα κεφαλαίου και δημόσιας επένδυσης σε όλα τα επίπεδα διακυβέρνησης. Εκτός αυτού είναι απόλυτα κρίσιμες για την οικονομική δραστηριότητα μιας χώρας». Συμπεριέλαβε σε αυτήν την κατηγορία αυτοκινητόδρομους, συστήματα δημόσιας συγκοινωνίας, έργα επεξεργασίας υγρών αποβλήτων, υδάτινους πόρους, εναέρια κυκλοφορία, αεροδρόμια και δημοτική ύδρευση (Congressional Budget Office, 1983).

Σύμφωνα με τους (Min et al. 2007) υποδομή ορίζεται ως το «πλαίσιο ανεξάρτητων δικτύων και συστημάτων που αποτελείται από αναγνωρίσιμους τομείς, θεσμούς (περιλαμβανομένων των ανθρώπων και των διαδικασιών) και δυνατότητες κατανομής, οι οποίες παρέχουν μια αξιόπιστη ροή προϊόντων και υπηρεσιών, απαραίτητες για την άμυνα και την οικονομική ασφάλεια των ΗΠΑ, την ομαλή λειτουργία των κυβερνήσεων σε όλα τα επίπεδα και την κοινωνία στο σύνολό της». Από αυτήν την πλευρά, οι υποδομές περιλαμβάνουν τα εξής: γεωργία/τρόφιμα, πόσιμο νερό, τράπεζες και χρηματοοικονομικά, χημική βιομηχανία και επικίνδυνα υλικά, βιομηχανία άμυνας, δημόσια υγεία, υπηρεσίες έκτακτης ανάγκης, ενέργεια, κυβέρνηση, πληροφορίες και τηλεπικοινωνίες και μεταφορές. Μετά την 11η Σεπτεμβρίου, έγιναν κι άλλες σημαντικές προσθήκες όπως τα εθνικά μνημεία, τα ταχυδρομεία και η ναυτιλία και άλλοι συγκεκριμένοι τύποι υποδομής, δημόσιων και εμπορικών πόρων.

Οι Utne et al. (2011) ενσωματώνουν άλλη μια σημαντική πτυχή στον ορισμό των κρίσιμων υποδομών: το γεγονός ότι οι κρίσιμες υποδομές διασυνδέονται εγγενώς και ευρέως μεταξύ τους και παίζουν σημαντικό ρόλο στη διατήρηση της κανονικής λειτουργίας της κοινωνίας (για αυτό και χαρακτηρίζονται «κρίσιμες»). Πιο συγκεκριμένα, αναφέρεται ότι οι κρίσιμες υποδομές είναι τεχνολογικά δίκτυα, όπως παροχή ενέργειας, υπηρεσίες μεταφορών, ύδρευση, παροχή πετρελαίου και αερίου, τράπεζες και χρηματοοικονομικά ιδρύματα και συστήματα πληροφορικής και τηλεπικοινωνιών. Αυτά τα συστήματα είναι ουσιώδη για τη διατήρηση των σημαντικών λειτουργιών μιας κοινωνίας και οι αστοχίες τους μπορούν να

προκαλέσουν σοβαρό πρόβλημα στον πληθυσμό, την οικονομία και την εθνική ασφάλεια. Οι κρίσιμες υποδομές αλληλεπιδρούν σε διάφορα επίπεδα και η πρόκληση προβλήματος σε μία από αυτές ενδέχεται να επηρεάσει τη λειτουργικότητα των άλλων υποδομών. Η σημασία αυτών των υποδομών για την κοινωνία και των επιπτώσεων της διακοπής λειτουργίας τους επιβάλλει τη λήψη μέτρων για την ασφάλεια και την προστασία τους ώστε να μειωθούν οι κίνδυνοι.

Στην Ευρωπαϊκή Ένωση ειδικότερα, υφίστανται αρκετές υποδομές μεταφορών που εάν διαταραχθούν ή καταστραφούν επηρεάζουν δύο ή περισσότερα κράτη-μέλη. Ενδέχεται επίσης η διαταραχή μιας υποδομής μεταφοράς σε ένα κράτος-μέλος να επιφέρει επιπτώσεις σε ένα άλλο κράτος-μέλος. Οι κρίσιμες υποδομές με επίδραση πέραν των εθνικών συνόρων πρέπει να αναγνωρίζονται και να αναδεικνύονται ως διευρωπαϊκές κρίσιμες υποδομές (European Critical Infrastructures ; ECI). Αυτό μπορεί να πραγματοποιηθεί μόνο μέσω μιας κοινής διαδικασίας για την αναγνώριση των ευρωπαϊκών κρίσιμων υποδομών και την εκτίμηση της ανάγκης για βελτίωση της προστασίας τους, όπως διαμορφώθηκε στην οδηγία 114/2008 (COUNCIL DIRECTIVE 2008/114/CE, 2008).

3. Διαχείριση επικινδυνότητας

Η διαχείριση επικινδυνότητας είναι μία καθολική έννοια, εφαρμόσιμη σε όλο σχεδόν το εύρος της ανθρώπινης δραστηριότητας. Στην πλειοψηφία βέβαια των περιπτώσεων αποτελεί μία αδόμητη δραστηριότητα, βασισμένη στην κοινή λογική, την εμπειρία και το ένστικτο.

Οι οργανισμοί που διαθέτουν τους κατάλληλους πόρους για την καλύτερη κατανόηση των κινδύνων που αντιμετωπίζουν και την αποτελεσματικότερη διαχείρισή τους μπορούν όχι μόνο να αποφύγουν «απρόβλεπτες» δυσκολίες, αλλά ταυτόχρονα να απελευθερώσουν πόρους προς άλλες κατευθύνσεις και να επωφεληθούν ευκαιριών (για νέες επενδύσεις), οι οποίες διαφορετικά ενδεχομένως να απορρίπτονταν ως απλά πολύ «επικίνδυνες». Γίνεται έτσι αντίληπτό ότι η οργανωμένη προσπάθεια ανάλυσης και διαχείρισης της επικινδυνότητας έχει να προσφέρει σημαντική βοήθεια στους οργανισμούς όχι μόνο προς την κατεύθυνση αποφυγής και ελέγχου επικίνδυνων καταστάσεων, που σε διαφορετική περίπτωση θα θεωρούνταν απρόβλεπτες, αλλά ταυτόχρονα και προς τη θεώρηση νέων πρακτικών ή προσπαθειών που προσφέρουν σημαντικές ευκαιρίες. Υπό αυτή την οπτική γωνία, είναι σαφές ότι ο κίνδυνος εμπεριέχει τόσο την έννοια της απειλής, όσο και αυτήν της ευκαιρίας (Blakley et al., 2001).

Όσον αφορά στην περιοχή της διαχείριση επικινδυνότητας, παρά την ραγδαία εξέλιξή της τα τελευταία έτη και τον εμπλουτισμό της με ισχυρό επιστημονικό υπόβαθρο και τον καθορισμό συστηματικών διαδικασιών για όλα τα στάδια του κύκλου ζωής ενός έργου, προγράμματος ή συστήματος, η διαχείριση επικινδυνότητας θεωρείτο μέχρι πολύ πρόσφατα σαν μια πρόσθετη διαδικασία (Stoneburner et al., 2002). Τελευταία, έχει ξεκινήσει η αναθεώρηση αυτής της πρακτικής και η πλήρης ενσωμάτωση της διαχείρισης επικινδυνότητας στην αποτελεσματική πρακτική της διαχείρισης έργων και συστημάτων. Η ενσωμάτωση αυτή προσφέρει τη μεγιστοποίηση της ωφέλειας από τη χρήση των διαδικασιών ανάλυσης και διαχείρισης της επικινδυνότητας, καθώς μόνο έτσι δίνεται πραγματικά η δυνατότητα για αυτό που περιγράφηκε προηγουμένως, ήτοι, όχι μόνο την αποφυγή των κινδύνων ή τον μετριασμό των επιπτώσεών τους, αλλά και την πλήρη εκμετάλλευση των ευκαιριών που προσφέρει ένα σύστημα.

3.1 Ανάλυση Επικινδυνότητας

Μια ουσιαστική αφετηρία για την ανάλυση επικινδυνότητας είναι μια δήλωση των στόχων κάθε συστήματος, οι οποίοι μπορούν να χωριστούν σε αποτελέσματα, ενέργειες και χαμηλότερου επιπέδου δραστηριότητες. Στη συνέχεια, είναι σημαντικό να γίνει η επιλογή της μεθόδου διαχείρισης επικινδυνότητας, που θα εφαρμοστεί. Οι υπάρχουσες διαφορετικές μέθοδοι είναι πολυποίκιλες, εάν και οι περισσότερες είναι απλά παραλλαγές μιας γενικής μεθοδολογίας.

Προκειμένου οι διαχειριστές να πάρουν σωστές αποφάσεις για την αποδοχή, αποτροπή ή μείωση των κινδύνων και την υλοποίηση αποδοτικών οικονομικά (cost effective) λύσεων ασφάλειας, είναι αναγκαία η υιοθέτηση μιας μεθόδου που θα αντιμετωπίζει τα θέματα με βάση το κόστος και το όφελος. Με τον καιρό έχει δημιουργηθεί μια πληθώρα διαδικασιών που ήρθαν να καλύψουν διαφορετικές ανάγκες για ανάλυση κινδύνων. Αν και υπάρχουν πολλές διαφορετικές διαδικασίες, η βασική μέθοδος παραμένει η ίδια (Tipton & Krause, 2012).

Η διαχείριση κινδύνων περιλαμβάνει τις διαδικασίες εντοπισμού, ανάλυσης και αντιμετώπισης των κινδύνων σε ένα έργο. Στόχος είναι να προβλεφθούν και να αποφευχθούν οι κίνδυνοι και οι κρίσεις εξαιτίας αυτών που μπορεί να προκύψουν κατά τη διάρκεια υλοποίησης του έργου. Παραδοτέα των διαδικασιών αυτών είναι οι πιθανές αιτίες κινδύνου και κρίσεων, τα συμπτώματα των προβλημάτων, οι μέθοδοι ποσοτικοποίησης και αξιολόγησης των δικτύων, τα σχέδια αντιμετώπισης κρίσεων, οι εφεδρείες, οι νομικές καλύψεις και οι διορθωτικές ενέργειες.

Ανάλυση κινδύνων ενός πληροφοριακού συστήματος είναι η διαδικασία αναγνώρισης και αξιολόγησης των κινδύνων ασφαλείας που εισάγει το σύστημα στη λειτουργία ενός οργανισμού, καθώς και το κόστος των απωλειών που θα προκληθούν σε περίπτωση που δημιουργηθεί πρόβλημα ασφαλείας (Da Veiga & Elof, 2010). Έτσι προσδιορίζεται ο βαθμός κινδύνου του πληροφοριακού συστήματος και οι απαιτήσεις ασφαλείας που υπάρχουν. Υπολογίζεται επιπλέον και το κόστος πρόληψης κάθε απώλειας ώστε να είναι δυνατή μια σωστή αντιμετώπιση των κινδύνων με ορθολογιστικά κριτήρια.

Ένας κίνδυνος αξιολογείται με τον εντοπισμό απειλών και των τρωτών σημείων και στη συνέχεια, με τον προσδιορισμό των πιθανοτήτων και των επιπτώσεων για κάθε κίνδυνο. Δυστυχώς, η εκτίμηση των κινδύνων είναι μια περίπλοκη επιχείρηση,

συνήθως βασισμένη σε ελλιπή ενημέρωση. Υπάρχουν πολλές μέθοδοι με στόχο η επιτρεπόμενη αξιολόγηση των κινδύνων να είναι επαναλήψιμη και να δίνει συνεπή αποτελέσματα.

Η γενική μεθοδολογία αποτελείται από τρία στάδια (Whitmann & Mattord, 2011):

- **Αναγνώριση Επικινδυνότητας (Risk Identification):** Δημιουργία ενός καταλόγου με όλους τους πιθανούς παράγοντες κινδύνου που θα μπορούσε να αντιμετωπίσει ένα σύστημα.
- **Εκτίμηση Επικινδυνότητας (Risk Estimation):** Προσδιορισμός της έκθεσης σε κάθε παράγοντα κινδύνου, βασισμένος στην εκτίμηση της πιθανότητας να συμβεί και της πιθανής επίπτωσής του, ή του βάρους του σε σχέση με τους υπολοίπους και της σοβαρότητάς του.
- **Αποτίμηση Επικινδυνότητας (Risk Evaluation):** Εκτίμηση της αποδοχής κάθε παράγοντα κινδύνου, με σκοπό να αποφασιστεί τι ενέργειες πρέπει να γίνουν.

3.1.1 Αναγνώριση Επικινδυνότητας

Η αναγνώριση επικινδυνότητας είναι η διαδικασία προσδιορισμού των επικίνδυνων γεγονότων, των συνθηκών κάτω από τις οποίες ενδεχομένως παράγονται οι δυσμενείς επιδράσεις και της φύσης αυτών.

Παράγοντες κινδύνου και επιπτώσεις	
Προετοιμασία	<ul style="list-style-type: none">• Συγκέντρωση των στόχων του συστήματος.• Δήλωση όλων των παραδοχών του συστήματος.• Καθορισμός των κριτηρίων για την επιτυχία.
Προσδιορισμός παραγόντων κινδύνου	<ul style="list-style-type: none">• Προβληματισμός για το τι μπορεί να οδηγήσει σε αρνητικές εξελίξεις.• Εξέταση των επακόλουθων παραγόντων κινδύνου.• Ονομασία κάθε παράγοντα κινδύνου.• Ταξινόμηση των παραγόντων κινδύνου, χρησιμοποιώντας κατάλληλες κατηγοριοποιήσεις.
Προσδιορισμός	<ul style="list-style-type: none">• Χρησιμοποίηση της λογικής συνάρτησης:

επιπτώσεων	AN (παράγοντας κινδύνου) ... TOTE (επίπτωση) <ul style="list-style-type: none"> • Εξέταση των επακόλουθων επιπτώσεων. • Ταξινόμηση των επιπτώσεων χρησιμοποιώντας τις σχετικές κατηγοριοποιήσεις.
Τεκμηρίωση παραγόντων κινδύνων	• Δημιουργία καταλόγου των παραγόντων κινδύνου (ανά κλάση) και των επιπτώσεων (ανά κατηγορία).

Πίνακας 1: Παράγοντες κινδύνου και επιπτώσεις

3.1.1.1 Μέθοδοι καταγραφής παραγόντων κινδύνου

Ο προσδιορισμός των παραγόντων κινδύνου για μια σειρά από παρόμοια συστήματα είναι μία επαναληπτική διαδικασία και για αυτόν τον λόγο η εμπειρία και τα ιστορικά αρχεία αποτελούν σημαντικές πηγές πληροφόρησης. Επιπλέον, επειδή είναι το αρχικό και ίσως το πιο βασικό στάδιο όλης της διαδικασίας, υπάρχει μια πληθώρα μεθόδων και εργαλείων για την όσο το δυνατόν πληρέστερη και μεθοδική καταγραφή των επιμέρους παραγόντων κινδύνου. Οι περισσότερες από αυτές περιγράφονται σύντομα στη συνέχεια (McManus, 2012):

Ερωτηματολόγια: Περιλαμβάνουν μία πρότυπη λίστα ερωτήσεων για την αρχική καταγραφή ενός αριθμού παραγόντων κινδύνου. Χρησιμοποιούνται για την συγκέντρωση ιδεών σχετικά με τους σημαντικότερους παράγοντες κινδύνου που αφορούν το σύστημα (Pickard, 2013).

Λίστα/Πίνακας Ελέγχου (Checklist): Είναι μια λίστα όλων των πιθανών περιοχών, όπου ενδέχεται να παρουσιαστούν προβλήματα. Αποτελεί ένα από τα πιο ευρέως χρησιμοποιούμενα μέσα προσδιορισμού των παραγόντων κινδύνου. Είναι διαφορετική για κάθε οργάνωση και δραστηριότητα και για αυτό δεν πρέπει να χρησιμοποιείται ως το μόνο εργαλείο στην αναγνώριση επικινδυνότητας. Απαραίτητη προϋπόθεση για την κατάρτισή της για κάθε οργανισμό είναι η ύπαρξη πλούσιου ιστορικού όσον αφορά στη διαχείριση επικινδυνότητας (Bryman, 2012).

Συνεντεύξεις: Το πρόσωπο που διεξάγει τις ερωτήσεις θα πρέπει κατά προτίμηση να είναι εκτός του οργανισμού, ώστε να εξασφαλίζεται η ουδετερότητα. Οι συνεντευξιαζόμενοι θα πρέπει να είναι άτομα από όλα τα επίπεδα της ιεραρχίας. Οι ερωτήσεις είναι επιθυμητό να είναι προκαθορισμένες και να συζητηθούν λεπτομερώς με τους συνεντευξιαζόμενους (Robson, 2011).

Συσκέψεις για την ανταλλαγή και την ανάπτυξη ιδεών (Brainstorming): Είναι μία τεχνική διασκέψεων, από την οποία μία ομάδα ατόμων προσπαθεί να αναπτύξει και να καταγράψει αυθόρυμητα όσο το δυνατόν περισσότερες ιδέες σε μια συγκεκριμένη περιοχή ενδιαφέροντος. Στο πρώτο στάδιο της διαδικασίας δεν επιτρέπεται καμία συζήτηση, αξιολόγηση ή κριτική των ιδεών, οι οποίες σκόπιμα αναπτύσσονται γρήγορα και αφορούν ευρύ πεδίο θεμάτων. Στόχος της απουσίας της ανάλυσης και της κρίσης σε αυτήν τη φάση είναι η ενθάρρυνση της δημιουργικότητας των εμπλεκομένων. Οι ιδέες μπορούν να αξιολογηθούν συμβατικά σε επόμενο στάδιο των συσκέψεων. Βασικός σκοπός είναι να αναπτυχθεί ένας περιεκτικός κατάλογος επικίνδυνων ενδεχομένων. Μπορεί να είναι χρήσιμες στην περίπτωση συστημάτων που περιλαμβάνουν νέους/σπάνιους παράγοντες κινδύνου ή καινοτόμες διοικητικές ρυθμίσεις ή για την ανάπτυξη των πινάκων ελέγχου (McManus, 2012).

Μητρώο Παραγόντων Κινδύνου (Risk Register/ Risk Log): Αναφέρεται σε ένα συγκεκριμένο πίνακα, όπου καταγράφονται όλοι οι παράγοντες κινδύνου που έχουν προσδιοριστεί. Επιπρόσθετα, γίνεται καταγραφή στοιχείων σχετικά με την εκτίμηση και την αξιολόγηση των επιμέρους παραγόντων κινδύνου. Η χρήση του διευκολύνεται με την ανάπτυξη μίας εφαρμογής υπολογιστών για την ταχύτερη και πληρέστερη εισαγωγή των στοιχείων στα πεδία και τη δημιουργία μίας συνοπτικής κατανομής παραγόντων κινδύνου (Summary Risk Profile, SRP) (Smith et al., 2013).

Δομή Αναλυτικής Παράθεσης Παραγόντων Κινδύνου (Risk Breakdown Structure): Ταξινόμηση των παραγόντων κινδύνου, προσανατολισμένη στην προέλευσή τους, όπου κάθε επόμενο επίπεδο παρουσιάζει πιο λεπτομερή καταγραφή των αιτιών. Βοηθάει στην αντίληψη της κατανομής και του τύπου των παραγόντων κινδύνου σε ένα σύστημα. Παρέχει μία τυποποιημένη παρουσίαση των παραγόντων κινδύνου του συστήματος, διευκολύνοντας την κατανόηση, την επικοινωνία και τη διαχείριση. Τα πρώτα επίπεδα μπορούν να χρησιμοποιηθούν σαν μία άμεση λίστα για την εξασφάλιση της πληρέστερης καταγραφής των ενδεχόμενων παραγόντων κινδύνου (Speier et al., 2011).

Ανάλυση Δυνατών και Αδύνατων Σημείων, Ευκαιριών και Απειλών (SWOT): Αποτελεί ένα μοντελοποιημένο τρόπο καταγραφής των κυριότερων συμπερασμάτων που προκύπτουν από την ανάλυση και την καταγραφή του εσωτερικού και εξωτερικού περιβάλλοντος του εξεταζόμενου οργανισμού. Απότερος στόχος της είναι η συμβολή στον καθορισμό των στρατηγικών κατευθύνσεων του οργανισμού.

Συνίσταται από τις εξής τέσσερις εξίσου σημαντικές παραμέτρους: Δυνατά Σημεία, Αδύνατα Σημεία, Ευκαιρίες και Απειλές. Οι δύο πρώτες παράμετροι (Δυνατά και Αδύνατα Σημεία) καθορίζονται από την ανάλυση του εσωτερικού περιβάλλοντος και αφορούν αποκλειστικά στον προσδιορισμό των πλεονεκτημάτων ή μειονεκτημάτων που πηγάζουν από την υφιστάμενη δομή και λειτουργική ευρωστία του οργανισμού. Αντίθετα, οι δύο τελευταίες παράμετροι (Ευκαιρίες και Απειλές) αφορούν στην αξιολόγηση των εξωτερικών παραγόντων, οι οποίοι συνιστούν το εξωτερικό περιβάλλον στο οποίο δραστηριοποιείται ο οργανισμός (Nikroo et al., 2013).

Χάρτης Αντίληψης Παραγόντων Κινδύνου (Risk Concept Map): Αποτελεί μια γραφική απεικόνιση των ενδεχόμενων παραγόντων κινδύνου. Συσχετίζει τα αίτια με τα αντίστοιχα επικίνδυνα γεγονότα και αποτελέσματα. Παράλληλα, παρουσιάζει τους παράγοντες κινδύνου με κριτήριο την αύξηση της σοβαρότητας τους (Wood et al., 2012).

Διάγραμμα Αιτίας - Επίδρασης (Cause-Effect Diagram): Παρουσιάζει γραφικά τις σχέσεις μεταξύ των αιτιών και των επιδράσεων. Δεν εμπεριέχει μεγέθη που να ποσοτικοποιούν τα αίτια και τις επιδράσεις (Curcin et al., 2014).

Ανάλυση παραδοχών: Κάθε σύστημα συλλαμβάνεται και αναπτύσσεται βασιζόμενο σε ένα σύνολο σεναρίων και παραδοχών. Η ανάλυση παραδοχών είναι μια τεχνική που εξερευνά την ακρίβεια των παραδοχών και προσδιορίζει τους παράγοντες κινδύνου για το σύστημα από την ανακρίβεια, την ασυνέπεια ή την ατέλεια των παραδοχών αυτών. Η ταξινόμηση των παραγόντων κινδύνου παρέχει την δυνατότητα της παρακολούθησης και ένταξής τους στις ίδιες στρατηγικές αντιμετώπισης ανάλογα με τις κατηγορίες στις οποίες ανήκουν. Αυτή μπορεί να γίνει με βάση (McManus, 2012):

- Την αιτία.
- Το αν απορρέουν από την εσωτερική λειτουργία του προγράμματος ή από εξωτερικούς παράγοντες.
- Το στάδιο υλοποίησης του προγράμματος στο οποίο ενδέχεται να συμβούν.
- Την πιθανότητα να συμβούν ή το βάρος τους σε σχέση με τους υπολοίπους.
- Το μέγεθος των επιπτώσεων ή της σοβαρότητάς τους εάν εμφανιστούν.
- Το αν χαρακτηρίζονται ως ελέγχιμοι ή όχι.

Επιπρόσθετα, ενδέχεται να κριθεί χρήσιμη και η κατηγοριοποίηση των επιπτώσεων που παρουσιάζονται αν συμβεί το αρνητικό ενδεχόμενο. Αυτή μπορεί να γίνει με βάση τα κάτωθι χαρακτηριστικά:

- Χρόνος.
- Κόστος.
- Επίτευξη / εκτέλεση / ποιότητα.
- Υγιεινή και ασφάλεια.
- Περιβάλλον.
- Πολιτική.

3.1.2 Εκτίμηση Επικινδυνότητας

Η εκτίμηση επικινδυνότητας πραγματοποιείται γενικά με τη χρήση δύο μεθόδων. Η μία μέθοδος συνίσταται στη διαδικασία εκτίμησης του βάρους των παραγόντων κινδύνου σε σχέση με τους υπολοίπους και της σοβαρότητάς τους σε περίπτωση που εμφανιστούν. Η άλλη μέθοδος, συνίσταται στη διαδικασία εκτίμησης της πιθανότητας εμφάνισης των επικινδυνών γεγονότων και της δριμύτητας των επιδράσεών τους. Αυτό οδηγεί σε μια εκτίμηση του βαθμού έκθεσης του συστήματος σε κίνδυνο (Munteanu, 2006).

Υπάρχει ένας πολύ μεγάλος αριθμός από τεχνικές εκτίμησης κινδύνων. Γενικά όμως υπάρχουν δύο μεγάλες κατηγορίες: Η ποσοτική (quantitative) και η ποιοτική (qualitative).

3.1.2.1 2.1 Ποσοτική αξιολόγηση

Η ποσοτική εκτίμηση των κινδύνων αξιοποιεί τις μεθόδους που χρησιμοποιούνται από οικονομολογικά ιδρύματα και ασφαλιστικές εταιρείες. Αναθέτοντας τιμές στις πληροφορίες, τα συστήματα, τις επιχειρηματικές διαδικασίες, το κόστος ανάκτησης, κ.λπ., οι επιπτώσεις και επομένως ο κίνδυνος, μπορούν να μετρηθούν από άποψη άμεσων και έμμεσων δαπανών (Kaplan & Garrick, 1981).

Η ποσοτική ανάλυση προσπαθεί να προσδιορίσει αντικειμενικές αριθμητικές τιμές (πχ. χρηματικά ποσά) για κάθε συνιστώσα της ανάλυσης κινδύνων. Για παράδειγμα προσπαθεί να υπολογίσει την χρηματική αξία των απωλειών ή την πιθανότητα (σε νούμερο) να συμβεί ένα περιστατικό. Στην περίπτωση που «ποσοτικοποιηθούν» όλες οι συνιστώσες (αξία περιουσιακών στοιχείων, συγνότητα απειλών,

αποτελεσματικότητα αντίμετρων, κόστος αντίμετρων, αβεβαιότητα και πιθανότητα) τότε η ανάλυση ονομάζεται πλήρως ποσοτική Van Der Sluijs et al., 2005).

Μαθηματικά, ο ποσοτικός κίνδυνος μπορεί να εκφραστεί ως Ετησιοποιημένα Απώλεια Προσδόκιμου (Annualized Loss Expectancy - ALE) και είναι η αναμενόμενη νομισματική ζημία που μπορεί να αναμένεται για ένα κεφάλαιο εξαιτίας του κινδύνου που πραγματοποιείται κατά τη διάρκεια ενός έτους.

$$ALE = SLE * ARO,$$

όπου SLE: Single Loss Expectancy - Ενιαίο Προσδόκιμο Απώλειας και ARO: Annualized Rate of Occurrence - Ετησιοποιημένος Ρυθμός εμφάνισης.

Από μαθηματικής άποψης, αυτό γίνεται περίπλοκο πολύ γρήγορα, με τη συμμετοχή στατιστικών τεχνικών. Ενώ η χρήση ποσοτικής εκτίμησης του κινδύνου φαίνεται απλή και λογική, υπάρχουν θέματα με τη χρήση της με τα συστήματα πληροφοριών. Ενώ το κόστος ενός συστήματος μπορεί να είναι εύκολο να καθοριστεί, το έμμεσο κόστος, όπως η αξία των πληροφοριών, η χαμένη παραγωγική δραστηριότητα και το κόστος ανάκτησης είναι ατελώς γνωστά στην καλύτερη περίπτωση. Επιπλέον, το άλλο σημαντικό στοιχείο του κινδύνου, η πιθανότητα, συχνά είναι επίσης άγνωστη (Punch, 2013).

Για τον υπολογισμό με αριθμητικό τρόπο των πιθανοτήτων εμφάνισης των παραγόντων κινδύνου και των επιπτώσεών τους, εφ' όσον εμφανιστούν, είναι απαραίτητη η ύπαρξη ενός πολύ πλούσιου και καλά ενημερωμένου ιστορικού από την διαχείριση αντίστοιχων συστημάτων σε βάθος χρόνου. Επιπλέον, για να είναι εφικτό οι αριθμητικές τιμές που θα προσδιοριστούν για τις πιθανότητες και τις επιπτώσεις των παραγόντων κινδύνου να μπορούν να χρησιμοποιηθούν για πράξεις μεταξύ τους, προκειμένου να υπολογιστεί αριθμητικά η σοβαρότητα κάθε παράγοντα και η συνολική έκθεση σε κίνδυνο, θα πρέπει να ισχύουν οι ακόλουθες προϋποθέσεις (Suh & Han, 2003):

- Τα κόστη να είναι αθροιστικά, δηλαδή το συνολικό κόστος να μπορεί να υπολογιστεί ως το αριθμητικό άθροισμα των επιμέρους.
- Ο χρόνος να είναι επίσης άθροισμα των επιμέρους χρόνων (αυτό συμβαίνει στις διαδοχικές δραστηριότητες).
- Οι παράγοντες κινδύνου να μπορούν να συμβαίνουν ανεξάρτητα.

Ως εκ τούτου, ένα μεγάλο περιθώριο λάθους είναι συνήθως συνυφασμένο με την ποσοτική εκτίμηση του κινδύνου στα πληροφοριακά συστήματα. Αυτό μπορεί να μη

συμβαίνει πάντα ή στο μέλλον. Δεδομένου ότι το σώμα των στατιστικών στοιχείων είναι διαθέσιμο, οι τάσεις μπορούν να επεκτείνουν την εμπειρία του παρελθόντος. Οι ασφαλιστικές εταιρείες και τα χρηματοοικονομικά ιδρύματα κάνουν άριστη χρήση αυτών των στατιστικών προκειμένου να εξασφαλίσουν ότι η ποσοτική αξιολόγηση του κινδύνου τους έχει νόημα, είναι επαναλαμβανόμενη και συνεπής. Τυπικά, δεν είναι οικονομικά αποδοτική για να εκτελέσει μια ποσοτική εκτίμηση του κινδύνου σε ένα πληροφοριακό σύστημα, λόγω της σχετικής δυσκολίας απόκτησης ακριβών και πλήρων πληροφοριών. Ωστόσο, εάν η πληροφορία θεωρείται αξιόπιστη, μια ποιοτική εκτίμηση κινδύνου αποτελεί ένα εξαιρετικά ισχυρό εργαλείο για την ανακοίνωση του κινδύνου σε όλα τα επίπεδα της διοίκησης. Η ποσοτική μέτρηση του κινδύνου είναι η τυπική (Gerber & Von Solms, 2005).

Συμπερασματικά, η ποσοτική μέτρηση του κινδύνου είναι ο συνήθης τρόπος μέτρησης του κινδύνου σε πολλούς τομείς, όπως η ασφάλιση, αλλά δεν χρησιμοποιείται συνήθως για τη μέτρηση του κινδύνου σε πληροφοριακά συστήματα. Δύο λόγοι που συμβαίνει αυτό είναι:

- οι δυσκολίες στον προσδιορισμό και την απόδοση αξίας των κεφαλαίων, και
- η έλλειψη στατιστικών πληροφοριών που θα καθιστούσαν δυνατό τον προσδιορισμό της συχνότητας.

Έτσι, τα περισσότερα από τα εργαλεία αξιολόγησης του κινδύνου που χρησιμοποιούνται σήμερα στα πληροφοριακά συστήματα είναι μετρήσεις του ποιοτικού κινδύνου.

3.1.2.1.1 Εργαλεία ποσοτικού προσδιορισμού του κινδύνου

Στη συνέχεια παρατίθενται τεχνικές και εργαλεία ποσοτικού προσδιορισμού του κινδύνου (McNeil et al., 2010):

- **Υπολογισμοί αναμενόμενης αξίας (expected value calculations)**

Εάν η πιθανότητα του να συμβεί ένα γεγονός είναι pB_{1B} , pB_{2B} , ..., pB_{nB} , και μία αντίστοιχη επίπτωση κόστους εκφράζεται ως cB_{1B} , cB_{2B} , ..., cB_{nB} , τότε η συνολική αναμενόμενη αξία του κινδύνου είναι το άθροισμα των επιμέρους γινομένων. Δηλαδή, ο συνολικός αναμενόμενος κίνδυνος ισούται με: $pB_{1B}cB_{1B}+pB_{2B}cB_{2B}+\dots+pB_{nB}cB_{nB}$.

- **Δένδρα πιθανοτήτων (Probability Trees)**

Τα δέντρα πιθανοτήτων είναι γραφικές αναπαραστάσεις του συνόλου των πιθανών στρατηγικών και μπορούν να είναι χρήσιμα για προγράμματα που απαιτούν διαδοχικές αποφάσεις. Οι διαφορετικές στρατηγικές οδηγούν σε διαφορετικά αποτελέσματα, ανάλογα με τις συνθήκες και τα γεγονότα που λαμβάνουν χώρα.

- **Συνδυασμός κατανομών (Combination of Distributions)**

Σε μερικές περιπτώσεις είναι χρησιμότερο να παρουσιάζονται οι πιθανότητες των επιπτώσεων με τη μορφή στατιστικής κατανομής. Έτσι, αντί η πιθανότητα κινδύνου να έχει μία τιμή μονοσήμαντη, παρουσιάζεται με τη μορφή μιας κατανομής. Αυτό είναι ιδιαίτερα χρήσιμο για τις αβεβαιότητες που έχουν να κάνουν με το κόστος και τα χρονοδιαγράμματα.

- **Ανάλυση ευαισθησίας**

Είναι ο υπολογισμός του τρόπου με τον οποίο διαφορετικά σενάρια όσον αφορά στις τιμές των πιθανοτήτων και των επιπτώσεων ή των βαρών και της σοβαρότητας των παραγόντων κινδύνου θα είχαν επιπτώσεις στις καθαρές παρούσες αξίες (NPVs), τις συνολικές δαπάνες, ή άλλες παραμέτρους του προγράμματος. Συγκεκριμένα, για κάθε αριθμητική τιμή επιλέγεται ο υπολογισμός όλων των παραμέτρων με βάση την διακύμανσή αυτής της τιμής, είτε προς τα πάνω, είτε προς τα κάτω. Με αυτό τον τρόπο δίδεται η δυνατότητα να εξακριβωθεί ποιες ακριβώς μεταβλητές επιβάλλεται να προσδιορισθούν με μεγάλη ακρίβεια και ποιες όχι. Ως αποτέλεσμα, προσδιορίζεται και η εμπιστοσύνη στους αρχικούς υπολογισμούς, δεδομένου ότι αν όλες οι μεταβλητές (η μικρή μεταβολή των οποίων επηρεάζει σημαντικά όλες τις παραμέτρους του προγράμματος), έχουν προσδιορισθεί με μεγάλη ακρίβεια, τότε αντίστοιχα μεγάλη θα είναι και η εμπιστοσύνη που θα πρέπει να δίδεται στα αποτελέσματα των υπολογισμών, ανεξάρτητα από την ακρίβεια με την οποία έχουν προσδιορισθεί οι υπόλοιπες μεταβλητές. Αντίστροφα, αν κάποια από αυτές τις σημαντικές μεταβλητές έχει προσδιορισθεί με μικρή ακρίβεια, τότε δεν είναι δυνατόν να υπάρξει εμπιστοσύνη στους αρχικούς υπολογισμούς, παρά μόνο σχετική, εφ' όσον συνεκτιμήθουν όλα τα εναλλακτικά σενάρια.

3.1.2.2 Ποιοτική αξιολόγηση

Οι ποιοτικές εκτιμήσεις κινδύνου υποθέτουν ότι υπάρχει ήδη ένας μεγάλος βαθμός αβεβαιότητας στην πιθανότητα και τις αξίες των επιπτώσεων και ορίζουν, κατά συνέπεια τον κίνδυνο, με υποκειμενικό τρόπο ή από ποιοτική άποψη. Όπως και στα θέματα για την ποσοτική αξιολόγηση των κινδύνων, η μεγάλη δυσκολία στην ποιοτική εκτίμηση κινδύνου έγκειται στον υπολογισμό των τιμών των πιθανοτήτων και των επιπτώσεων. Επιπλέον, αυτές οι τιμές πρέπει να οριστούν κατά τρόπο που να επιτρέπει τις ίδιες κλίμακες να χρησιμοποιηθούν με συνέπεια στις πολλαπλές εκτιμήσεις κινδύνου (Fletcher, 2005).

Τα αποτελέσματα των ποιοτικών εκτιμήσεων κινδύνου είναι εγγενώς πιο δύσκολο να κοινοποιηθούν συνοπτικά στη διαχείριση. Η ποιοτική εκτίμηση κινδύνων δίνει συνήθως αποτελέσματα κινδύνου "Υψηλός", "Μέτριος" και "Χαμηλός". Ωστόσο, με την παροχή των πινάκων ορισμού των επιπτώσεων και των πιθανοτήτων και την περιγραφή των επιπτώσεων τους, είναι δυνατόν να κοινοποιηθεί επαρκώς η εκτίμηση στη διαχείριση του οργανισμού.

3.1.2.2.1 Μέθοδος Πιθανότητας - Επίπτωσης

Ποια η πιθανότητα εμφάνισης των παραγόντων κινδύνου;	
Πόσο σοβαρές είναι οι επιπτώσεις τους;	
Πιθανότητα εμφάνισης παράγοντα κινδύνου	<ul style="list-style-type: none"> • Εκτίμηση της πιθανότητας κάθε παράγοντα κινδύνου να συμβεί (ποιοτικά ή ποσοτικά).
Επίπτωση παράγοντα κινδύνου	<ul style="list-style-type: none"> • Εκτίμηση του μεγέθους κάθε επίπτωσης (ποιοτικά ή ποσοτικά).
Έκθεση στον κίνδυνο	<ul style="list-style-type: none"> • Εκτίμηση της συνολικής έκθεσης σε κίνδυνο (ποιοτικά ή ποσοτικά). • Ταξινόμηση των παραγόντων κινδύνου ανάλογα με το βαθμό έκθεσης.
Τεκμηρίωση παραγόντων κινδύνου	<ul style="list-style-type: none"> • Καταγραφή των πιθανοτήτων εμφάνισης, επιπτώσεων και έκθεσης στον κίνδυνο.

Πίνακας 2 - Εκτίμηση Επικινδυνότητας με τη μέθοδο Πιθανότητας-Επίπτωσης

Η πιθανότητα εμφάνισης ενός παράγοντα κινδύνου (probability), αναφέρεται στο ενδεχόμενο ένας συγκεκριμένος παράγοντας να εμφανιστεί πραγματικά κατά τη διάρκεια ζωής του συστήματος. Σε λίγες σχετικά περιπτώσεις είναι δυνατό να υπολογιστεί αριθμητικά η πιθανότητα εμφάνισης ενός παράγοντα κινδύνου. Τις περισσότερες φορές, όμως, υπολογίζεται και εκφράζεται ποιοτικά σύμφωνα με την εμπειρία ή τη διαίσθηση. Οι επιπτώσεις μπορούν επίσης, σε μερικές περιπτώσεις, να υπολογιστούν χρησιμοποιώντας τις ποσοτικές τεχνικές. Όμως, συχνά και αυτές

προκύπτουν από υποκειμενική ποιοτική εκτίμηση βασισμένη στη γνώση τόσο της κατηγορίας του παράγοντα κινδύνου όσο και των λεπτομερειών του ίδιου του συστήματος.

Η έκθεση σε κίνδυνο ορίστηκε με βάση το συνδυασμό της πιθανότητας ενός ενδεχομένου να συμβεί και των επιπτώσεων που θα έχει σε περίπτωση που συμβεί. Εάν οι πιθανότητες και οι επιπτώσεις του παράγοντα κινδύνου έχουν ποσοτικοποιηθεί, η έκθεση σε κίνδυνο (η οποία μετράται με τη σοβαρότητα -severity του εκάστοτε παράγοντα κινδύνου), μπορεί να υπολογιστεί ως το γινόμενο της πιθανότητας και των επιπτώσεων. Εάν ο προσδιορισμός του μεγέθους των πιθανοτήτων και των επιδράσεων δεν είναι δυνατός, τότε τα δύο μεγέθη μπορούν μόνο να συνδυαστούν για να δείξουν την έκθεση σε κίνδυνο χρησιμοποιώντας μια μέθοδο ισοδυναμίας. Οι διαφορετικοί παράγοντες κινδύνου που προσδιορίζονται μπορούν να ταξινομηθούν από την άποψη της πιθανότητας εμφάνισής τους και του μεγέθους των επιπτώσεών τους εάν εμφανιστούν χρησιμοποιώντας μια μήτρα Πιθανότητας/Επιπτώσεων. Από αυτόν τον συνδυασμό της πιθανότητας και των επιπτώσεων ενός παράγοντα κινδύνου προκύπτει η σοβαρότητα (severity) του εκάστοτε παράγοντα. Τέλος, η συνολική έκθεση σε κίνδυνο μπορεί να προσδιοριστεί σαν το πηλίκο του αθροίσματος της σοβαρότητας όλων των παραγόντων κινδύνου δια του πλήθους τους (Zsidisin et al., 2004).

Παρακάτω παρουσιάζονται οι κλίμακες βαθμολόγησης που χρησιμοποιούνται για την εκτίμηση της πιθανότητας εμφάνισης και των επιπτώσεων των παραγόντων κινδύνου, καθώς και η μήτρα Πιθανότητας-Επιπτώσεων:

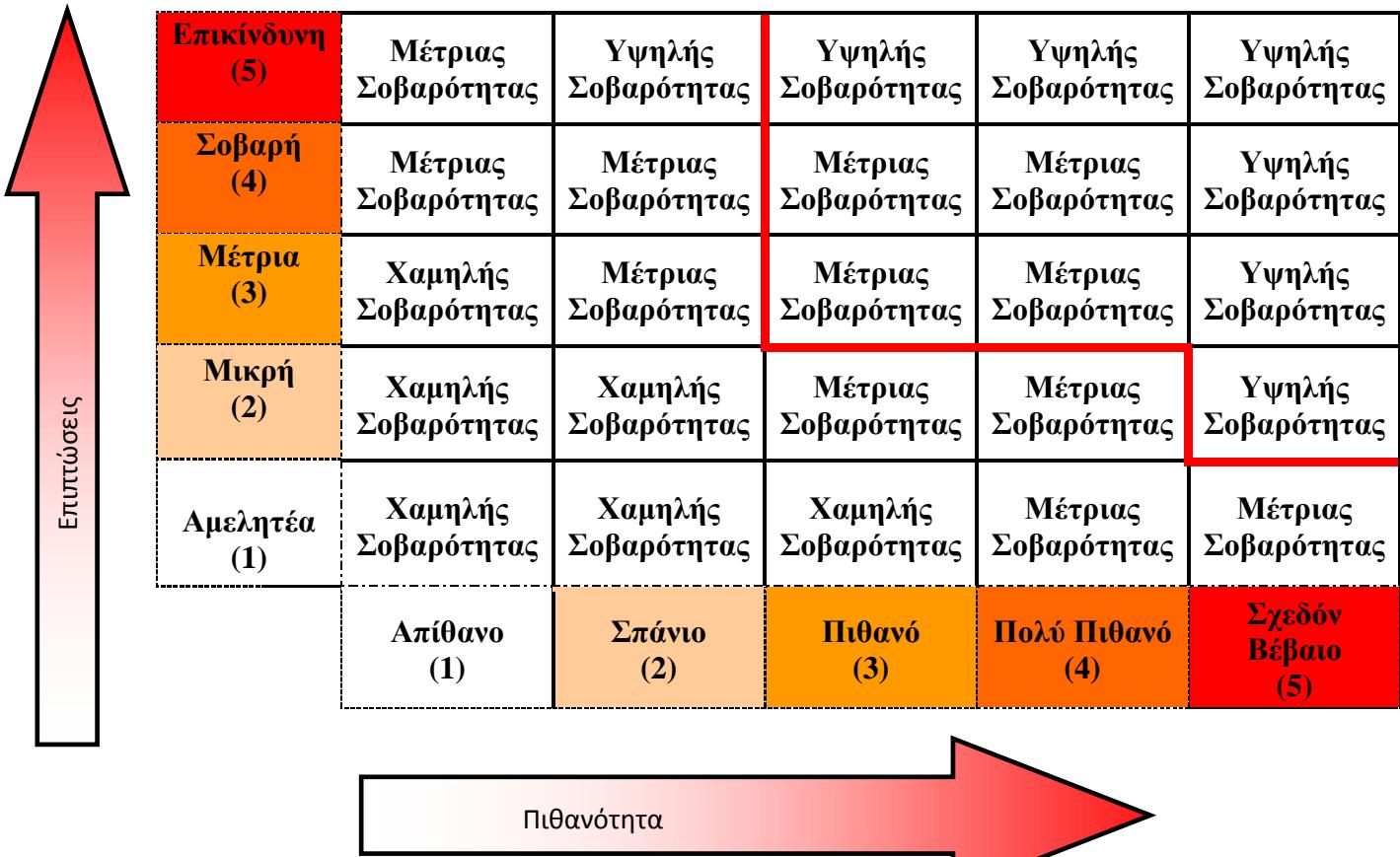
	Απεικόνιση		Ορισμός
5	Σχεδόν Βέβαιο	>80%	Αναμένεται να συμβεί στις περισσότερες περιπτώσεις.
4	Πολύ Πιθανό	51-80%	Ενδεχομένως να συμβεί στις περισσότερες περιπτώσεις.
3	Πιθανό	21-50%	Πιθανώς να συμβεί κάποια στιγμή.
2	Σπάνιο	6-20%	Μπορεί να συμβεί σε μερικές περιπτώσεις.
1	Απίθανο	0-5%	Μπορεί να συμβεί μόνο σε εξαιρετικές περιπτώσεις.

Πίνακας 3 - Εκτίμηση πιθανότητας

	Απεικόνιση	Ορισμός
5	Επικίνδυνη	Εάν συμβεί θα προκαλέσει αποτυχία του προγράμματος.
4	Σοβαρή	Εάν συμβεί θα προκαλέσει σημαντικές επιπτώσεις.
3	Μέτρια	Εάν συμβεί θα προκαλέσει σοβαρές επιπτώσεις, αλλά οι σημαντικοί στόχοι θα επιτευχθούν.

2	Μικρή	Εάν συμβεί θα προκαλέσει κάποιες επιπτώσεις, αλλά σχεδόν όλοι οι στόχοι θα επιτευχθούν.
1	Αμελητέα	Εάν συμβεί δεν θα προκαλέσει επιπτώσεις στο σύστημα.

Πίνακας 4 - Εκτίμηση επιπτώσεων



3.1.2.2.2 Μέθοδος Βάρος-Σοβαρότητα

Σύμφωνα με τη μέθοδο εκτίμησης επικινδυνότητας Πιθανότητα-Επίπτωση που περιγράφηκε προηγουμένως, η πιθανότητα κινδύνου (probability) αναφέρεται στο ενδεχόμενο ένας συγκεκριμένος παράγοντας κινδύνου να εμφανιστεί πραγματικά κατά τη διάρκεια ζωής ενός συστήματος. Όπως αναφέρθηκε, όμως, σε λίγες σχετικά περιπτώσεις είναι δυνατό να υπολογιστεί αριθμητικά η πιθανότητα εμφάνισης ενός παράγοντα. Τις περισσότερες φορές υπολογίζεται και εκφράζεται ποιοτικά σύμφωνα με την εμπειρία ή τη διαίσθηση.

Οι επιπτώσεις (impacts) μπορούν επίσης, σε μερικές περιπτώσεις, να υπολογιστούν χρησιμοποιώντας τις ποσοτικές τεχνικές. Όμως, συχνά και αυτές προκύπτουν από

υποκειμενική ποιοτική εκτίμηση βασισμένη στη γνώση τόσο της κατηγορίας κινδύνου όσο και των λεπτομερειών του ίδιου του συστήματος.

Οι παραπάνω λόγοι, σε συνδυασμό με το μεγάλο πλήθος παραγόντων κινδύνου που συναντάμε σε ένα σύστημα, οδήγησαν στην ανάγκη χρήσης μιας ποσοτικής μεθόδου για την εκτίμηση του κινδύνου. Έτσι, φτάσαμε στη μέθοδο εκτίμησης επικινδυνότητας Βάρος-Σοβαρότητα (Mays & Pope, 2000).

Η εκτίμησης επικινδυνότητας με αυτήν τη μέθοδο, είναι η διαδικασία της εκλογής βαρών για τους παράγοντες κινδύνου και της εκτίμησης της σοβαρότητάς τους. Αυτό οδηγεί σε μια εκτίμηση του βαθμού έκθεσης του έργου/προγράμματος σε κίνδυνο.

Ποιο είναι το βάρος του κάθε παράγοντα κινδύνου; Πόσο σοβαρός είναι;	
Βάρος παράγοντα κινδύνου	<ul style="list-style-type: none">• Επιλογή του βάρους κάθε παράγοντα κινδύνου (ποιοτικά ή ποσοτικά).
Σοβαρότητα παράγοντα κινδύνου	<ul style="list-style-type: none">• Εκτίμηση της σοβαρότητάς του (ποιοτικά ή ποσοτικά).
Έκθεση σε κίνδυνο	<ul style="list-style-type: none">• Εκτίμηση της συνολικής έκθεσης σε κίνδυνο (ποιοτικά ή ποσοτικά).• Ταξινόμηση των συστημάτων ανάλογα με το βαθμό έκθεσης.
Τεκμηρίωση παραγόντων κινδύνου	<ul style="list-style-type: none">• Καταγραφή των βαρών των παραγόντων κινδύνου, της σοβαρότητάς τους και της έκθεσης σε κίνδυνο.

Πίνακας 6 – Εκτίμηση Επικινδυνότητας με τη μέθοδο Βάρος-Σοβαρότητα

Εδώ, η έκθεση σε κίνδυνο ορίζεται με βάση το συνδυασμό του βάρους κάθε παράγοντα κινδύνου και της σοβαρότητας που έχει για το σύστημα. Εάν τα βάρη και οι σοβαρότητες των παραγόντων κινδύνου έχουν ποσοτικοποιηθεί, η έκθεση σε κίνδυνο, η οποία μετράται με την επικινδυνότητα του εκάστοτε συστήματος, μπορεί να υπολογιστεί ως το άθροισμα των γινομένων των βαρών με τις σοβαρότητες των παραγόντων κινδύνου (Baskerville, 1993).

3.1.3 Αποτίμηση Επικινδυνότητας

Η αποτίμηση επικινδυνότητας είναι μία διαδικασία, η οποία έχει ως αντικείμενο την εκτίμηση του βαθμού της αποδοχής της έκθεσης του συστήματος σε κάθε παράγοντα κινδύνου σε σχέση με τα κριτήρια κινδύνου που καθορίζονται για το σύστημα. Διερευνά, επίσης, σε πρώτο επίπεδο και τις αντιδράσεις/μέσα, με τα οποία μπορούν να μειωθούν τα επίπεδα έκθεσης σε κίνδυνο.

Η αποτίμηση επικινδυνότητας είναι ένα ζωτικής σημασίας προαπαιτούμενο βήμα για τη διαχείριση επικινδυνότητας. Χωρίς αυτή, η αποτελεσματική διαχείριση δεν μπορεί να πραγματοποιηθεί, δεδομένου ότι οι υπεύθυνοι δεν θα έχουν γνώση και άποψη για τους σημαντικότερους παράγοντες κινδύνου που θα οδηγήσουν το σύστημα σε αστοχίες. Υπάρχει, επομένως, ο γενικότερος κίνδυνος να διαχειριστούν πρώτα τα προβλήματα με τα οποία αισθάνονται πιο οικείοι, ή με τα οποία έχουν προγενέστερη εμπειρία και να καθυστερήσουν ή να μην προσπαθήσουν να ελέγξουν άλλες σημαντικές δραστηριότητες. Όποια κι αν είναι η περίπτωση, η επιτυχής επίτευξη των στόχων του συστήματος γίνεται πολύ λιγότερο πιθανή (Hong et al., 2003).

Είναι αποδεκτοί οι παράγοντες κινδύνου; Τι μπορεί να γίνει για να μειωθούν;	
Αποδοχή	<ul style="list-style-type: none"> • Καθιέρωση κριτηρίων αποδοχής των παραγόντων κινδύνου. • Εκτίμηση του βαθμού αποδοχής της έκθεσης σε κάθε παράγοντα κινδύνου.
Εναλλακτικές	<ul style="list-style-type: none"> • Μεταφορά : Μεταφορά του παράγοντα κινδύνου σε τρίτους. • Δράση : Εξέταση των μέσων μείωσης της έκθεσης σε αποδεκτά επίπεδα. • Αποφυγή : Αν είναι εφικτό, επιλογή μίας εκ των εναλλακτικών λύσεων, η οποία εξασφαλίζει μηδενικά επίπεδα έκθεσης στον υπό εξέταση παράγοντα κινδύνου.
Τεκμηρίωση παραγόντων κινδύνου	<ul style="list-style-type: none"> • Καταγραφή για κάθε παράγοντα κινδύνου του βαθμού αποδοχής του και των προτεινόμενων εναλλακτικών αντιδράσεων για την αντιμετώπισή του.

Πίνακας 7 - Αποτίμηση Κινδύνου

Εάν η ανάλυση επικινδυνότητας έχει εκτελεσθεί σε ποσοτική βάση, κατόπιν είναι σχετικά εύκολο να συγκριθούν τα αριθμητικά επίπεδα έκθεσης με τα αποδεκτά όρια που εκφράζονται στις ίδιες μονάδες. Για τις ποιοτικές αξιολογήσεις πρέπει να νιοθετηθούν περισσότερο προσεγγιστικές μέθοδοι, όπως είναι η γραμμή ανοχής. Το όριο ανοχής κινδύνου (γραμμή ανοχής), είναι η μέγιστη πιθανή έκθεση σε κίνδυνο, που μπορεί να γίνει αποδεκτή, με βάση τις πιθανές συνέπειες αλλά και τα εμπλεκόμενα οφέλη που σχετίζονται με τις αιτίες των επικινδυνών ενδεχομένων. Το όριο ανοχής αφορά κάθε επιμέρους παράγοντα κινδύνου, αλλά και τη συνολική έκθεση σε κίνδυνο (Vose, 2008).

Για να προσδιοριστεί το όριο ανοχής για κάθε σύστημα, θα πρέπει να εξεταστεί ιδιαίτερα προσεκτικά για κάθε σημαντικό παράγοντα κινδύνου. Ο κίνδυνος ενδέχεται να βρίσκεται έξω από το όριο ανοχής και άρα να αποτελεί αιτία διακοπής του

προγράμματος. Η ανοχή απέναντι σε έναν παράγοντα κινδύνου μπορεί να ποικίλει ανάλογα με την σοβαρότητα του, αλλά και τον χρόνο, όπως και την περιοχή, που ενδέχεται να προκύψει (Kasperson et al., 1988).

3.2 Μεθοδολογία Διαχείρισης Επικινδυνότητας

Στην ανάλυση επικινδυνότητας το κύριο μέλημα είναι να προσδιορισθούν τα μέσα και οι τρόποι για να μειωθεί ο κίνδυνος του συστήματος. Στη διαχείριση της επικινδυνότητας, έμφαση δίνεται στην ανάπτυξη αυτών των ενεργειών, μέσα από μία πιο αναλυτική και λεπτομερή έρευνα της εφικτότητας των μεθόδων για να επιτευχθεί το προσδοκώμενο αποτέλεσμα, χωρίς να υπάρξουν ανεπιθύμητες επιπτώσεις. Στο τέλος αυτού του σταδίου ετοιμάζεται ένα σχέδιο διαχείρισης της επικινδυνότητας.

Οι δυνατότητες που παρέχονται στη διαχείριση επικινδυνότητας ταξινομούνται ουσιαστικά σε τέσσερις μεγάλες κατηγορίες (Cardona, 2004):

- **Αποφυγή κινδύνου:** Πρόκειται για τη χρησιμοποίηση εναλλακτικών προσεγγίσεων, οι οποίες δεν περιέχουν καθόλου κίνδυνο. Αυτή η δυνατότητα, αν και είναι η πιο αποτελεσματική από τις άλλες τεχνικές διαχείρισης κινδύνου, δεν είναι πάντα διαθέσιμη, καθώς σε πάρα πολλές περιπτώσεις είναι πρακτικά αδύνατη η υιοθέτηση μιας στρατηγικής χωρίς καθόλου κίνδυνο. Τέλος, δεν θα πρέπει να παραβλέπεται το γεγονός ότι ο κίνδυνος εμπλέκεται σε πάρα πολλά έργα και προγράμματα, με την προοπτική του κέρδους, καθώς σχεδόν πάντοτε η πορεία προς την υλοποίηση σημαντικών στόχων δεν μπορεί να γίνει χωρίς κίνδυνο.
- **Μεταφορά κινδύνου:** Πρόκειται για τη μεταφορά του κινδύνου σε κάποιο άλλο εμπλεκόμενο μέρος. Πρακτικά, η υλοποίηση αυτής της τακτικής γίνεται με την μεταφορά του κινδύνου μέσα σε μια σύμβαση και άρα με την ανάληψη του κινδύνου από το έτερο συμβαλλόμενο μέρος (outsourcing).
- **Δράση για τον έλεγχο/περιορισμό του κινδύνου:** Πρόκειται για την τακτική, στην οποία υπάγονται οι περισσότεροι παράγοντες κινδύνου. Σε αυτήν εντάσσονται όλες οι δράσεις που στοχεύουν στον περιορισμό, είτε της πιθανότητας εμφάνισης ενός παράγοντα κινδύνου, είτε των συνεπειών από την εμφάνιση ενός παράγοντα κινδύνου. Οι δράσεις περιορισμού του κινδύνου δεν είναι δυνατόν να εξειδικευθούν περαιτέρω σε αυτό το επίπεδο, καθώς εξαρτώνται από την φύση και το είδος του υπό εξέταση παράγοντα κάθε φορά.

- **Αποδοχή κινδύνου:** Πρόκειται για την αποδοχή του κινδύνου, με τον προγραμματισμό καμιάς απολύτως ενέργειας διαχείρισης του. Αυτό είναι δυνατό να συμβεί σε αρκετές περιπτώσεις (που αφορούν βεβαίως μη κρίσιμους για την επιτυχία του προγράμματος παράγοντες κινδύνου), στις οποίες είτε η οποιαδήποτε προγραμματιζόμενη αντίδραση θα έχει μεγαλύτερο κόστος από τις συνέπειες της ενδεχόμενης εμφάνισης του παράγοντα κινδύνου, είτε ο κίνδυνος ελέγχεται εξ' ολοκλήρου από εξωτερικούς παράγοντες στους οποίους υπάρχει αδυναμία παρέμβασης.

Όσο πιο νωρίς ενταχθούν οι διαδικασίες διαχείρισης της επικινδυνότητας στη διαχείριση του συστήματος, τόσο μεγαλύτερα θα είναι τα οφέλη, καθώς είναι φανερό ότι άλλες δυνατότητες παρέχονται για αποτελεσματική διαχείριση της επικινδυνότητας, όταν το σύστημα είναι στην φάση της σύλληψης και του σχεδιασμού του και άλλες δυνατότητες παρέχονται όταν πια βρίσκεται στην διαδικασία εφαρμογής του.

4. Νομοθετικό πλαίσιο των πληροφοριακών συστημάτων

Κάθε οργανισμός οφείλει να συμμορφώνεται με το νομοθετικό πλαίσιο που ορίζει τόσο ο τομέας των δραστηριοτήτων του όσο και η χώρα στην οποία ανήκει. Ιδιαίτερα τα πληροφοριακά συστήματα υπακούουν σε νόμους που σχετίζονται με την ασφάλεια πληροφοριών, το απόρρητο των επικοινωνιών, την προστασία της ιδιωτικότητας και των πνευματικών δικαιωμάτων κ.λπ.

4.1 Πρότυπα

Η κατακτημένη εμπειρία στον αμυντικό τομέα οδήγησε σε καταιγιστική έκδοση προτύπων και αντίστοιχη εισαγωγή και εφαρμογή Συστημάτων Διαχείρισης με πρώτα αυτά της Ποιότητας. Έτσι έχουμε τόσο πρότυπα που είναι τεχνικά όσο και έκδοση προτύπων που δεν είναι τεχνικά, με την έννοια της καταγραφής τεχνικών χαρακτηριστικών που πρέπει να πληροί ένα προϊόν ή του τρόπου ελέγχου τους, αλλά πρότυπα που ορίζουν τις ελάχιστες – διοικητικές και λειτουργικές απαιτήσεις που πρέπει να ικανοποιεί μια επιχείρηση, ώστε να αποδεικνύει πρώτα εσωτερικά και δευτερευόντως προς το εξωτερικό της περιβάλλον, ότι μπορεί να παράγει συνεχώς προϊόντα που ανταποκρίνονται σε δεδομένες προδιαγραφές ανεξάρτητα από που προέρχονται αυτές (πελάτες, νομοθεσία, ίδιες προδιαγραφές ή οποιοσδήποτε συνδυασμός τους).

Ομοίως πρότυπα εμφανίζονται και στη μελέτη και διαχείριση επικινδυνότητας, με τα οποία οι οργανισμοί πρέπει να συμμορφώνονται.

4.1.1 Πρότυπο Information Security Forum (ISF) Standard of Good Practice

Το Forum Ασφάλειας Πληροφοριών (Information Security Forum - ISF) ιδρύθηκε το 1989 και αποτελεί έναν ανεξάρτητο, μη κερδοσκοπικό οργανισμό με μέλη που προέρχονται από σημαντικούς οργανισμούς στον κόσμο. Στοχεύει στην έρευνα, την αποσαφήνιση και την επίλυση βασικών θεμάτων στον τομέα της ασφάλειας των πληροφοριών και τη διαχείριση της επικινδυνότητας, με την ανάπτυξη μεθόδων βάσει βέλτιστων πρακτικών, διαδικασιών και λύσεων που ανταποκρίνονται στις επιχειρηματικές ανάγκες των μελών του. Ο ISF έχει αναπτύξει ένα μοντέλο που δείχνει πώς πρέπει να αντιμετωπίζονται τα θεμελιώδη στοιχεία ενός προγράμματος για την ασφάλεια πληροφοριών. Παρέχει εκπαίδευση στα μέλη του, πρότυπα βέλτιστων πρακτικών και εργαλεία, τα οποία αγγίζουν κάθε πτυχή του μοντέλου

αυτού για να ενισχύσουν τον εκάστοτε οργανισμό στην αντιμετώπιση θεμάτων που έχουν να κάνουν με το περιβάλλον και τους κινδύνους που αντιμετωπίζει.

Στο πλαίσιο των διεθνών προτύπων και των αναγκών των οργανισμών για πιστοποίηση, που αφορά στην ασφάλεια πληροφοριών, ο ISF εξέδωσε το δικό του πρότυπο που ονομάζεται *ISF Standard of Good Practice*. Σήμερα βρίσκεται στην έκδοση 2011 με ένα αρκετά ολοκληρωμένο και περιεκτικό οδηγό που στοχεύει στην οργάνωση του τομέα της Τεχνολογίας και της Πληροφορικής ενός οργανισμού και τον επαρκή έλεγχο αυτού. Περιέχει αναλυτική καθοδήγηση και μεθόδους που ξεκινούν από την ανάλυση της επικινδυνότητας από επιχειρησιακής πλευράς, μεθόδους ανάλυσης και αξιολόγησης των κινδύνων, των απειλών και των αδυναμιών στο τεχνολογικό περιβάλλον, καθώς επίσης και μια εκτενή σειρά από σημεία ελέγχου που κάθε οργανισμός επιλέγει να υλοποιήσει ανάλογα με την ανοχή σε επίπεδα κινδύνου.

Το πρότυπο περιλαμβάνει πέντε οπτικές, κάθε μια από τις οποίες καλύπτει ένα συγκεκριμένο τύπο αξιολόγησης. Οι οπτικές αφορούν στα εξής:

- (i) Διαχείριση της ασφάλειας,
- (ii) Κρίσιμες επιχειρηματικές εφαρμογές,
- (iii) Πληροφοριακή υποδομή,
- (iv) Δίκτυα και
- (v) Ανάπτυξη συστημάτων.

Το πρότυπο του 2011 είναι ο πυρήνας όλων αυτών που παρέχει ο ISF στα μέλη του και αποτελεί τον πυρήνα των εργαλείων και τεχνικών. Επίσης, είναι στενά συνδεδεμένο με τη Μέθοδο Ανάλυσης Επικινδυνότητας των Πληροφοριών του ISF, το λεγόμενο IRAM (Information Risk Analysis Methodology). Ακόμα, καλύπτει πλήρως το φάσμα των διατάξεων ασφάλειας που πρέπει να εφαρμοστούν για να κρατήσει ένας οργανισμός τους επιχειρηματικούς κινδύνους που σχετίζονται με τα συστήματα πληροφοριών εντός των αποδεκτών ορίων και παρουσιάζει πρακτικές για την εφαρμογή τους, με σαφείς προτάσεις. Ωστόσο, το πρότυπο δε στοχεύει μόνο στη βελτίωση της ποιότητας και της αποτελεσματικότητας των διαδικασιών της ασφάλειας των πληροφοριών που εφαρμόζονται από έναν οργανισμό, αλλά λειτουργεί και ως ένα ισχυρό υπόβαθρο προς τη συμμόρφωση της ασφάλειας των πληροφοριών με άλλα διεθνώς αναγνωρισμένα και καθιερωμένα πρότυπα.

Η αναθεώρηση του προτύπου εκσυγχρονίζει το περιεχόμενο και τη δομή του, ενώ παράλληλα ενημερώνει και τις πληροφορίες, καλύπτοντας τις ακόλουθες τέσσερις

βασικές κατηγορίες: (i) διαχείριση της ασφάλειας, (ii) απαιτήσεις ασφάλειας, (iii) πλαίσιο ελέγχου και (iv) παρακολούθηση και βελτίωση. Το ISF standard πραγματεύεται 118 θέματα και σύμφωνα με την ISF, έχει σχεδιαστεί για να βοηθήσει τους οργανισμούς να καλύψουν τις απαιτήσεις από αναγνωρισμένα πρότυπα ασφάλειας στον κόσμο των πληροφοριών, συμπεριλαμβανομένων αυτά των: ISO, COBIT, NIST κ.λπ. Συμπληρώνει και εμπλουτίζει τα πρότυπα αυτά με δεδομένα που προέρχονται από έργα κα κ μέλη του ISF. Σε αντίθεση με άλλα πρότυπα του κλάδου, καλύπτει τα νέα τρέχοντα θέματα της ασφάλειας των πληροφοριών, όπως το υπολογιστικό νέφος, την κοινωνική δικτύωση, την αποθήκευση δεδομένων, τη διαχείριση των ψηφιακών δικαιωμάτων και την εικονικοποίηση. Επιπρόσθετα, παρέχει μεγαλύτερο βάθος και καθοδήγηση για τα υπάρχοντα θέματα προστασίας, όπως η διαρροή πληροφοριών, οι μηχανισμοί ελέγχου πρόσβασης, η επιχειρηματική συνέχεια και η διαχείριση ελέγχου ασφάλειας.

4.1.2 Οικογένεια προτύπων 27000

Η σειρά των ISO/IEC 27000 (που είναι επίσης γνωστή ως 'ISMS Family of Standards' ή 'ISO27k' για συντομία) περιλαμβάνει τα πρότυπα ασφάλειας πληροφοριών που εκδίδονται από το διεθνή οργανισμό πιστοποίησης (ISO) και την International Electrotechnical Commission (IEC).

Η σειρά παρέχει τις καλύτερες συστάσεις σχετικά με τη διαχείριση της ασφάλειας πληροφοριών, τους κινδύνους και τους ελέγχους που πραγματοποιούνται για τα Information Security Management Systems (ISMS). Στην πραγματικότητα αυτά τα πρότυπα καλύπτουν πολλά περισσότερα από την εμπιστευτικότητα και τεχνικά θέματα ασφαλείας. Όλοι οι οργανισμοί ενθαρρύνονται να εκτιμήσουν τους κινδύνους της ασφάλειας πληροφοριών, έπειτα να εφαρμόσουν τους κατάλληλους ελέγχους ασφάλειας πληροφοριών σύμφωνα με τις ανάγκες τους, χρησιμοποιώντας καθοδήγηση και συστάσεις όπου κρίνεται απαραίτητο (Humphreys, 2011).

Τα πρότυπα εφαρμόζονται σε οργανισμούς κάθε είδους και μεγέθους.

- ISO/IEC 27000 – Μία εισαγωγή για την οικογένεια των προτύπων ISMS, και επιπλέον λεξικό με τους συνηθισμένους όρους.
- ISO/IEC 27001 – Πρότυπο με το οποίο οι οργανισμοί μπορούν να πιστοποιηθούν.

- ISO/IEC 27002 – Πρότυπο με καλές συμβουλές πάνω στα ISMS (στο παρελθόν ήταν γνωστό ως το ISO 17799 και πριν από αυτό ήταν το BS 7799 Part 1).
- ISO/IEC 27003 – Οδηγός εφαρμογής του ISMS.
- ISO/IEC 27004 – Πρότυπο για τις μετρήσεις διαχείρισης της ασφάλειας πληροφοριών.
- ISO/IEC 27005 – Πρότυπο για τη διαχείριση των κινδύνων ασφαλείας των πληροφοριών.
- ISO/IEC 27006 – Οδηγός για τη διαδικασία πιστοποίησης/δήλωσης
- ISO/IEC 27007 – Οδηγός για το διαχειριστικό έλεγχο των ISMS (επικεντρώνεται στα συστήματα διοίκησης).
- ISO/IEC 27008 Οδηγός για το διαχειριστικό έλεγχο της ασφάλειας πληροφοριών (Επικεντρώνεται στους ελέγχους ασφαλείας).
- ISO/IEC 27011 – Οδηγός εφαρμογής ISMS για τη βιομηχανία των τηλεπικοινωνιών (είναι επίσης γνωστό ως X.1051).
- ISO/IEC 27031 – Ειδίκευση για την ICT ετοιμότητα για τις επιχειρηματικές δραστηριότητες.
- ISO/IEC 27032 – Οδηγός για την ασφάλεια στο διαδίκτυο.
- ISO/IEC 27033 – Δικτυακή ασφάλεια των πληροφοριακών συστημάτων, ένα πρότυπο με πολλές ενότητες το οποίο είναι στην παρούσα φάση γνωστό ως ISO/IEC 18028:2006.
- ISO/IEC 27034 – Οδηγός για την εφαρμογή ασφαλείας.

Στη συνέχεια αναλύονται τα πιο σημαντικά πρότυπα για τον τομέα της μελέτης επικινδυνότητας.

4.1.2.1 ISO/IEC 27001:2005

Το ISO 27001:2005 αποτελεί ένα διεθνώς αναγνωρισμένο πρότυπο, το οποίο ορίζει τις προδιαγραφές για τη διαχείριση της ασφάλειας πληροφοριών. Το ISO/IEC 27001 είναι μέρος μίας αναπτυσσόμενης οικογένειας των ISO/IEC standards ('ISO/IEC 27000 series') και είναι ένα πρότυπο σύστημα διαχείρισης ασφάλειας πληροφοριών (ISMS) το οποίο εκδόθηκε τον Οκτώβρη του 2005 από το διεθνή οργανισμό πιστοποίησης (ISO) και την International Electrotechnical Commission (IEC). Το πλήρες του όνομα είναι ISO/IEC 27001:2005 - Information technology - Security

techniques - Information security management systems - Requirements αλλά για λόγους συντομίας αναφερόμαστε σε αυτό ως "ISO 27001".

Χρησιμοποιείται σε συνδυασμό με το ISO/IEC 27002, the Code of Practice for Information Security Management, το οποίο βρίσκεται στη λίστα των σκοπών ελέγχου ασφαλείας και συνιστά ένα εύρος συγκεκριμένων ελέγχων ασφαλείας. Οι οργανισμοί οι οποίο θα εφαρμόσουν ένα ISMS είναι πιθανότατα ταυτόχρονα καλυμμένοι για τις απαιτήσεις του ISO/IEC 27001, αλλά η επικύρωση με την πιστοποίηση είναι καθαρά προαιρετική.

Μπορεί να χρησιμοποιηθεί από εταιρείες, οι οποίες επιθυμούν να εγκαταστήσουν και να ενισχύσουν την ασφάλεια διαχείρισης τόσο των δεδομένων τους όσο και των πελατών τους. Το πρότυπο περιέχει 10 θεματικές ενότητες, οι οποίες εξετάζουν τις βασικές περιοχές διαχείρισης πληροφοριών:

Ενότητα	Περιεχόμενο
Πολιτική Ασφάλειας Πληροφοριών	Λεπτομερής κατανόηση των επιχειρησιακών στόχων της εταιρείας και δημιουργία της κατάλληλης πολιτικής ασφάλειας των πληροφοριών.
Υποδομή Ασφάλειας Πληροφοριών	Διαμόρφωση ενός διοικητικού πλαισίου το οποίο χρειάζεται για την έναρξη της εφαρμογής και ελέγχου της ασφάλειας των πληροφοριών μέσα στην εταιρεία.
Κατηγοριοποίηση και Έλεγχος Αγαθών	Λεπτομερής καταγραφή των εταιρικών πόρων και προσδιορισμός του επιπέδου ασφάλειας που απαιτείται για τους πόρους αυτούς.
Ασφάλεια Προσωπικού	Μείωση κινδύνων από ανθρώπινο σφάλμα, κλοπή, απάτη ή κακή χρήση των εταιρικών πόρων, καθώς και διασφάλιση ότι το προσωπικό γνωρίζει την πολιτική ασφάλειας των πληροφοριών και την εφαρμόζει στην καθημερινή εργασία του.
Φυσική και Περιβαλλοντική Ασφάλεια	Αποτροπή της μη εξουσιοδοτημένης πρόσβασης, της ζημίας και της παρέμβασης στις επιχειρησιακές εγκαταστάσεις και τις πληροφορίες καθώς και επίπτωση απώλειας, ζημίας ή και διακοπής στις δραστηριότητες της επιχείρησης.
Διαχείριση Υπολογιστών και	Εξασφάλιση της σωστής και ασφαλούς λειτουργίας

Δικτύου	των δυνατοτήτων επεξεργασίας πληροφοριών, ελαχιστοποίηση του κινδύνου να τεθούν τα συστήματα πληροφορικής εκτός λειτουργίας, προστασία της ακεραιότητας του λογισμικού και των πληροφοριών, εξασφάλιση της προστασίας των πληροφοριών στα δίκτυα και τη σχετική υποδομή.
Έλεγχος Πρόσβασης	Έλεγχος πρόσβασης στις πληροφορίες, εξασφάλιση προστασίας των δικτύων, αποτροπή αναρμόδιας πρόσβασης σε υπολογιστές, ανίχνευση αναρμόδιων δραστηριοτήτων.
Ανάπτυξη και Συντήρηση Συστήματος	Η ενότητα αυτή έχει στόχο να εξασφαλίσει ότι η αναγκαία ασφάλεια εμπεριέχεται στα λειτουργικά συστήματα, να αποτρέψει την απώλεια, την τροποποίηση ή την κακή χρήση των στοιχείων χρηστών εφαρμογών, να εξασφαλίσει ότι τα προγράμματα και οι δραστηριότητες υποστήριξης διευθύνονται με έναν ασφαλή τρόπο.
Σχεδιασμός Συνέχεια Δραστηριοτήτων	Διαμόρφωση τρόπου αντίδρασης σε διακοπές επιχειρησιακών δραστηριοτήτων και κρίσιμων επιχειρησιακών διαδικασιών που είναι αποτελέσματα σημαντικών αποτυχιών ή καταστροφών.
Συμμόρφωση	Αποφυγή παραβιάσεων εγκληματικού ή αστικού δικαίου, νομικών, ρυθμιστικών ή συμβατικών υποχρεώσεων και οποιονδήποτε απαιτήσεων ασφάλειας.

Πίνακας 8: Θεματικές ενότητες ISO/IEC 27001

Η μέθοδος ανάπτυξης του συστήματος με βάση το ISO 27001 περιλαμβάνει τα ακόλουθα βήματα:

- Αρχικά πραγματοποιείται αποτύπωση της υπάρχουσας κατάστασης και η δημιουργία πλαισίου διαχείρισης της πληροφορίας.
- Πραγματοποιείται εκτίμηση επικινδυνότητας και ακολουθεί καθοδήγηση και προσδιορισμός των κατάλληλων ενεργειών για τη διαχείριση της επικινδυνότητας της ασφάλειας των πληροφοριών.

- Ακολουθεί η επιλογή και εφαρμογή των ελέγχων και των ελεγκτικών μεθόδων προκειμένου να επιτευχθεί η μείωση της επικινδυνότητας σε αποδεκτά επίπεδα, τα οποία είναι σύμφωνα με τους στόχους που έχουν τεθεί.
- Στη συνέχεια το σύστημα τίθεται σε λειτουργική εφαρμογή και ακολουθεί υλοποίηση εκπαιδευτικού προγράμματος με στόχο την ενημέρωση των εργαζομένων.
- Κρίνονται αναγκαίες εσωτερικές επιθεωρήσεις συστήματος προκειμένου οι υπεύθυνοι να προβούν σε ενδεχόμενες διορθωτικές προληπτικές ενέργειες για τη βελτίωση του συστήματος.
- Έχοντας ολοκληρώσει τα παραπάνω βήματα, το σύστημα είναι έτοιμο για πιστοποίηση κατά το πρότυπο ISO 27001 από Οργανισμό Πιστοποίησης.
- Τέλος, θα πρέπει να ακολουθήσει εντατική παρακολούθηση του συστήματος.

Συνοπτικά, η πιστοποίηση με το πρότυπο ISO/IEC 27001, συνήθως εμπεριέχει μία διαδικασία με τρία βήματα:

1. Στο πρώτο βήμα γίνεται μία ανασκόπηση της ύπαρξης και της πληρότητας σημαντικών εγγράφων όπως η πολιτική ασφαλείας του οργανισμού, Statement of Applicability (SoA) and Risk Treatment Plan (RTP).
2. Στο δεύτερο βήμα γίνεται ένας λεπτομερής, σε βάθος έλεγχος για την ύπαρξη και την αποτελεσματικότητα των ελέγχων ασφάλειας που δηλώνονται στο SoA και στο RTP καθώς επίσης και τα υποστηρικτικά τους έγγραφα.
3. Στο τρίτο βήμα πραγματοποιείται μία επανεκτίμηση για να επιβεβαιώσει ότι ο οργανισμός ο οποίος έχει ήδη πιστοποιηθεί, παραμένει συμμορφωμένος με το πρότυπο.

Η συντήρηση της πιστοποίησης περιέχει περιοδικές ανασκοπήσεις και επανεκτιμήσεις για να επιβεβαιωθεί ότι το ISMS συνεχίζει να λειτουργεί όπως έχει καθοριστεί.

4.1.2.2 ISO/IEC 27002:2005

Το ISO/IEC 27002:2005 αποτελεί κώδικα πρακτικής για τη διαχείριση της Ασφάλειας Πληροφοριών. Το πρότυπο έχει στόχο τη «θέσπιση» κατευθυντήριων γραμμάτων και των γενικών αρχών για την έναρξη, την υλοποίηση, τη διατήρηση και τη βελτίωση της διαχείρισης της ασφάλειας των πληροφοριών στο πλαίσιο ενός οργανισμού. Περιγράφει μια σειρά από 12 ρήτρες ασφάλειας, καθεμιά με υποκατηγορίες για τις οποίες ελέγχονται οι στόχοι και καθορίζονται οι

κατευθυντήριες γραμμές σχετικά με το πώς μπορεί να εφαρμοστεί ο έλεγχος. Επιπρόσθετα, το ISO/IEC 27002 δίνει μερικές προτάσεις βέλτιστων πρακτικών για τη διεξαγωγή μιας επίσημης μελέτης επικινδυνότητας. Το πρότυπο, επικεντρώνεται στον περιορισμό του κινδύνου και υποστηρίζεται από εκτενείς ταξονομίες, εννοιολογικά μοντέλα και Πλαίσιο Διαχείρισης Επικινδυνότητας (ISO 13335).

Το πρότυπο δεν προσδιορίζει τα επιμέρους βήματα που πρέπει να πραγματοποιηθούν, αλλά καθορίζει το γενικό περίγραμμα στο οποίο πρέπει να συμμορφώνεται η μελέτη επικινδυνότητας. Οι διαδικασίες που πρέπει να αποτελούν μέρος της εκτίμησης κινδύνου σύμφωνα με το πρότυπο ISO/IEC 27002 είναι οι εξής:

1. Ταυτοποίηση των κινδύνων, ποσοτικοποίηση και ιεράρχηση βάσει στόχων που σχετίζονται με τον οργανισμό.
2. Ανάλυση επικινδυνότητας: Εκτίμηση του μεγέθους των κινδύνων που απειλούν τα αγαθά του οργανισμού.
3. Εκτίμηση Επικινδυνότητας: Καθορίζει τη σημαντικότητα των κινδύνων από τη σύγκριση των εκτιμώμενων επιπέδων επικινδυνότητας με χρήση καθορισμένων κριτηρίων.
4. Περιορισμός επικινδυνότητας με τον καθορισμό των κριτηρίων αποδοχής και χρήση τους προκειμένου να αποφανθεί εάν τα προτεινόμενα μέτρα είναι όντως δικαιολογημένα.

4.1.2.3 Σύγκριση ISO/IEC 27001 και 27002

Τα ISO/IEC 27001 και 27002 είναι δύο πλαίσια τα οποία είναι συμπληρωματικά. Το ISO/IEC 27002 παρέχει μια συλλογή των βέλτιστων πρακτικών των ελέγχων που μπορούν να εφαρμοστούν ώστε να υπάρξουν ορατά αποτελέσματα για την προστασία του συστήματος. Το ISO/IEC 27001 περιγράφει την ανάγκη για πόρους, τις διορθωτικές κινήσεις που πρέπει να γίνουν και γενικότερα τη στήριξη που πρέπει να παρέχει η διοίκηση στον οργανισμό. Επομένως, το ISO/IEC 27001 εστιάζει κυρίως στο επίπεδο της διοίκησης, ενώ το ISO 27002 περιλαμβάνει πιο τεχνικά ζητήματα.

Το ISO/IEC 27001 αποτελεί σε μεγάλο βαθμό ένα πρότυπο διαχείρισης, καθώς καθορίζει το σύστημα διαχείρισης ασφάλειας πληροφοριών (ISMS) και τις απαιτήσεις για το πώς μπορεί η ασφάλεια των πληροφοριών να σχεδιαστεί, να εφαρμοστεί, να παρακολουθείται, να αξιολογείται και να βελτιωθεί. Θέτει επίσης διακριτές ευθύνες όπου υπάρχει στοχοθεσία, μέτρηση και αξιολόγηση των αποτελεσμάτων. Επίσης, περιγράφει το πλαίσιο του ελέγχου των αρχείων, των

εγγράφων και των διοικητικών αναθεωρήσεων σε εσωτερικό επίπεδο. Το ISO 27002 περιλαμβάνει τις καλύτερες πρακτικές που πρέπει να εφαρμοστούν.

Χωρίς το πλαίσιο διαχείρισης του ISO/IEC 27001, το ISO/IEC 27002 είναι ένα σύνολο αποσπασματικών διαδικασιών χωρίς αποδοχή από την ανώτερη διοίκηση και χωρίς πραγματικό αντίκτυπο στην οργάνωση του οργανισμού. Ακόμα, εν αποντίᾳ του ISO/IEC 27002, οι έλεγχοι που καθορίζονται στο ISO/IEC 27001 δε θα μπορούσαν να εφαρμοστούν. Επομένως, οι οργανισμοί χρειάζονται ένα πλαίσιο διαχείρισης το οποίο παρέχει το ISO/IEC 27001 και κατευθυντήριες γραμμές εφαρμογής που περιλαμβάνονται στο ISO/IEC 27002. Ο λόγος που τα πρότυπα αυτά παραμένουν ξεχωριστά και δε συνενώνονται σε ένα ενιαίο είναι η χρηστικότητα, καθώς το νέο πρότυπο θα είναι περίπλοκο και πολύ μεγάλο για πρακτική χρήση.

4.2 Πολιτικές προστασίας κρίσιμων υποδομών

4.2.1 Πολιτικές προστασίας κρίσιμων υποδομών στην Ευρωπαϊκή Ένωση

Με δεδομένο το υψηλό ενδιαφέρον για την προστασία των κρίσιμων υποδομών, η Ευρωπαϊκή Επιτροπή παρουσίασε μια γενική στρατηγική για τη βελτίωση της προστασίας των κρίσιμων υποδομών. Στις 22 Οκτωβρίου 2004 με το κείμενο «Προστασία κρίσιμων υποδομών στον αγώνα κατά της τρομοκρατίας» τέθηκαν επί τάπητος προτάσεις για να βελτιωθεί η προστασία, η ετοιμότητα και η ανταπόκριση της Ευρώπης σε τρομοκρατικές επιθέσεις που αφορούν τις κρίσιμες υποδομές (European Commission, 2004).

Μεταξύ άλλων, προτάθηκε η δημιουργία ενός Ευρωπαϊκού Προγράμματος Προστασίας Κρίσιμων Υποδομών (European Program on Critical Infrastructure Protection-EPCIP) με σκοπό να αναγνωριστούν οι κρίσιμες υποδομές με πανευρωπαϊκή διάσταση, αναλύοντας την τρωτότητα και την αλληλεξάρτησή τους, στοχεύοντας στην αναγνώριση λύσεων για την προστασία αλλά και την προετοιμασία τους για την αντιμετώπιση ενδεχόμενων απειλών. Εκτός αυτού, η Επιτροπή εξέφρασε την άποψη ότι θα πρέπει να δημιουργηθεί ένα δίκτυο προειδοποιητικής πληροφόρησης κρίσιμων υποδομών (Critical Infrastructure Warning and Information Network - CIWIN). Το δίκτυο θα συγκεντρώνει ειδικούς στην προστασία κρίσιμων υποδομών από τα κράτη-μέλη με σκοπό να βοηθήσουν την Επιτροπή να καταρτίσει το εν λόγω πρόγραμμα (Spence, 2007).

Στη συνέχεια η Επιτροπή υιοθέτησε την Πράσινη Βίβλο σχετικά με την προστασία των κρίσιμων υποδομών (Επιτροπή Ευρωπαϊκών Κοινοτήτων, 2005). Ο κύριος στόχος της Πράσινης Βίβλου είναι να λάβει απόψεις σχετικά με τις πιθανές επιλογές της πολιτικής EPCIP εμπλέκοντας έναν σημαντικό αριθμό φορέων, όπως ιδιοκτήτες και φορείς εκμετάλλευσης της υποδομής, νομοθέτες, επαγγελματικές και βιομηχανικές ενώσεις σε συνεργασία με όλα τα επίπεδα της κυβέρνησης και του δημοσίου. Αυτή ήταν και η δεύτερη φάση μιας διαδικασίας διαβούλευσεων για την καθιέρωση ενός Ευρωπαϊκού Προγράμματος Προστασίας Κρίσιμων Υποδομών (Burgess, 2006).

Το Δεκέμβριο του 2005, το Συμβούλιο Δικαιοσύνης και Εσωτερικών Υποθέσεων κάλεσε την Επιτροπή να υποβάλλει πρόταση για το Ευρωπαϊκό Πρόγραμμα Προστασίας Κρίσιμων Υποδομών και αποφάσισε ότι αυτό θα πρέπει να βασίζεται σε μια ολιστική προσέγγιση των κινδύνων ενώ ως προτεραιότητά θα έχει την αποτροπή τρομοκρατικών απειλών. Σύμφωνα με αυτήν την προσέγγιση, οι ανθρωπογενείς, τεχνολογικές απειλές και οι φυσικές καταστροφές θα πρέπει να λαμβάνονται υπόψη στη διαδικασία προστασίας των κρίσιμων υποδομών, αλλά η απειλή της τρομοκρατίας θα πρέπει να έχει κυρίαρχη προτεραιότητα. Στις 12 Δεκεμβρίου 2006, η Επιτροπή υιοθέτησε την πρόταση για το Ευρωπαϊκό Πρόγραμμα Προστασίας Κρίσιμων Υποδομών, το οποίο θέτει το γενικό πλαίσιο των δραστηριοτήτων για την προστασία των κρίσιμων υποδομών σε επίπεδο ευρωπαϊκής ένωσης.

Η διαδικασία αναγνώρισης και προσδιορισμού των ευρωπαϊκών κρίσιμων υποδομών είναι ένα από τα βασικά στοιχεία του Ευρωπαϊκού Προγράμματος Προστασίας Κρίσιμων Υποδομών. Συγκεκριμένα, αυτό το πακέτο πολιτικών πρωτοβουλιών αποτελείται από τα εξής:

- Μια πρόταση για μια Οδηγία του Συμβουλίου σχετικά με την αναγνώριση και τον προσδιορισμό των ευρωπαϊκών κρίσιμων υποδομών και την εκτίμηση της ανάγκης για βελτίωση της προστασίας. Η προτεινόμενη Οδηγία παγιώνει μια διαδικασία για την αναγνώριση και τον προσδιορισμό των κρίσιμων υποδομών και μια κοινή προσέγγιση της εκτίμησης των αναγκών για τη βελτίωση της προστασίας αυτών των υποδομών.
- Μέτρα που έχουν σχεδιαστεί με σκοπό να διευκολύνουν την εφαρμογή του Ευρωπαϊκού Προγράμματος Προστασίας Κρίσιμων Υποδομών περιλαμβανομένων των εξής:

- Σχέδιο δράσης του Ευρωπαϊκού Προγράμματος Προστασίας Κρίσιμων Υποδομών.
- Πρόταση για απόφαση του Συμβουλίου σχετικά με το δίκτυο προειδοποιητικών πληροφοριών για τις κρίσιμες υποδομές.
- Χρήση ειδικών ομάδων.
- Αναγνώριση και ανάλυση της αλληλεξάρτησης.
- Υποστήριξη των κρατών-μελών σχετικά με τις εθνικές κρίσιμες υποδομές.
- Συνοδευτικά οικονομικά μέτρα, συγκεκριμένα το προτεινόμενο ευρωπαϊκό πρόγραμμα για την «Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks (CIPS)» για το διάστημα 2007-2013, που δημιούργησε ευκαιρίες χρηματοδότησης των μέτρων για την προστασία των κρίσιμων υποδομών τα οποία έχουν τη δυνατότητα να μεταφερθούν και να υιοθετηθούν από διάφορα κράτη-μέλη της Ευρώπης.

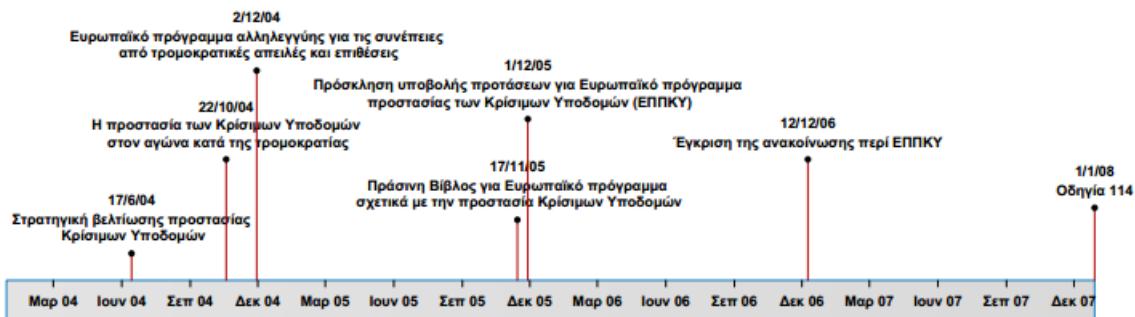
Στις 8 Δεκεμβρίου 2008, το Συμβούλιο υιοθέτησε την Οδηγία 2008/114/EK11 για την αναγνώριση και τον προσδιορισμό των ευρωπαϊκών κρίσιμων υποδομών και την εκτίμηση της ανάγκης για βελτίωση της προστασίας. Τα δίκτυα μεταφορών αναγνωρίστηκαν ως μία από τις κρίσιμες υποδομές οι οποίες, εάν διαταραχθούν ή καταστραφούν, μπορούν να επιφέρουν σημαντικές επιπτώσεις στην υγεία, την ασφάλεια, την προστασία, την οικονομική ευημερία των πολιτών και την αποτελεσματική λειτουργία των κυβερνήσεων των κρατών-μελών. Η Οδηγία θέτει τις αρχές βάσει των οποίων τα κράτη-μέλη πρέπει να διασφαλίσουν την ύπαρξη ενός σχεδίου ασφάλειας του φορέα εκμετάλλευσης (Operator Security Plan-OSP) ή ένα ισοδύναμο μέτρο για κάθε προσδιορισμένη ευρωπαϊκή κρίσιμη υποδομή. Η Οδηγία 2008/114/EK επισημαίνει ότι η πρωταρχική και απότερη ευθύνη για την προστασία των ευρωπαϊκών κρίσιμων υποδομών ανήκει στα κράτη-μέλη και στους ιδιοκτήτες/φορείς εκμετάλλευσης αυτών των υποδομών.

Το Ευρωπαϊκό Πρόγραμμα Προστασίας Κρίσιμων Υποδομών (EPCIP) και αντίστοιχα η Οδηγία 2008/114/EK θέτει το νομικό υπόβαθρο για κάθε προσπάθεια εύρεσης μιας λύσης. Το Ευρωπαϊκό Πρόγραμμα Προστασίας Κρίσιμων Υποδομών παραπέμπει σε ένα ολιστικό πλαίσιο για τις δράσεις προστασίας των κρίσιμων υποδομών σε επίπεδο Ευρωπαϊκής Ένωσης βάσει μιας κοινά αποδεκτής προσέγγισης όλων των τύπων κινδύνων, αλλά παράλληλα δίνει προτεραιότητα στην αντιμετώπιση

τρομοκρατικών και άλλων απειλών. Η Οδηγία 2008/114/EK νιοθετήθηκε από κάθε κράτος-μέλος, διασφαλίζοντας την ύπαρξη ενός μέτρου, όπως το σχέδιο ασφάλειας του φορέα εκμετάλλευσης, για κάθε προσδιορισμένη ευρωπαϊκή κρίσιμη υποδομή. Η Οδηγία 2008/114/EK και η προγραμματιζόμενη αναθεώρησή της προσδιορίζει τις κρίσιμες υποδομές ως εξής:

- Εγκαταστάσεις και δίκτυα ενέργειας.
- Μεταφορές (αεροδρόμια, λιμένες, σιδηροδρομικά δίκτυα και δίκτυα μαζικής μεταφοράς, συστήματα ελέγχου κυκλοφορίας).
- Επικοινωνίες και πληροφορική.
- Παραγωγή, αποθήκευση και μεταφορά επικίνδυνων αγαθών.
- Οικονομία (τράπεζες, χρεόγραφα και επενδύσεις).
- Κυβέρνηση (π.χ. Κρίσιμες υπηρεσίες, εγκαταστάσεις, δίκτυα πληροφοριών, στοιχεία και βασικές εθνικές τοποθεσίες και μνημεία).
- Υγεία.
- Ύδρευση (φράγματα, αποθήκευση, επεξεργασία και δίκτυα).
- Τρόφιμα.

Τα προαναφερθέντα έγγραφα, συνοψίζονται χρονολογικά στην Εικόνα 1.



Εικόνα 1: Πολιτικές προστασίας κρίσιμων υποδομών στην Ευρωπαϊκή Ένωση

4.2.2 Πολιτικές προστασίας κρίσιμων υποδομών στις ΗΠΑ

Η Εθνική Πολιτική για την Προστασία Κρίσιμων Υποδομών στις ΗΠΑ καθορίζεται από το Homeland Security Presidential Directive (HSPD-7), που στοχεύει στην ενίσχυση της προστασίας των υποδομών με τη δημιουργία ενός πλαισίου συνεργασίας για τους φορείς που συνεργάζονται με το Τμήμα Εσωτερικής Ασφάλειας (Department of Homeland Security) να εντοπίσουν, να ιεραρχήσουν και να

προστατεύσουν τις κρίσιμες υποδομές στις κοινότητές τους από τρομοκρατικές επιθέσεις (Bush, 2003). Η οδηγία κατέδειξε 17 κρίσιμους τομείς και, για κάθε τομέα ένας συγκεκριμένος φορέας ανέλαβε την υποχρέωση να οδηγήσει τις διαδικασίες και δραστηριότητες για την προστασία και την ανθεκτικότητα των αντίστοιχων υποδομών. Το Εθνικό Πρόγραμμα Προστασίας των Υποδομών (National Infrastructure Protection Programme / NIPP) αποτελεί το κύριο πλαίσιο υλοποίησης για την προστασία κρίσιμων υποδομών που παρέχει τις κατευθυντήριες γραμμές για την εφαρμογή του προγράμματος. Μεταξύ άλλων ενσωματώνει τις προσπάθειες για την προστασία των κρίσιμων υποδομών σε διάφορους τομείς, καθορίζει τους ρόλους και τις ευθύνες των διαφόρων φορέων σε πολιτειακό και ομοσπονδιακό επίπεδο, αλλά και θέτει το πλαίσιο διαχείρισης επικινδυνότητας.

4.2.3 Πολιτικές προστασίας κρίσιμων υποδομών στην Ελλάδα

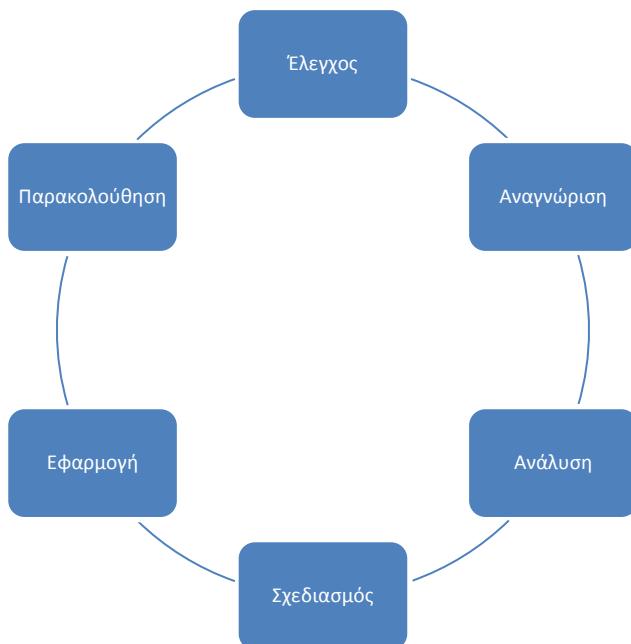
Σύμφωνα με το ΠΔ 39/2011 «Προσαρμογή της ελληνικής νομοθεσίας προς τις διατάξεις της Οδηγίας 2008/114/EK του Συμβουλίου της 8ης Δεκεμβρίου 2008 ‘σχετικά με τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας, και σχετικά με την αξιολόγηση της ανάγκης βελτίωσης της προστασίας τους’», το Κέντρο Μελετών Ασφάλειας του Υπουργείου Δημόσιας Τάξης και Προστασίας του Πολίτη ανέλαβε ως εθνικό σημείο επαφής για την εφαρμογή της οδηγίας 114/2008. Με το ΠΔ αυτό, θεσπίστηκε η διαδικασία προσδιορισμού και χαρακτηρισμού των ευρωπαϊκών υποδομών ζωτικής σημασίας, καθώς και η προσέγγιση της αξιολόγησης της ανάγκης βελτίωσης της προστασίας των υποδομών αυτών προκειμένου να συμβάλλει στην προστασία του κοινού.

Ταυτόχρονα κάθε εθνική κρίσιμη υποδομή υποχρεούται να καταθέτει ολοκληρωμένα σχέδια ασφαλείας λειτουργίας που προσδιορίζουν τα περιουσιακά στοιχεία τους και τα μέτρα ασφάλειας που υπάρχουν ή εφαρμόζονται για την προστασία τους.

4.2.4 Πρότυπα προστασίας κρίσιμων υποδομών

Στη διεθνή βιβλιογραφία, υπάρχουν πολλά πρότυπα, πρακτικές και μέθοδοι διαθέσιμες για την αντιμετώπιση των κινδύνων που απειλούν την ασφάλεια κρίσιμων υποδομών. Η κατάλληλη επιλογή για κάθε οργανισμό εξαρτάται από το σύνολο των νόμων και των κανονισμών, τους στόχους και τους σκοπούς, τις πρακτικές

διαχείρισης και τις πολιτικές που ορίζουν τις παραμέτρους με τις οποίες πρέπει να συμφωνεί η διαδικασία διαχείρισης κινδύνων. Η διαδικασία διαχείρισης κινδύνων σε έναν οργανισμό είναι μια συνεχής προσπάθεια που καλύπτει όλο το εύρος λειτουργίας και τους εργαζόμενους του.



Εικόνα 2: Διαδικασία διαχείρισης κινδύνων εντός οργανισμού

Ανεξάρτητα από το πλαίσιο εντός του οποίου εφαρμόζεται η διαδικασία διαχείρισης επικινδυνότητας, τα θεμελιώδη βήματα προς τη διαμόρφωση ενός ποσοτικά καθορισμένου πλαισίου εκτίμησης είναι τα ίδια: αναγνώριση, εκτίμηση και αντιμετώπιση. Το πρώτο και πιο σημαντικό βήμα στην ποσοτική ανάλυση κινδύνων (Quantitative Risk Assessment- QRA) είναι η επεξεργασία των σεναρίων κινδύνου. Στην πλειοψηφία των περιπτώσεων, ο αριθμός αυτών των σεναρίων είναι μεγάλος, και για αυτό το λόγο, το δεύτερο βήμα είναι το φίλτραρισμα και η ιεράρχηση των σεναρίων ανάλογα με τη σοβαρότητά τους, με βάση τις πιθανότητες και τις συνέπειες τους (Straub & Welke, 1998). Οι προτεινόμενες μεθοδολογίες για να γίνει αυτό συνοψίζονται παρακάτω.

Στις αρχές της δεκαετίας του '90, αναπτύχθηκε μια απλή προσέγγιση για την ποσοτική ανάλυση κινδύνων στη Νορβηγία, που ονομάστηκε Ανάλυση Κινδύνων και Ευπάθειας (Risk and Vulnerability Analysis - RVA) (Turner et al., 2003), η οποία είναι αρκετά παρόμοια με την Προκαταρκτική Ανάλυση Κινδύνων (Preliminary

Hazard Assessment) (Paté-Cornell, 1996). Μέθοδοι ανάλυσης κινδύνων, όπως η Πιθανοκρατική Ανάλυση Ασφάλειας (Probabilistic Safety Analysis) και Ποσοτική Ανάλυση Κινδύνων (Quantitative Risk Analysis), αποτελούν λεπτομερή πιθανοθεωρητικά και φυσικά μοντέλα (Thompson & Graham, 1996). Αυτά τα μοντέλα απαιτούν περισσότερες γνώσεις και πόρους από ότι είναι συνήθως διαθέσιμα στις μικρές και μεσαίες επιχειρήσεις και στο δημόσιο τομέα με αποτέλεσμα η λιγότερο απαιτητική Ανάλυση Κινδύνων και Τρωτότητας να έχει εξελιχθεί σε μια αρκετά διαδεδομένη προσέγγιση. Τις τελευταίες δύο δεκαετίες, η Ανάλυση Κινδύνων και Τρωτότητας εφαρμόζεται ξεχωριστά σε διάφορες κρίσιμες υποδομές, αλλά όχι ως μια ενοποιημένη προσέγγιση για όλους τους τομείς περιλαμβανομένης και της αλληλεξάρτησης μεταξύ των διαφόρων υποδομών.

Στο άρθρο των Carr et al. (1993) ακολουθήθηκε μια διαδικασία αναγνώρισης κινδύνων με έρευνα πεδίου που αποτελείται από μια σειρά συνεντεύξεων με ομάδες επιλεγμένου προσωπικού. Κάθε συνεδρία συνέντευξης αποτελείται από δύο μέρη:

1. Ερώτηση και απάντηση: Γίνεται χρήση ενός ερωτηματολογίου που περιέχει δοκιμαστικές ερωτήσεις ευαίσθητου περιεχομένου για την αναμόχλευση προβλημάτων, αποριών ή κινδύνων που ενδέχεται να ελλοχεύουν στην επιτυχή ολοκλήρωση του έργου.
2. Ανάλυση του ζητήματος: Αφορά τη διευκρίνιση της διατύπωσης και τη σημασία των ζητημάτων που προέκυψαν από τη φάση Ερώτηση/Απάντηση μέσω της ταξινόμησης κινδύνων σε ομάδες σε επίπεδο κλάσης/στοιχείου. Όταν οι συμμετέχοντες ταξινομήσουν τα ζητήματα, τα αξιολογούν συναινετικά για να καθορίσουν ποια είναι κατά βάση ισοδύναμα. Στη συνέχεια τα ισοδύναμα ζητήματα συγχωνεύονται.

Οι Webler et al. (1995) περιέγραψαν μια μεθοδολογία κατάταξης κινδύνων μέσω ενός εκτεταμένου παραδείγματος που είχε σχέση με την υποδομή μιας δημόσιας υπηρεσίας (κεντρική κυβέρνηση) στο Νιού Τζέρσεϋ, ΗΠΑ. Επέδειξαν τον τρόπο με τον οποίο μπορούν οι προσεγγίσεις κατάταξης κινδύνων που βασίζονται στη συζήτηση να λειτουργήσουν συμπληρωματικά στις ισχύουσες μεθοδολογικές προσεγγίσεις και παρουσίασαν μια ταξινόμηση η οποία καλύπτει την ουσιαστική ανάγκη για δημόσια συζήτηση σχετικά με τους κινδύνους.

Οι Morgan et al. (2000) προτείνουν μια μεθοδολογία κατάταξης σχεδιασμένη για χρήση από τις υπηρεσίες διαχείρισης κινδύνων, η οποία καλεί τις τακτικές δυνάμεις (taskforces) να ορίσουν και να κατηγοριοποιήσουν τους κινδύνους, καθώς και τα κριτήρια αξιολόγησης. Η κατάταξη υλοποιείται από τέσσερις ομάδες: διαχειριστές κινδύνου εντός και εκτός της εμπλεκόμενης υπηρεσίας, μια ομάδα κυβερνητικών λειτουργών για τη διαχείριση κινδύνων και μια ομάδα τοπικών λειτουργών για τη διαχείριση κινδύνων. Κάθε ομάδα κατάταξης θα ακολουθήσει δύο διαφορετικές διαδικασίες: (1) μια αναλυτική προσέγγιση με περιορισμούς και (2) μια ολιστική και αφαιρετική προσέγγιση. Τα αποτελέσματα στη συνέχεια θα πρέπει να συνδυαστούν ώστε να προκύψει η καλύτερη κατάταξη.

Οι Baron et al. (2000) διεξήγαγαν εκτενείς έρευνες εξειδικευμένων και μη μεθοδολογιών στην ανάλυση κινδύνων για να επαληθεύσουν τις προτεραιότητές τους σχετικά με την ατομική, επιχειρησιακή και κυβερνητική δράση για τη μείωση κινδύνων, λαμβάνοντας υπόψη τη σοβαρότητα του κινδύνου, τον αριθμό των εμπλεκόμενων ατόμων, την ανησυχία και τις πιθανότητες ο κίνδυνος να έχει επιπτώσεις στα ίδια τα άτομα και σε άλλους. Ένα από τα σημαντικότερα πορίσματα της έρευνας «είναι ότι το ενδιαφέρον για δράση, σε ατομικό και κυβερνητικό επίπεδο, σχετίζεται άμεσα με την ανησυχία. Η ανησυχία, με τη σειρά της, επηρεάζεται κυρίως από τις πεποιθήσεις σχετικά με την πιθανότητα να συμβεί κάτι». Παράλληλα, αναπτύχθηκε μια μεθοδολογία κατάταξης και φιλτραρίσματος κινδύνων με σκοπό να τεθεί προτεραιότητα στα αποτελέσματα των λειτουργιών αστοχίας και ανάλυσης επιπτώσεων (Haimes 1998). Αυτή η μεθοδολογία ιεράρχησης κινδύνων λαμβάνει υπόψη πολλαπλούς ποσοτικούς παράγοντες, όπως υπολογισμούς αξιοπιστίας, καθώς και ποιοτικούς παράγοντες, όπως γνώμες ειδικών (expert choice-rating) για την κρισιμότητα ορισμένων στοιχείων.

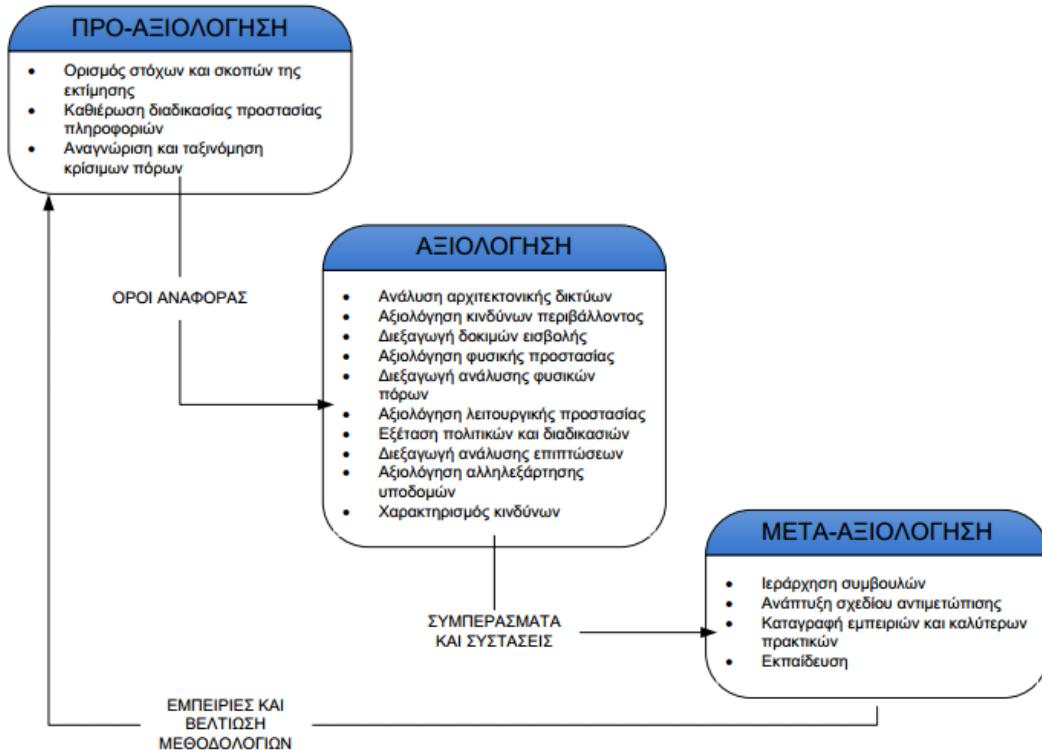
Οι Morgan et al. (2001) ασχολούνται με τα εγγενή προβλήματα κατά την ομαδοποίηση ενός μεγάλου αριθμού σεναρίων κινδύνων σε εύκολα διαχειριζόμενες κατηγορίες και υποστηρίζουν ότι αυτές οι κατηγορίες κινδύνων πρέπει να αξιολογούνται σε σχέση με ένα σύνολο κριτηρίων. Αυτό είναι ιδιαίτερα σημαντικό όταν πρέπει να ληφθούν σοβαρές αποφάσεις συγκρίνοντας και κατατάσσοντας χιλιάδες συγκεκριμένους κινδύνους. Ο απότερος χαρακτηρισμός κινδύνων θα πρέπει λογικά να είναι συνεπής, συμβατός με το διοικητικό πλαίσιο, ισόνομος και συμμορφούμενος με τους γνωστικούς φραγμούς και προκαταλήψεις.

Οι Rinaldi et al. (2001) εισήγαγαν την έννοια ότι οι κρίσιμες υποδομές είναι πολυεπίπεδα διασυνδεδεμένες και αμοιβαία εξαρτώμενες με σύνθετους τρόπους, σε φυσικό επίπεδο αλλά και μέσω πληροφοριακών και επικοινωνιακών συστημάτων (τα λεγόμενα «κυβερνοσυστήματα»), κάτι που είναι περισσότερο από μια αφηρημένη θεωρητική έννοια.

4.2.4.1 Διαχείριση Ασφάλειας στις ΗΠΑ

Το US Department of Energy (Radvanovsky & McDougall, 2009) παρουσιάζει μια ολοκληρωμένη μεθοδολογία εκτίμησης της ευπάθειας κρίσιμων υποδομών. Όπως προκύπτει, η μεθοδολογία χωρίζεται σε τρεις βασικές φάσεις: προαξιολόγηση, αξιολόγηση και μεταγενέστερη αξιολόγηση. Κάθε φάση αποτελείται από μια σειρά στοιχείων ή εργασιών που έχουν σχεδιαστεί για την εκτίμηση της ευπάθειας. Τα διδάγματα που προκύπτουν από την εφαρμογή της ενσωματώθηκαν και χρησιμοποιούνται για να βελτιωθεί, όποτε αυτό είναι εφικτό και να επεκταθεί η μεθοδολογία. Τα συγκεκριμένα στοιχεία ή εργασίες που σχετίζονται με κάθε φάση εκτίμησης μπορούν να προσαρμοστούν ώστε να καλύψουν συγκεκριμένους στόχους. Παρόλο που η μεθοδολογία έχει ενσωματώσει μοναδικά στοιχεία που απαιτούν άτομα με ειδική τεχνογνωσία των ειδικών, η μεθοδολογία μπορεί να προσαρμοστεί και σε ατομικό επίπεδο.

Για την ανάπτυξη της μεθοδολογίας έχει μελετηθεί ένας αριθμός τεχνικών, μεθόδων και προσεγγίσεων εκτίμησης που χρησιμοποιούνται από άλλους οργανισμούς του δημόσιου και ιδιωτικού τομέα. Περιλαμβάνει πληροφορίες που έχουν συγκεντρωθεί μέσω ανοιχτής βιβλιογραφίας, παρουσιάσεων, οδηγιών και συζητήσεων. Επιπλέον, τα στοιχεία της μεθοδολογίας έχουν αντληθεί από συνεχιζόμενα προγράμματα διασφάλισης υποδομών και προστασίας αυτών. Η βασική φιλοσοφία της διαδικασίας εκτίμησης της ευπάθειας είναι να μοχλεύσει της τεχνικές, τις μεθόδους και τις προσεγγίσεις εκτίμησης της ευπάθειας που έχουν αποδειχθεί χρήσιμες και αξιοποιήσιμες.



Εικόνα 3: Φάσεις εκτίμησης της ευπάθειας

Κατά τους McFadden και Green (2007) είναι εφικτό να προκύψουν σημαντικές πληροφορίες για τη βελτίωση της διαχείρισης κινδύνων εξετάζοντας την πολυπλοκότητα που σχετίζεται με τον καθορισμό του περιβάλλοντος και της ομαδοποίησης. Υποστηρίζουν ότι η «ευπάθεια/τρωτότητα» αναδύθηκε ως μια σημαντική έννοια για την κατανόηση και τη διαχείριση πόρων, παρόλα αυτά αναγνωρίζουν ότι ο όρος είναι αρκετά αμφιλεγόμενος. Η έρευνα θεωρεί ότι οι διάφορες χρήσεις του όρου τονίζουν το γεγονός ότι ο χαρακτηρισμός ενός πόρου ως ευπαθίους δεν αποτελεί ουδέτερη πράξη. Η εννοιολογική σύλληψη της «ευπάθειας/τρωτότητας» πρέπει να λαμβάνεται υπόψη όχι μόνο από τεχνικής πλευράς αλλά και από πλευράς κοινωνικών σχέσεων μεταξύ αυτών που εμπλέκονται στη διαχείριση του πόρου. Αυτό υποχρεώνει τους επιστήμονες, τους πολιτικούς ηγέτες και άλλους εμπλεκόμενους φορείς, να θεωρήσουν την ανάλυση της ευπάθειας ως ένα διεξοδικό σύστημα εκτίμησης πόρων. Η διαδικασία μάθησης, μέσω της οποίας επιτυγχάνεται η ολοκληρωμένη εκτίμηση, είναι σημαντική για τη δημιουργία νέων και πιο χρήσιμων πληροφοριών για τον τρόπο συμπεριφοράς ολόκληρου του συστήματος. Στο συμπέρασμά τους τονίζουν ότι η απλοποίηση της εκτίμησης ευπάθειας στη

διαχείριση πόρων προέκυψε σε βάρος της απαραίτητης πολυπλοκότητας των συστημάτων και των πόρων τους.

4.2.4.2 Διαχείριση Ασφάλειας στην Ευρώπη (τομέας ενέργειας)

Η Γενική Διεύθυνση Ενέργειας της Ευρωπαϊκής Επιτροπής δημιούργησε ένα μη δεσμευτικού χαρακτήρα σχέδιο αναφοράς για την ολιστική διαχείρισης της ασφάλειας κρίσιμων ενεργειακών υποδομών. Το σχέδιο προορίζεται να αποτελέσει έναν χρήσιμο οδηγό για διαχειριστές υποδομών ενέργειας, πόρων, συστημάτων ή τμημάτων, ανεξάρτητα από την ταξινόμησή τους ως ευρωπαϊκές ή εθνικές κρίσιμες υποδομές. Αυτό επικεντρώνεται σε κακόβουλες, ανθρωπογενείς απειλές, ενώ δίνει προσοχή σε όλες τις σχετικές πτυχές λειτουργίας της υποδομής. Η ακεραιότητα των υποδομών ενέργειας και η αξιόπιστη λειτουργία τους αποτελούν βασικούς παράγοντες για τη διασφάλιση της παραγωγής ενέργειας, η οποία είναι ζωτική για την ευημερία των πολιτών και τη λειτουργία της οικονομίας.

Το Σχέδιο Αναφοράς (Reference Security Management Plan, 2010) συντάχθηκε με σκοπό την αποκλειστική του χρήση από τη σκοπιά του φορέα διαχειριστή των υποδομών και καλύπτει ένα ευρύ πεδίο από την ανάγκη συμμόρφωσης με τα ισχύοντα εθνικά ή διεθνή νομικά και τεχνικά πλαίσια, έως την ενσωμάτωση των σωστών διαδικασιών διαχείρισης κινδύνου στο πλαίσιο των γενικών στόχων και στρατηγικών της εταιρείας που είναι υπεύθυνη για την υποδομή.

Το ευρωπαϊκό σύστημα ενέργειας είναι ένα αλληλεξαρτώμενο, διεθνές δίκτυο μεταφοράς ισχύος, δικτύων αγωγών, διαύλων και εγκαταστάσεων διανομής, που είναι εξ' ορισμού πέρα από τις δυνατότητες προστασίας οποιουδήποτε μεμονωμένου εθνικού οργανισμού ασφάλειας, άμυνας, ελέγχου ή συντονισμού. Ως εκ τούτου, οι μεθοδολογίες, τα κριτήρια αξιολόγησης της ευπάθειας και τα μέτρα κατά της τρομοκρατίας πρέπει να διέπονται από τη διεθνή συνεργασία η οποία αντανακλά το διεθνή χαρακτήρα των κρίσιμων υποδομών του συστήματος ενέργειας (Bailes, 2004). Πριν από τα βήματα για την εκτίμηση των απειλών προς τις κρίσιμες υποδομές του συστήματος ενέργειας και την ανάπτυξη αντιτρομοκρατικών στρατηγικών για την προστασία τους, απαιτείται να βρεθεί ένας περιεκτικός ορισμός του όρου «κρίσιμες υποδομές του συστήματος ενέργειας». Οι κρίσιμες υποδομές του συστήματος ενέργειας περιλαμβάνουν όλα τα στάδια, από την παραγωγή έως και την κατανάλωση

της ενέργειας. Έτσι ενώ η παροχή ενέργειας είναι ένα σημαντικό στοιχείο για τις κρίσιμες υποδομές του συστήματος ενέργειας, δεν είναι πάρα ένα επιμέρους μόνο στοιχείο ενός πολύ ευρύτερου συστήματος.

4.2.4.3 Προστασία κρίσιμων υποδομών Πληροφορικής και Επικοινωνιών

Οι κρίσιμες υποδομές Τεχνολογιών Πληροφορικής και Επικοινωνιών (Critical Information Infrastructure - CII) γενικά αναφέρονται σε τεχνολογικά συστήματα πληροφοριών και επικοινωνιών τα οποία είναι απαραίτητα για τη λειτουργία εθνικών και διεθνών κρίσιμων υποδομών. Παραδείγματα αυτών περιλαμβάνουν Gorman et al., 2004):

1. Δίκτυα τηλεπικοινωνιών, διαχείρισης, υπηρεσίες για κλήσεις έκτακτης ανάγκης με βάση την τοποθεσία.
2. Μεταφορές: διαχείριση εναέριας κίνησης, δρομολόγηση και έλεγχος τρένων, διαχείριση οδικής κίνησης.
3. Οικονομικές υπηρεσίες: συναλλαγές πιστωτικών καρτών, συστήματα διακανονισμών, αρχεία συναλλαγών, ηλεκτρονικές συναλλαγές μετοχών/ομολόγων.
4. Συστήματα ελέγχου/SCADA (Supervisory, Control and Data Acquisition) για τη διαχείριση της παραγωγής και τη διακίνησης ενέργειας, χημικών παρασκευών και διαδικασιών διύλισης.

Το γεγονός ότι τα όρια μεταξύ της προστασίας των Κρίσιμων Υποδομών και των Κρίσιμων Υποδομών Τεχνολογιών Πληροφορικής και Επικοινωνιών είναι ολοένα και πιο δυσδιάκριτα καταμαρτυρείται από πολλά περιστατικά. Για παράδειγμα, το Μάρτιο του 2007 ένα πείραμα (η δοκιμή της γεννήτριας ARTIC) το οποίο διενεργήθηκε από τα Εθνικά Εργαστήρια του Αινταχο των Η.Π.Α. έδειξε ότι μια μεγάλη γεννήτρια diesel μπορούσε να υποστεί σοβαρές ζημιές μέσω της εκμετάλλευσης μιας τρωτότητας στο υπολογιστικό σύστημα, αποδεικνύοντας ότι φυσική ζημιά μπορούσε να προκληθεί μέσω ένα υπολογιστικού συστήματος (Weiss, 2010).

5. Ολοκληρωμένες Προσεγγίσεις Εκτίμησης Επικινδυνότητας

5.1 Μέθοδος CRAMM

Η μέθοδος CRAMM αναπτύχτηκε από το CCTA (Central Computer and Telecommunications Agency, 1996) της βρετανικής κυβέρνησης το 1985, ώστε να εφοδιάσει τα διάφορα τμήματα της κυβέρνησης με μια κοινή μέθοδο ανάλυσης κινδύνων πληροφοριακών συστημάτων. Στη συνέχεια η χρήση της επεκτάθηκε και στη μελέτη επικινδυνότητας σε μεγάλης κλίμακας ιδιωτικούς και δημόσιους οργανισμούς. Η μέθοδος CRAMM είναι ικανή να καλύψει ένα ευρύ φάσμα διοικητικών, επιχειρησιακών και τεχνικών απαιτήσεων (Landoll & Landoll, 2005).

Η CRAMM έχει κερδίσει διεθνή αναγνώριση για τους εξής λόγους:

- Αποτελεί πρότυπη μέθοδο και έχει αναπτυχθεί με σκοπό να εφαρμοστεί κυρίως σε μεγάλης κλίμακας οργανισμούς και επιχειρήσεις κοινής ωφέλειας.
- Από το 1987 μέχρι σήμερα έχει εφαρμοστεί σε χιλιάδες περιπτώσεων, συνεπώς είναι ωριμή μέθοδος ευρισκόμενη ήδη στην 5^η έκδοσή της (version 5.2.2011).
- Συνοδεύεται από αυτοματοποιημένο εργαλείο λογισμικού που υποστηρίζει όλα τα στάδια της εφαρμογής της, καθώς και την επιλογή αντιμέτρων.
- Καλύπτει όλες τις συνιστώσες της ασφάλειας, περιλαμβανομένων του τεχνικού παράγοντα, των θεμάτων διαδικασιών και προσωπικού, της φυσικής ασφάλειας, της ασφάλειας δικτύων κ.λπ.

Η υπολογιστική μέθοδος και η τεχνική την οποία υιοθετεί η CRAMM για το συσχετισμό και τον προσδιορισμό των αποτελεσμάτων βασίζεται σε μια ποιοτική προσέγγιση. Η βασική ιδέα είναι ότι από την ανάλυση επικινδυνότητας μπορεί να προβλεφθεί η πιθανή ζημία που θα προκαλέσει η απώλεια της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας ενός αγαθού. Παράλληλα, παρέχει επαρκή βεβαιότητα ότι έχουν εντοπιστεί όλοι οι πιθανοί κίνδυνοι, οι αδυναμίες και οι απειλές και ότι όλα τα αποτελέσματα είναι συνεπή σε όλο το φάσμα του πληροφοριακού συστήματος που αξιολογείται. Η μέθοδος CRAMM περιέχει μια πολύ μεγάλη βιβλιοθήκη αντιμέτρων που αποτελείται από περίπου 3.500 λεπτομερή αντίμετρα οργανωμένα σε περισσότερες από 70 κατηγορίες.

Το κόστος για την εξάλειψη όλων των κινδύνων που απειλούν ένα πληροφοριακό σύστημα είναι απαγορευτικό. Ωστόσο, σύμφωνα με την CRAMM, η επικινδυνότητα μπορεί να αντιμετωπισθεί αποτελεσματικά και οικονομικότερα, μέσα από την δομημένη ανάλυση και αποτίμηση των αγαθών. Σύμφωνα με την μέθοδο CRAMM, η επικινδυνότητα θεωρείται ότι είναι ο συνδυασμός της πιθανότητας να συμβεί ένα ανεπιθύμητο περιστατικό και των επιπτώσεων που θα μπορούσαν να προκύψουν από αυτό. Επομένως, η μέθοδος CRAMM καταδεικνύει το δυνητικό κόστος που μπορεί να επιβαρύνει έναν οργανισμό, συντελώντας καταλυτικά στη δικαιολόγηση του κόστους των προτεινόμενων αντιμέτρων.

Η CRAMM είναι συνεργατική μέθοδος και αποτελείται από τρία βασικά στάδια:

1. Προσδιορισμός-αποτίμηση αγαθών (identification and valuation of assets),
2. Ανάλυση επικινδυνότητας (risk analysis) και
3. Διαχείριση επικινδυνότητας (risk management).

Στάδιο	Βήματα
Προσδιορισμός και αποτίμηση αγαθών (identification and valuation of assets)	<p><i>Βήμα 1:</i> Περιγραφή πληροφοριακών συστημάτων και εγκαταστάσεων</p> <p><i>Βήμα 2:</i> Αποτίμηση αγαθών πληροφοριακών συστημάτων και εγκαταστάσεων</p> <p><i>Βήμα 3:</i> Επιβεβαίωση και επικύρωση αποτίμησης</p>
Ανάλυση επικινδυνότητας (risk analysis)	<p><i>Βήμα 1:</i> Προσδιορισμός απειλών που αφορούν κάθε Αγάθο (asset)</p> <p><i>Βήμα 2:</i> Εκτίμηση απειλών (threat assessment) και αδυναμιών (vulnerability assessment)</p> <p><i>Βήμα 3:</i> Υπολογισμός επικινδυνότητας συνδυασμών Αγάθο-Απειλή-Αδυναμία</p> <p><i>Βήμα 4:</i> Επιβεβαίωση και επικύρωση βαθμού επικινδυνότητας</p>
Διαχείριση επικινδυνότητας (risk management)	<p><i>Βήμα 1:</i> Προσδιορισμός προτεινόμενων αντιμέτρων</p> <p><i>Βήμα 2:</i> Σχέδιο ασφάλειας πληροφοριακών συστημάτων και εγκαταστάσεων</p>

Πίνακας 9: Στάδια και βήματα της CRAMM

Η μέθοδος CRAMM είναι η κύρια μέθοδος πιστοποίησης για τα πρότυπα ISO 27000, ενώ επικεντρώνεται στα ISO/IEC 27001:2005. Παράλληλα, καλύπτει τις απαιτήσεις της ευρωπαϊκής και της ελληνικής νομοθεσίας, που απαιτούν από τα πληροφοριακά συστήματα που επεξεργάζονται προσωπικά δεδομένα, τη λήψη μέτρων προστασίας. Με τον τρόπο αυτό, εξασφαλίζεται επίπεδο ασφάλειας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων.

Η CRAMM διαχωρίζει τα αγαθά στις εξής κατηγορίες: εξοπλισμός, υπηρεσίες, λογισμικό, δεδομένα και τοποθεσίες. Κατά την αποτίμηση των αγαθών η CRAMM εξετάζει τις παρακάτω πτυχές: διαθεσιμότητα, ακεραιότητα και εμπιστευτικότητα. Για την αποτίμηση αγαθών η CRAMM διαθέτει 10 επίπεδα. Το εργαλείο CRAMM καλύπτει τα παρακάτω είδη απειλών: λογικές απειλές, απειλές επικοινωνιών, τεχνικές βλάβες, ανθρώπινα σφάλματα και φυσικές απειλές. Η μέθοδος CRAMM εξετάζει κάθε συνδυασμό του γινομένου επισφάλεια και επίπτωση και βρίσκει ποιο είναι το πιο επικίνδυνο. Αυτό το γινόμενο είναι που καθορίζει ποια μέτρα θα ληφθούν, λαμβάνοντας υπόψη μόνο το worst-case scenario.

Κάθε αντίμετρο στην CRAMM αποτιμάται σε μια κλίμακα από το ένα μέχρι το επτά. Τα αντίμετρα διαχωρίζονται σε κατηγορίες και υποκατηγορίες, βάσει επτά διαστάσεων, οι οποίες δηλώνουν το είδος του μέτρου: λογισμικό, υλικό, επικοινωνίας, διαδικαστικό, φυσικό, προσωπικού και περιβάλλοντος. Αφού υπολογιστούν τα προτεινόμενα αντίμετρα, ο αναλυτής επιλέγει για κάθε αντίμετρο αν είναι εφαρμόσιμο ή όχι και υπολογίζεται η προτεραιότητα εφαρμογής κάθε μέτρου σε κλίμακα από το δύο έως το δέκα. Ο υπολογισμός βασίζεται στον αριθμό των απειλών, αν απαιτείται για την προστασία μιας κρίσιμης εφαρμογής ή αν υπάρχουν ήδη εγκατεστημένα εναλλακτικά αντίμετρα. Επίσης λαμβάνεται υπόψη το κόστος εφαρμογής, καθώς και η αποτελεσματικότητα και το είδος της προστασίας που προσδίδει κάθε αντίμετρο. Για κάθε αντίμετρο ορίζεται και ο τύπος προστασίας στον οποίο αναφέρεται. Οι τύποι που ορίζει η CRAMM είναι: μείωση απειλής, μείωση τρωτότητας, μείωση επίπτωσης, ανίχνευση και ανάκαμψη. Πολύ σημαντική κρίνεται και η δυνατότητα επανιχνηλάτησης για την εξέταση συγκεκριμένου συνδυασμού αγαθού/απειλής/ευπάθειας που οδήγησε στην επιλογή των αντίστοιχων αντιμέτρων. Κάθε ομάδα αντιμέτρων στο εργαλείο CRAMM, έχει την ακόλουθη δομή:

- Δήλωση πολιτικής, η οποία εξάγεται αυτολεξεί από το κατάλληλο έγγραφο ασφάλειας.

- Ο στόχος και η ανάγκη που θα ικανοποιηθεί από την εφαρμογή των συγκεκριμένων αντιμέτρων.
- Λεπτομερής περιγραφή της σχετιζόμενης επιχειρησιακής λειτουργίας με το αντίμετρο.
- Τρόποι ή επιλογές που μπορούν να διασφαλίσουν την επιθυμητή λειτουργικότητα.

5.2 Μέθοδος Magerit - Εργαλείο EAR/Pilar

Η μέθοδος MAGERIT είναι μια ανοικτή μέθοδος για την ανάλυση και διαχείριση κινδύνου, η οποία αναπτύχθηκε από το Ισπανικό Ανώτατο Συμβούλιο για την Ηλεκτρονική Διακυβέρνηση (Crespo et al., 2006). Τόσο η μέθοδος Magerit όσο και το εργαλείο EAR/Pilar περιγράφονται στο αντίστοιχο κεφάλαιο.

5.3 Μέθοδος NIST

To NIST Special Publication (SP) 800-30, Risk Management Guide for Information Technology Systems αποτελεί πρότυπο της Ομοσπονδιακής κυβέρνησης των ΗΠΑ (Stoneburner et al., 2002). Η συγκεκριμένη μέθοδος είναι σχεδιασμένη κυρίως για να είναι ποιοτική και βασίζεται σε εξειδικευμένους αναλυτές ασφάλειας που εργάζονται με τους ιδιοκτήτες του συστήματος και εμπειρογνώμονες τεχνικούς για τον εις βάθος εντοπισμό, την αξιολόγηση και τη διαχείριση του κινδύνου στα πληροφοριακά συστήματα. Το πρότυπο NIST 800-30 αποτελεί οδηγό που καθορίζει όλες τις πτυχές ενός αποτελεσματικού προγράμματος διαχείρισης επικινδυνότητας. Ενσωματώνει τις κατευθυντήριες γραμμές και τη διαδικασία που απαιτείται για την αξιολόγηση και τον περιορισμό των κινδύνων των πληροφοριακών συστημάτων. To NIST 800-30 στοχεύει κυρίως σε μεγάλης κλίμακας οργανισμούς (όπως κυβερνητικούς οργανισμούς και μεγάλες εταιρείες) για την καλύτερη διαχείριση της ασφάλειας των πληροφοριακών συστημάτων τους.

Η προτεινόμενη προσέγγιση της διαχείρισης κινδύνου περιλαμβάνει δύο κύριες διαδικασίες:

- Εκτίμηση Επικινδυνότητας (Risk Assessment): Περιλαμβάνει τον προσδιορισμό και την αξιολόγηση των απειλών, αδυναμιών και κινδύνων, καθώς και τη σύσταση των κατάλληλων μέτρων προστασίας.

- Περιορισμός Επικινδυνότητας (Risk Mitigation): Περιλαμβάνει την ιεράρχηση, την αξιολόγηση και την εφαρμογή των μηχανισμών ασφάλειας που προτάθηκαν κατά την προηγούμενη διαδικασία (Εκτίμηση Επικινδυνότητας).

Η διαδικασία Εκτίμησης Επικινδυνότητας αποτελείται από εννέα (9) βασικά βήματα (Stoneburner et al., 2002):

Βήμα 1 - Χαρακτηρισμός του Συστήματος

Το πρώτο βήμα αποτελεί τον καθορισμό της έκτασης της μελέτης. Σε αυτό το σημείο, εντοπίζονται τα όρια του πληροφοριακού συστήματος, μαζί με τους πόρους και τις πληροφορίες που το συνθέτουν. Με το χαρακτηρισμό ενός πληροφοριακού συστήματος καθιερώνεται η έκταση της προσπάθειας εκτίμησης της επικινδυνότητας, σκιαγραφούνται τα όρια της επιχειρησιακής άδειας (ή διαπίστευσης) και παρέχονται πληροφορίες (π.χ. υλικό, λογισμικό, συνδεσιμότητα του συστήματος, και αρμόδιο τμήμα ή προσωπικό υποστήριξης) θεμελιώδους σημασίας για τον καθορισμό του κινδύνου.

Βήμα 2 - Προσδιορισμός απειλών

Σε αυτό το βήμα προσδιορίζονται οι απειλές του υπό ανάλυση συστήματος. Μια απειλή είναι μια ευπάθεια που μπορεί να ενεργοποιηθεί κατά λάθος ή να γίνει εκμεταλλεύσιμη σκοπίμως. Κατά τον καθορισμό της πιθανότητας μιας απειλής, πρέπει να ληφθούν υπόψη οι ευπάθειες και οι υπάρχοντες μηχανισμοί ασφάλειας.

Βήμα 3 - Προσδιορισμός αδυναμιών

Ο προσδιορισμός των απειλών σε ένα σύστημα πληροφορικής πρέπει να περιλαμβάνει μια ανάλυση των τρωτών σημείων που συνδέονται με το περιβάλλον του συστήματος. Ο στόχος αυτού του βήματος είναι η σύνταξη ενός καταλόγου των τρωτών σημείων του συστήματος που θα μπορούσαν να αξιοποιηθούν από τις πιθανές πηγές των απειλών. Θα πρέπει να σημειωθεί ότι τα είδη των τρωτών σημείων που ενδεχομένως υπάρχουν, καθώς και η μέθοδος που απαιτείται για να καθοριστεί αν υπάρχουν αυτά τα σημεία, συνήθως ποικίλει ανάλογα με τη φύση των πληροφοριακών συστημάτων και τη φάση στην οποία είναι. Πιο συγκεκριμένα:

- Αν το πληροφοριακό σύστημα δεν έχει ακόμη σχεδιαστεί, η αναζήτηση των αδυναμιών σημείων πρέπει να επικεντρωθεί στις πολιτικές ασφάλειας του οργανισμού, στις προγραμματισμένες διαδικασίες ασφάλειας και στους ορισμούς των απαιτήσεων του συστήματος.
- Αν το πληροφοριακό σύστημα έχει τεθεί σε εφαρμογή, ο προσδιορισμός των σημείων αδυναμίας πρέπει να διευρυνθεί ώστε να περιλαμβάνει πιο

συγκεκριμένες πληροφορίες, όπως τα προγραμματισμένα χαρακτηριστικά ασφάλειας που περιγράφονται στα σχετικά έγγραφα για το σχεδιασμό της ασφάλειας καθώς και τα αποτελέσματα των δοκιμών της πιστοποίησης του συστήματος και της αξιολόγησης.

- Αν το πληροφοριακό σύστημα είναι λειτουργικό, η διαδικασία προσδιορισμού των αδυναμιών πρέπει να περιλαμβάνει ανάλυση των χαρακτηριστικών ασφάλειας του πληροφοριακού συστήματος, καθώς και τους μηχανισμούς ασφάλειας, τεχνικούς και διαδικαστικούς, που χρησιμοποιούνται για την προστασία του.

Βήμα 4 - Καταγραφή υπαρχόντων μέτρων ασφάλειας

Ο στόχος αυτού του βήματος είναι να γίνει ανάλυση των μηχανισμών ασφάλειας που έχουν υλοποιηθεί, ή προγραμματιστεί για να εφαρμοστούν από τον οργανισμό για την ελαχιστοποίηση ή την εξάλειψη της πιθανότητας μια απειλή να χρησιμοποιήσει μια ευπάθεια στο σύστημα. Για να προκύψει μια συνολική εκτίμηση της επικινδυνότητας, που υποδεικνύει την πιθανότητα ότι μια ευπάθεια μπορεί να χρησιμοποιηθεί κατά την κατασκευή του συναφούς απειλητικού περιβάλλοντος (Βήμα 5), πρέπει να ληφθεί υπόψη η εφαρμογή των εν εξελίξει ή προβλεπόμενων μηχανισμών ασφάλειας. Για παράδειγμα, μια ευπάθεια (π.χ. αδυναμία του συστήματος ή διαδικαστική αδυναμία) δεν είναι πιθανό να χρησιμοποιηθεί, ή η πιθανότητα είναι μικρή, αν υπάρχει ένα χαμηλό επίπεδο ενδιαφέροντος ή εάν υπάρχουν αποτελεσματικές διαδικασίες ασφάλειας που μπορεί να εξαλείψουν ή να μειώσουν το μέγεθος της βλάβης.

Βήμα 5 - Προσδιορισμός πιθανότητας

Για να προκύψει μια συνολική εκτίμηση της επικινδυνότητας, οι ακόλουθοι παράγοντες πρέπει να ληφθούν υπόψη:

- Κίνητρο και δυνατότητα απειλής – πηγής.
- Φύση της ευπάθειας.
- Ύπαρξη και αποτελεσματικότητα των τρεχόντων ελέγχων.

Βήμα 6 - Ανάλυση των επιπτώσεων

Το επόμενο σημαντικό βήμα για τη μέτρηση του επιπέδου της επικινδυνότητας είναι να προσδιοριστούν οι επιπτώσεις που προκύπτουν από μια επιτυχημένη πραγματοποίηση μια απειλής. Πριν αρχίσει η ανάλυση των επιπτώσεων, είναι αναγκαίο να έχουν ληφθεί οι ακόλουθες απαραίτητες πληροφορίες:

- Η αποστολή του συστήματος (π.χ. οι διαδικασίες που εκτελούνται από το πληροφοριακό σύστημα).

- Η κριτιμότητα του συστήματος και των δεδομένων (π.χ. η αξία ή η σημασία ενός συστήματος σε έναν οργανισμό).
- Η ευαισθησία του συστήματος και των δεδομένων.
- Η επίπτωση της εκδήλωσης μια απειλής μπορεί να περιγραφεί από την άποψη της απώλειας ή της υποβάθμισης οποιωνδήποτε από τους ακόλουθους τρεις στόχους ασφάλειας (ή και συνδυασμού τους): της ακεραιότητας, της διαθεσιμότητας και της εμπιστευτικότητας.

Βήμα 7 - Προσδιορισμός επικινδυνότητας

Ο σκοπός αυτού του βήματος είναι να αξιολογηθεί το επίπεδο της επικινδυνότητας για το πληροφορικό σύστημα. Ο προσδιορισμός της επικινδυνότητας για ένα συγκεκριμένο ζεύγος απειλής/ευπάθειας μπορεί να εκφραστεί ως συνάρτηση:

- Της πιθανότητας να πραγματοποιηθεί μια συγκεκριμένη απειλή.
- Του μεγέθους των επιπτώσεων που θα προκύψουν από την πραγματοποίηση της απειλής.
- Της επάρκειας των ισχυουσών ή προβλεπόμενων μηχανισμών ασφάλειας για τη μείωση ή την εξάλειψη των απειλών.

Σύμφωνα με το NIST 800-30, η επικινδυνότητα είναι συνάρτηση της πιθανότητας να πραγματοποιηθεί μια συγκεκριμένη απειλή (η οποία εκμεταλλεύεται συγκεκριμένες αδυναμίες) και των επιπτώσεων της εν λόγω ανεπιθύμητης απειλής στην ομαλή λειτουργία του πληροφοριακού συστήματος. Ο τελικός προσδιορισμός του επιπέδου της επικινδυνότητας (Υψηλό, Μέτριο, Χαμηλό) υπολογίζεται από τον πολλαπλασιασμό της πιθανότητας της απειλής (Υψηλή, Μέτρια, Χαμηλή) και της επίπτωσης της απειλής (Υψηλή-Μεσαία-Χαμηλή).

Ο πίνακας που ακολουθεί είναι μια 3x3 μήτρα της πιθανότητας εκδήλωσης μιας απειλής (Υψηλή, Μέτρια, Χαμηλή) και της επίπτωσης της απειλής (Υψηλή, Μέτρια, Χαμηλή). Η επικινδυνότητα προκύπτει ως το ακόλουθο γινόμενο: *Επικινδυνότητα = Πιθανότητα Απειλής x Επίπτωση Απειλής*.

Πιθανότητα Απειλής	Επίπτωση Απειλής		
	Χαμηλή (10)	Μέτρια (50)	Υψηλή (100)
Υψηλή (1.0)	Χαμηλό $10 \times 1.0 = 10$	Μέτριο $50 \times 1.0 = 50$	Μέτριο $100 \times 1.0 = 100$
Μέτρια (0.5)	Χαμηλό $10 \times 0.5 = 5$	Μέτριο $50 \times 0.5 = 25$	Μέτριο $100 \times 0.5 = 50$
Χαμηλή (0.1)	Χαμηλό $10 \times 0.1 = 1$	Χαμηλό $50 \times 0.1 = 5$	Χαμηλό $100 \times 0.1 = 10$

Πίνακας 10: Μήτρα υπολογισμού επικινδυνότητας

Το δείγμα της μήτρας που παρουσιάζεται στον πίνακα δείχνει πώς προκύπτουν τα συνολικά επίπεδα επικινδυνότητας (Υψηλό, Μέσο και Χαμηλό επίπεδο). Ο καθορισμός αυτών των επιπέδων μπορεί να είναι υποκειμενικός. Το σκεπτικό για αυτήν την αιτιολόγηση μπορεί να εξηγηθεί στα πλαίσια της πιθανότητας που έχει δοθεί για κάθε ενδεχόμενο κίνδυνου και της τιμής που έχει δοθεί για κάθε επίπεδο επιπτώσεων.

Στη συνέχεια περιγράφονται τα επίπεδα επικινδυνότητας. Η κλίμακα, με αξιολογήσεις ως Υψηλό, Μέτριο και Χαμηλό, αντιπροσωπεύει το βαθμό ή το επίπεδο επικινδυνότητας ενός συστήματος πληροφορικής αν χρησιμοποιηθεί μια συγκεκριμένη ευπάθεια. Η κλίμακα επικινδυνότητας παρουσιάζει επίσης τα μέτρα ασφάλειας που πρέπει να λάβουν ανώτερα διοικητικά στελέχη για κάθε επίπεδο επικινδυνότητας.

- **Υψηλό Επίπεδο:** Εάν μια παρατήρηση ή εύρημα αξιολογείται ως υψηλής επικινδυνότητας, υπάρχει μεγάλη ανάγκη για λήψη διορθωτικών μέτρων.
- **Μέτριο Επίπεδο:** Εάν μια παρατήρηση βαθμολογείται ως μέσης επικινδυνότητας, χρειάζονται διορθωτικές ενέργειες και πρέπει να αναπτυχθεί ένα σχέδιο για να ενσωματωθούν αυτές οι ενέργειες μέσα σε εύλογο χρονικό διάστημα.
- **Χαμηλό Επίπεδο:** Εάν μια παρατήρηση περιγράφεται ως χαμηλής επικινδυνότητας, η διοίκηση του οργανισμού πρέπει να καθορίσει αν απαιτούνται διορθωτικές ενέργειες ή να αποφασίσει την αποδοχή του κινδύνου.

Βήμα 8 - Προτεινόμενα μέτρα ασφάλειας

Σε αυτό το βήμα της διαδικασίας, παρέχονται οι μηχανισμοί ασφάλειας που θα μπορούσαν να περιορίσουν ή να εξαλείψουν τους κινδύνους που εντοπίστηκαν, όπως αρμόζει στις δραστηριότητες του οργανισμού. Ο στόχος των προτεινόμενων μηχανισμών ασφάλειας είναι να μειώσουν το επίπεδο της επικινδυνότητας για το πληροφοριακό σύστημα και για τα δεδομένα του σε ένα αποδεκτό επίπεδο. Οι ακόλουθοι παράγοντες πρέπει να εξετάζονται κατά τη σύσταση των προτεινόμενων μηχανισμών ασφάλειας και των εναλλακτικών λύσεων για την ελαχιστοποίηση ή την εξάλειψη των εντοπιζόμενων κινδύνων:

- Η αποτελεσματικότητα των προτεινόμενων επιλογών (π.χ. συμβατότητα του συστήματος).

- Νομοθεσία και κανονιστικές ρυθμίσεις.
- Οργανωτική πολιτική.
- Επιχειρησιακές επιπτώσεις.
- Ασφάλεια και αξιοπιστία.

Τα μέτρα ασφάλειας είναι τα αποτελέσματα της διαδικασίας αξιολόγησης του κινδύνου και συμβάλλουν στη διαδικασία μείωσης της επικινδυνότητας. Κατά τη διάρκεια της διαδικασίας αυτής, τα μέτρα αξιολογούνται, ιεραρχούνται και υλοποιούνται. Δεν είναι δυνατό να μπορούν να εφαρμοστούν όλα τα μέτρα για τη μείωση των επιπτώσεων. Για τον προσδιορισμό απαραίτητων μέτρων ασφάλειας πρέπει να πραγματοποιηθεί ανάλυσης κόστους – οφέλους, ώστε να αποδειχθεί ότι το κόστος της εφαρμογής των μέτρων μπορεί να δικαιολογηθεί από τη μείωση του επιπέδου της επικινδυνότητας. Επιπλέον, οι επιχειρησιακές επιπτώσεις (π.χ. επιπτώσεις στην απόδοση του συστήματος) και η σκοπιμότητα (π.χ. τεχνικές προδιαγραφές, αποδοχή των χρηστών) της εισαγωγής της προτεινόμενης επιλογής πρέπει να αξιολογηθούν προσεκτικά κατά τη διάρκεια της διαδικασίας μείωσης της επικινδυνότητας.

Βήμα 9 - Αποτελέσματα Τεκμηρίωσης

Μετά την ολοκλήρωση της αξιολόγησης επικινδυνότητας, τα αποτελέσματα πρέπει να τεκμηριωθούν με επίσημη έκθεση ή ενημέρωση. Η έκθεση διαχείρισης βοηθά τα ανώτερα διευθυντικά στελέχη στη λήψη αποφάσεων σχετικά με την πολιτική, τα διαδικαστικά θέματα, τον προϋπολογισμό και το σύστημα λειτουργίας και διαχείρισης των αλλαγών. Αντίθετα από την έκθεση ελέγχου ή έρευνας, η έκθεση αξιολόγησης επικινδυνότητας δε θα πρέπει να παρουσιάζεται με κατηγορητικό τρόπο, αλλά ως μια συστηματική και αναλυτική προσέγγιση για την εκτίμηση της. Έτσι, τα ανώτερα διοικητικά στελέχη μπορούν να κατανοήσουν τους κινδύνους και να διαθέσουν πόρους για τη μείωση και τη διόρθωση ενδεχόμενων απωλειών. Για το λόγο αυτό, ορισμένοι ειδικοί του χώρου προτιμούν να αντιμετωπίζουν τα ζευγάρια απειλής/ευπάθειας ως παρατηρήσεις αντί για διαπιστώσεις στις εκθέσεις αξιολόγησης κινδύνου. Τα βήματα 2, 3, 4, και 6, μπορούν να διεξάγονται παράλληλα αφού το Βήμα 1 ολοκληρωθεί.

Η μέθοδος είναι συμβατή με το πρότυπο ISO / IEC 27001:2005 και λαμβάνει υπόψη της όλες τις προϋποθέσεις για την καθιέρωση και εφαρμογή ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριακών Συστημάτων (ISMS).

5.4 Μέθοδος EBIOS

Η μέθοδος EBIOS - Expression des Besoins et Identification des Objectifs de Securite (DCSSI, 2004) αναπτύχθηκε από τη Γαλλική Γενική Γραμματεία Εθνικής Άμυνας με στόχο την αξιολόγηση και την αντιμετώπιση κινδύνων σε πληροφοριακά συστήματα υλοποιώντας τα εξής βήματα:

- Προσδιορισμό του συστήματος και των αλληλεξαρτήσεών του.
- Προσδιορισμό και στη συνέχεια αξιολόγηση των πιθανών απειλών.
- Αξιολόγηση της επικινδυνότητας.
- Προσδιορισμό και επιλογή των μέτρων προστασίας.

Η μέθοδος είναι απλή και αρκετά ευέλικτη, ώστε να μπορεί να χρησιμοποιηθεί σε κάθε είδους οργανισμό ανεξάρτητα μεγέθους. Η προσέγγιση που ακολουθεί η συγκεκριμένη μέθοδος είναι κατά βάση ποιοτική, ενώ παρέχει τη δυνατότητα για ανάπτυξη συνεργατικών δραστηριοτήτων. Τέλος, το βασικό της μειονέκτημα είναι η έλλειψη κάποιου πληροφοριακού εργαλείου ώστε να διευκολύνεται η εφαρμογή της.

5.5 Μέθοδος/Εργαλείο OCTAVE

Η μέθοδος OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) αναπτύχθηκε από το Carnegie Mellon University των Η.Π.Α. για την εκτίμηση της στρατηγικής και το σχεδιασμό της ασφάλειας της πληροφορίας. Η μέθοδος υλοποιείται σε τρία βήματα (Alberts & Dorofee, 2002):

1. Δημιουργία προφίλ απειλών με βάση τους διαθέσιμους πόρους.
2. Εντοπισμός ευπαθειών.
3. Ανάπτυξη στρατηγικής και πλάνων ασφάλειας.

Βασίζεται στη χρήση ομάδων εργασίας (workshop-based) και ερωτηματολογίων ενθαρρύνοντας έτσι την ανοικτή συζήτηση και τη συνεργασία. Η προσέγγιση που ακολουθεί η συγκεκριμένη μέθοδος βασίζεται σε μια ποιοτική κλίμακα η οποία δε λαμβάνει υπόψη τη γνώση σχετικά με το εταιρικό περιβάλλον του οργανισμού.

Τέλος, υπάρχει η δυνατότητα χρήσης ενός υπολογιστικού εργαλείου για την αυτοματοποιημένη χρήση της μεθόδου από το Advanced Technology Institute.

5.6 Μέθοδος MEHARI

Η μέθοδος MEHARI αποτελεί μια ακόμα ποιοτική προσέγγιση για την ανάλυση και τη διαχείριση της επικινδυνότητας που δημιουργήθηκε από τον οργανισμό CLUSIF (Club de la Securite de l'Information Francais) (El Fray, 2012). Για την υλοποίησή της προβλέπονται βήματα που αφορούν στον προσδιορισμό του πλαισίου εφαρμογής, στην ανάλυση και κατηγοριοποίηση των αγαθών, στην αναγνώριση, στην ανάλυση, στην αξιολόγηση και στη διαχείριση του κινδύνου καθώς και στα αποδεκτά επίπεδα κινδύνου. Η συγκεκριμένη μέθοδος είναι κατάλληλη για μεσαίου και μεγάλου μεγέθους οργανισμούς ενώ παρέχει περιορισμένες μόνο δυνατότητες συνεργατικής δράσης.

5.7 Μέθοδος/Εργαλείο CORAS

Η μέθοδος CORAS είναι ένα πλαίσιο εκτίμησης επικινδυνότητας που αποτελείται από τέσσερα στοιχεία (Lund et al., 2010):

1. Μια μέθοδο/διαδικασία.
2. Μια γλώσσα μοντελοποίησης κινδύνων.
3. Ένα απλό εργαλείο με τη χρήση της γλώσσας μοντελοποίησης κινδύνων για τη δημιουργία διαγραμμάτων και μοντέλων σε κάθε στάδιο της εκτίμησης.
4. Ένα εργαλείο για τη βηματική υλοποίησης της μεθόδου CORAS.

Η μέθοδος CORAS αναπτύχθηκε ως μια μέθοδος υποστηριζόμενη από ένα εργαλείο για την εκτίμηση κινδύνων βάσει μοντέλων προσομοίωσης διεργασιών. Βασίστηκε στη γλώσσα UML για τη μοντελοποίηση των χαρακτηριστικών εκτίμησης επικινδυνότητας και στη συνέχεια εξελίχθηκε σε μια συγκεκριμένη «γλώσσα κινδύνων» που χρησιμοποιείται ως κοινή γλώσσα μεταξύ εμπλεκόμενων από διαφορετικούς τομείς κρίσιμων υποδομών παρέχοντας κοινή κατανόηση των όρων και των σχέσεων που χρησιμοποιούνται στην εκτίμηση επικινδυνότητας.

Κάνει εκτεταμένη χρήση των υφιστάμενων μεθόδων εκτίμησης επικινδυνότητας, όπως η ανάλυση SWOT (strengths-weaknesses-opportunities-threats), η ανάλυση

κινδύνων και λειτουργικότητας (Hazards and Operability Analysis - HazOp) και η ανάλυση τύπων διαταραχής και επιπτώσεων (FMEA - failure mode effects analysis) και περιγράφει συνδυαστικές μεθόδους που μπορούν να χρησιμοποιούν τις εκροές μιας τεχνικής ως εισροές για μια άλλη με σκοπό να δημιουργήσουν νέους κινδύνους (ή περιοχές ενδιαφέροντος). Αυτό σημαίνει ότι η πλήρης εφαρμογή μιας τέτοιας τεχνικής θα είναι εξαντλητική εάν εφαρμοστεί πλήρως, αλλά κάθε δραστηριότητα μπορεί να τερματιστεί όταν ο υπεύθυνος αποφασίσει ότι τα αποτελέσματα είναι επαρκώς ακριβή. Η μέθοδος CORAS περιλαμβάνει τη χρήση ειδικών πινάκων και διαγραμμάτων για κάθε στάδιο της διαδικασίας εκτίμησης κινδύνων οι οποίοι (όπως και με τις μεθόδους ανάλυσης) χρησιμοποιούνται διαδοχικά για την παροχή εισροών σε μετέπειτα δραστηριότητες.

Η μέθοδος CORAS φαίνεται να είναι γενικά εφαρμόσιμη στους περισσότερους τύπους υποδομών. Ωστόσο, χρειάζεται κατάλληλη εκπαίδευση των χρηστών για να μη γίνει υπερεκτίμηση ή υποτίμηση του επιπέδου ενός κινδύνου, ενώ από την άλλη να είναι σε θέση οι χρήστες να προσδιορίσουν τις περιοχές ενδιαφέροντος με ακρίβεια, καθώς δεν παρέχει κανένα μέσο εντοπισμού της σημασίας κάθε κινδύνου έναντι κάποιου άλλου, εκτός από τη σύγκριση των τιμών των κινδύνων (συχνότητες και συνέπειες).

5.8 Μέθοδος της Χάγης (DHM)

Η μέθοδος διαχείρισης ασφάλειας DHM (De Haagse Methodiek – The Hague Method, 1987) περιλαμβάνει μια φάση εκτίμησης επικινδυνότητας (ονομάζεται Έλεγχος Εσωτερικής Ασφάλειας) καθώς και μια φάση διαχείρισης επικινδυνότητας (ονομάζεται Πακέτο Διαχείρισης Ασφάλειας) (Uijt de Haag & Ale, 1999).

Ο εσωτερικός έλεγχος ασφάλειας αποτελείται από τα παρακάτω στοιχεία:

- Πολιτική για την ασφάλεια.
- Προφίλ και σενάρια κινδύνων.
- Απογραφή και χαρακτηρισμός πόρων.
- Καταγραφή μέτρων ασφάλειας και της κατάστασής τους.
- Οργάνωση ασφάλειας: ανάλυση βάσει χρόνου (ανίχνευση, καθυστέρηση και απόκριση) των συνεπειών των σεναρίων κινδύνων.

- Αποτελεσματικότητα μέτρων ασφαλείας, σε σχέση με τα σενάρια κινδύνων και βάσει του επιπέδου έλεγχου πάνω σε αυτά.
- Αδιάλειπτες συνδέσεις μεταξύ οργανισμού εσωτερικής και εξωτερικής ασφάλειας.
- Προτάσεις βελτίωσης (όποτε είναι απαραίτητο).

Η διασφάλιση ποιότητας επιτυγχάνεται μέσω εσωτερικών έλεγχων ασφαλείας σε τακτά χρονικά διαστήματα και διατηρώντας ενημερωμένο το πακέτο διαχείρισης ασφάλειας. Η μέθοδος έχει τη δική της δομή έλεγχου και πιστοποίησης.

Η μέθοδος DHM αφορά σε φυσικούς πόρους, οργανωτικούς πόρους, ανθρώπινο δυναμικό και στις ΤΠΕ. Το επίκεντρο της μεθόδου αυτής είναι οι απειλές που προκαλούνται από ανθρώπινη πρόθεση. Σκοπός της μεθόδου είναι να δημιουργήσει, να διαχειρίζεται και να συντηρεί ένα αποτελεσματικό σύστημα διαχείρισης κινδύνων, που εμποδίζει και προστατεύει την περιουσία μιας εταιρείας. Η μέθοδος παρέχει συγκρίσιμα αποτελέσματα μεταξύ των εκτιμήσεων, ενώ εφαρμόζεται σε επίπεδα που ποικίλουν από εταιρείες μέχρι και πολυεθνικές ελεγκτικές αρχές αλλά και σε εγκαταστάσεις πυρηνικής ενέργειας. Τα ισχυρά σημεία της μεθόδου είναι το εμπεριστατωμένο μεθοδολογικό υπόβαθρο, η πληρότητά της εντός του προκαθορισμένου πλαισίου εργασίας και η ωριμότητά της.

5.9 Μέθοδος PAS 55

Η μέθοδος εκτίμησης PAS 55 αναπτύχθηκε το 2003 από διάφορες οργανώσεις υπό την ηγεσία του Institute of Asset Management και αναθεωρήθηκε το 2008. Είναι βασισμένη στην προσέγγιση Plan-Do-Check-Act των συστημάτων διαχείρισης ποιότητας. Στηρίχτηκε στη δομή των υπαρχόντων προτύπων προκεμένου να διευκολυνθεί η κατανόηση και η υιοθέτηση. Περιλαμβάνει ένα σύνολο οδηγιών που εστιάζουν στη διαχείριση των φυσικών πόρων. Οι ανθρώπινοι πόροι, οι τεχνολογικοί πόροι που αφορούν στα συστήματα πληροφορικής και οι πόροι που αφορούν στην οργάνωση λαμβάνονται υπόψη στη μέθοδο μόνο εφόσον έχουν άμεση επίπτωση στη διαχείριση των φυσικών υποδομών.

Αν και το πλαίσιο της μεθόδου είναι ολιστικό, η εστίαση δεν είναι. Στην πραγματικότητα η μέθοδος διακρίνει πέντε κατηγορίες πόρων (Woodhouse, 2006):

- Φυσικούς πόρους (φυσικοί πόροι, υποδομές, μηχανήματα, εργοστάσια, εξοπλισμός, κτήρια, συστήματα πληροφορικής).
- Ανθρώπινους πόρους (ηγεσία, διοίκηση, εργατικό δυναμικό, δεξιότητες, γνώσεις και πείρα).
- Οικονομικούς πόρους (μετρητά, επενδύσεις, ιδία κεφάλαια, φερεγγυότητα).
- Πληροφοριακούς πόρους (δεδομένα και πληροφορίες).
- Άυλους πόρους (φήμη, εντύπωση πελατών και προσωπικού, δημόσια εικόνα/σχέσεις, αξία του οργανισμού, άδειες, ευρεσιτεχνίες, εμπορικά σήματα, πνευματικά δικαιώματα και φιλοσοφία).

Η εκτίμηση όλων των κινδύνων αποτελεί ένα από τα στοιχεία της μεθόδου. Χαρακτηρίζεται από οδηγίες για τη διαχείριση πόρων και όχι την παροχή μιας στατικής μεθόδου. Τα βασικά βήματα που προτείνονται για να εξασφαλίσουν μια συστηματική προσέγγιση είναι τα παρακάτω:

- Ταξινόμηση πόρων.
- Αναγνώριση αξιολόγηση κινδύνων.
- Αναγνώριση των υφιστάμενων μέτρων ελέγχου των κινδύνων.
- Καθορισμός επιπέδου κινδύνου.
- Καθορισμός ανοχής των κινδύνων.
- Προετοιμασία και αξιολόγηση επιλογών και σχεδίων δράσης για βελτίωση των μέτρων ελέγχου των κινδύνων.
- Εξέταση της επάρκειας του σχεδίου δράσης.
- Συντήρηση νέων και υφιστάμενων μέτρων ελέγχου κινδύνων και διασφάλιση της αποτελεσματικότητάς τους.

Τα πλεονεκτήματα αυτής της μεθόδου είναι η καλή συμμόρφωση με τα πρότυπα και το γεγονός ότι προσφέρονται μαθήματα και παρέχεται σχετική πιστοποίηση. Αν και η μέθοδος δεν είναι στατική, οι οδηγίες υποστηρίζουν το χρήστη ως ένα βαθμό σε κάθε του βήμα.

5.10 Μέθοδος Handreiking Risico-analyse (Guide to Risk – Ολλανδική μέθοδος)

Ο Ολλανδικός οδηγός ανάλυσης κινδύνων αποτελείται από πέντε βήματα (Ale, 2002):

1. Προετοιμασία: ορισμός πεδίου εφαρμογής και προσέγγιση της εκτίμησης κινδύνων.
2. Ανάλυση εξάρτησης: αναγνώριση εσωτερικών και εξωτερικών παραγόντων ζωτικής σημασίας για τη λειτουργία του οργανισμού.
3. Ανάλυση απειλών: καθορισμός των αντιπάλων, των προθέσεων και των δυνατοτήτων τους.
4. Ανάλυση ευπάθειας: βάσει των εκτιμώμενων απειλών, αξιολογείται η ανθεκτικότητα του οργανισμού απέναντι σε αυτές τις απειλές.
5. Αξιολόγηση κινδύνων: εκτιμώνται οι πιθανές επιπτώσεις των σχετικών απειλών και αξιολογούνται οι παράγοντες κινδύνου μεταξύ τους.

Η συγκεκριμένη μέθοδος αποτελείται από δέκα πρακτικά μοντέλα εκτίμησης επικινδυνότητας και πίνακες ελέγχου που έχουν ενσωματωθεί σε έναν ενιαίο οδηγό. Παρέχει χρήσιμες πληροφορίες για τη διεξαγωγή μιας επιτυχούς εκτίμησης επικινδυνότητας. Ασχολείται με όλους τους πόρους, αλλά εστιάζει στην ανθρώπινη πρόθεση και επίσης θεωρεί απειλές τα κλιμακωτά συμβάντα, ενώ επίσης περιλαμβάνει λίστα ελέγχου απειλών. Επιπλέον η μέθοδος παρέχει μια προτεινόμενη προσέγγιση (μη υποχρεωτική) της ποσοτικής εκτίμησης πιθανοτήτων και επιδράσεων, που είναι σημαντική για τη λήψη συγκρίσιμων αποτελεσμάτων.

Το ισχυρό σημείο αυτής της προσέγγισης είναι ότι περιλαμβάνονται οι πίνακες ελέγχου για τον καθορισμό των πόρων και τον προγραμματισμό της εκτίμησης κινδύνων.

5.11 Μέθοδος NRB

Το 2007, το Ολλανδικό Υπουργείο Εσωτερικών αποφάσισε να υιοθετήσει μια νέα στρατηγική για την εθνική ασφάλεια και προστασία (Pruyt et al., 2013). Η στρατηγική καλύπτει δύο ευδιάκριτες φάσεις, η πρώτη εκ των οποίων αφορά την ανάλυση των απειλών και των κινδύνων. Η δεύτερη φάση στηρίζεται στα αποτελέσματα της προηγούμενης ανάλυσης και στοχεύει στην ανάπτυξη επαρκών πολιτικών, ώστε να διαχειριστεί τους προσδιορισμένους κινδύνους ισόρροπα, δίνοντας έμφαση στην προετοιμασία, πρόληψη, απόκριση και παρακολούθηση.

Προκειμένου να υποστηριχθεί η πρώτη φάση και να προσδιοριστούν οι παράγοντες κινδύνου με έναν επιστημονικά αιτιολογημένο τρόπο, αναπτύχθηκε μια μέθοδος

εκτίμησης επικινδυνότητας από μια διεπιστημονική ομάδα έργου. Η μέθοδος αυτή υποστηρίζει μια ομοιόμορφη ανάλυση όλων των κινδύνων σε όλους τους τομείς, εξασφαλίζοντας συμβατά αποτελέσματα που επιτρέπουν τις συγκρίσεις μεταξύ απειλών και τομέων. Η μέθοδος εκτίμησης κινδύνων έχει σχεδιαστεί για να αξιολογεί τις απειλές στις κρίσιμες υποδομές και τις επιπτώσεις της δυσλειτουργίας τους σε εθνική κλίμακα και να εκτιμά τον κοινωνικό κίνδυνο που μπορεί να ενέχει μια δυσλειτουργία τους (π.χ. μετανάστευση πληθυσμού, εξτρεμισμός).

Η μέθοδος NRB έχει ως βασικό στοιχείο το γεγονός ότι οι απειλές πρέπει να περιγράφονται υπό τη μορφή σεναρίων και αποτελείται από τα παρακάτω βήματα:

- Διατύπωση ενός αντιπροσωπευτικού και πλήρους συνόλου σεναρίων για την περιγραφή των υπό μελέτη απειλών.
- Αξιολόγηση των επιπτώσεων καθενός από τα σενάρια.
- Αξιολόγηση της πιθανότητας για καθένα από τα σενάρια. Η μέθοδος εκτίμησης των πιθανοτήτων των κινδύνων διακρίνει τους κινδύνους σε απειλές (κακόβουλες αιτίες) και σε ατυχήματα (μη-κακόβουλες αιτίες) βάσει στατιστικών στοιχείων ή μετά από αξιολόγηση ειδικών.
- Ανάλυση του απορρέοντος κινδύνου που απεικονίζεται σε ένα δισδιάστατο διάγραμμα κινδύνου.

Η μέθοδος περιλαμβάνει το σύνολο των πόρων και των τύπων των απειλών, ενώ εφαρμόζει έναν ορθολογικό ποσοτικό μηχανισμό βαθμολόγησης, που επιτρέπει τη σύγκριση εκτιμήσεων. Χρησιμοποιεί έναν εξαιρετικά μεγάλο αριθμό δέκα (10) σταθμισμένων κριτηρίων επιπτώσεων, που περιλαμβάνουν τόσο τις φυσικές επιπτώσεις (οικονομικές απώλειες, θάνατοι, κ.λπ.) όσο και λοιπές επιπτώσεις (κοινωνικός ή ψυχολογικός αντίκτυπος, περιβαλλοντικές επιπτώσεις, κ.λπ.). Η μέθοδος καθορίζει ποιες απειλές και επιπτώσεις πρέπει να αξιολογούνται.

Τα δυνατά σημεία της μεθόδου συνίστανται στο ότι παρέχει μια σύγκριση των διαφορετικών τύπων απειλής προκειμένου να ιεραρχήσει τις απειλές και ότι αυτές οι απειλές διατυπώνονται σε ένα ή περισσότερα σενάρια που είναι εύληπτα. Αυτό είναι σημαντικό, δεδομένου ότι η μέθοδος περιλαμβάνει ένα ευρύ φάσμα εμπλεκόμενων φορέων ώστε να εξασφαλιστεί η ευρεία αποδοχή της εκτίμησης. Ένα άλλο πλεονέκτημα της μεθόδου είναι ότι ενσωματώνει προσεγγίσεις για την σύγκλιση

διαφορετικών αντιλήψεων σχετικά με τη σημασία που έχουν οι διάφοροι τύποι επιπτώσεων.

5.12 Μέθοδοι βάσει οργανισμού ISF

Ο διεθνής οργανισμός ISF έχει εκδώσει αρκετές πρακτικές, μεθόδους και εργαλεία για την Αποτίμηση και Διαχείριση της Επικινδυνότητας, τα οποία συνεχώς ανανεώνει και επικαιροποιεί. Οι πρακτικές, οι μέθοδοι και τα εργαλεία είναι στενά συνδεόμενα μεταξύ τους, αναφέρονται συχνά το ένα στο άλλο και μπορούν να λειτουργήσουν ως συμπληρωματικά, ανάλογα με το εύρος της ανάλυσης που θέλει κανείς να πετύχει και την περιοχή μελέτης. Όλα τα εργαλεία και οι μέθοδοι που παρέχει ο οργανισμός ISF βασίζονται στο Πρότυπο του ISF 2011 και είναι τα παρακάτω (Wahlgren et al., 2013):

- FIRM (Fundamental Information Risk Management) ή/και FIRM Scorecard.
- Information Security Status Survey.
- Information Risk Analysis Methodologies (IRAM) project.
- SARA (Simple to Apply Risk Analysis).
- SPRINT (Simplified Process for Risk Identification).

Σαν γενικότερη μέθοδο αυτή του ISF, με τη σειρά των εργαλείων και των μεθόδων που διαθέτει, καλύπτει πλήρως, αναλυτικά και επαρκώς όλα τα βήματα και στη Εκτίμηση της Επικινδυνότητας (Risk Assessment) όπως επίσης και στη Διαχείριση της Επικινδυνότητας (Risk Management) των πληροφοριακών συστημάτων. Το επίπεδο ανάλυσης είναι λεπτομερές τόσο στο κομμάτι της διαχείρισης (Management) και των Λειτουργιών (Operational) όσο και στο τεχνικό (Technical).

Η μέθοδος FIRM είναι μια αναλυτική μέθοδος για την παρακολούθηση και τον έλεγχο της επικινδυνότητας των πληροφοριών σε επιχειρησιακό επίπεδο. Έχει κατασκευαστεί ως μια πρακτική προσέγγιση για την παρακολούθηση της αποτελεσματικότητας της ασφάλειας των πληροφοριών. Ως εκ τούτου, επιτρέπει τη συστηματική διαχείριση της επικινδυνότητας σε επιχειρήσεις όλων των μεγεθών. Περιλαμβάνει ολοκληρωμένες κατευθυντήριες γραμμές για να εξασφαλιστεί η υποστήριξη των προτεινόμενων μέτρων από το ανθρώπινο δυναμικό, γεγονός που θα οδηγήσει στην ευκολότερη υιοθέτηση και λειτουργία τους.

Το εργαλείο Information Security Status Survey είναι ένα ολοκληρωμένο εργαλείο διαχείρισης της επικινδυνότητας που αξιολογεί ένα μεγάλο φάσμα των μέτρων ασφάλειας που χρησιμοποιούνται από τους οργανισμούς ώστε να περιορίσουν τους επιχειρηματικούς κινδύνους που σχετίζονται με τα πληροφοριακά τους συστήματα.

Η μέθοδος SARA είναι μια αναλυτική μέθοδος για την ανάλυση της επικινδυνότητας των πληροφοριών σε συστήματα που υποστηρίζουν κρίσιμες υποδομές. Αποτελείται από 4 στάδια: σχεδιασμός, αναγνώριση των επιχειρηματικών απαιτήσεων στον τομέα της ασφάλειας, εκτίμηση τρωτοτήτων και απαιτήσεις μέτρων ασφάλειας και, τέλος, τεκμηρίωση.

Συγκρινόμενη με τη μέθοδο SARA, η μέθοδος SPRINT είναι μια σχετικά γρήγορη και εύκολη μέθοδος. Χρησιμοποιείται για την εκτίμηση των επιπτώσεων στις επιχειρήσεις και για την ανάλυση της επικινδυνότητας των πληροφοριών σε σημαντικά αλλά όχι κρίσιμα συστήματα πληροφοριών. Η μέθοδος SPRINT αρχικά αποφασίζει το επίπεδο της επικινδυνότητας ενός συστήματος. Αφού οι κίνδυνοι γίνουν πλήρως κατανοητοί, η μέθοδος SPRINT βοηθά στον καθορισμό των επόμενων βημάτων και, η διαδικασία ολοκληρώνεται με την παραγωγή ενός συμφωνημένου σχεδίου δράσης για τον περιορισμό των κινδύνων σε αποδεκτά όρια. Γενικά, η μέθοδος SPRINT μπορεί να βοηθήσει στον προσδιορισμό των αδύναμων σημείων των υπαρχόντων συστημάτων και να προτείνει τα μέτρα ασφάλειας που απαιτούνται για την προστασία από αυτούς τους κινδύνους. Επιπρόσθετα, μπορεί να καθορίσει τις απαιτήσεις ασφάλειας για τα συστήματα υπό ανάπτυξη και τους ελέγχους που απαιτούνται για την ικανοποίηση των απαιτήσεων αυτών.

Η μέθοδος IRAM αποτελείται από τρείς διακριτές φάσεις και τα αποτελέσματα της μιας είναι σημείο αναφοράς της επόμενης. Υπάρχουν προκαθορισμένα σύνολα με βάση τα οποία ο αναλυτής κρίνει το εύρος της επίπτωσης σε επιχειρησιακό επίπεδο και τα αποτελέσματα συνυπολογίζονται αυτόματα και συνολικά. Στο τρίτο και τελευταίο κομμάτι υπάρχει μια βάση με πάνω από 100 μηχανισμούς ασφάλειας και ο αναλυτής, βάσει των πιο υψηλών κινδύνων και επιχειρησιακών αντίκτυπων που έχει αναγνωρίσει στα δύο προηγούμενα στάδια, καθώς επίσης και άλλων παραμέτρων που συνυπολογίζονται από τη μέθοδο IRAM, επιλέγει τους απαραίτητους μηχανισμούς για να υλοποιήσει στον εκάστοτε οργανισμό για τον οποίο γίνεται η εργασία. Κατά σειρά οι φάσεις της μεθόδου αυτής είναι:

- Ανάλυση Επιχειρησιακής Επίπτωσης (Business Impact Analysis).
- Εκτίμηση Απειλών και Ευπαθειών (Threat and Vulnerability Assessment).
- Επιλογή Μηχανισμών Ασφάλειας (Controls Selection).

Η μέθοδος IRAM υλοποιεί τα ISO/IEC 27001 και 27001 και τη μέθοδο Cobit 4.1. Αυτό μπορεί να θεωρηθεί μεγάλο συγκριτικό πλεονέκτημα σε σχέση με τις άλλες μεθόδους, αφού η αξιολόγηση εφαρμόζεται σε ένα πληροφοριακό σύστημα μεν, αλλά λαμβάνεται υπόψη και το περιβάλλον που το πλαισιώνει και κυρίως η επιχειρησιακή δραστηριότητα.

Το Πρότυπο του ISF 2011 (Standard of Good Practice), στο οποίο είναι βασισμένη η μέθοδος IRAM, είναι πλήρως ευθυγραμμισμένο με τις απαιτήσεις για ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ISMS) που καθορίζονται από το ISO/IEC 27001 και παρέχει μια ευρύτερη και βαθύτερη κάλυψη των σημείων ελέγχου και των αντικειμενικών τους στόχων που περιλαμβάνονται στο ISO/IEC 27002. Το Πρότυπο ISF του 2011 κρίνεται ιδανικό πλαίσιο με τις μεθόδους που προσφέρει για τη διευκόλυνση στην αξιολόγηση κατά ISO/IEC 27001.

5.13 Εργαλείο CARVER2

Το CARVER2 είναι ένα εργαλείο που αναπτύχθηκε από το US NI2 Centre for Infrastructure Expertise προκειμένου να εξυπηρετήσει τις ανάγκες ανάλυσης των κρίσιμων υποδομών κυρίως από την οπτική γωνία των υπεύθυνων για τη χάραξη πολιτικής ασφάλειας (Markowsky, 2011). Για την εφαρμογή αυτής της μεθόδου, αναπτύχθηκε ένα αυτόνομο πληροφοριακό εργαλείο και μια έκδοση διακομιστή/πελάτη (CARVER2Web). Η μέθοδος καλύπτει τις τρομοκρατικές απειλές καθώς επίσης και τις φυσικές καταστροφές, εφαρμόζοντας μια κοινή προσέγγιση για όλους τους κινδύνους. Αυτή η μέθοδος εφαρμόζεται μέσω έξι διαφορετικών κριτηρίων βάσει των οποίων μελετάται ένας πόρος ή μια υποδομή. Η κριτιμότητα (criticality) είναι το μέρος εκτίμησης της μεθόδου που αφορά τις επιπτώσεις. Είναι αξιοσημείωτο ότι συμφωνεί με τα θεμελιώδη κριτήρια της Οδηγίας 114/2008 (για την προστασία Ευρωπαϊκών Υποδομών Ζωτικής Σημασίας) από πλευράς κατηγοριών επιπτώσεων (επηρεασμένοι χρήστες, άμεση οικονομική απώλεια, κόστος ανοικοδόμησης, πιθανές απώλειες).

Η δυνατότητα προσβασιμότητας (accessibility) αναφέρεται στην πιθανότητα να εισέλθουν τρομοκράτες στην υποδομή για να προκαλέσουν καταστροφή, πράγμα που αποτελεί κυρίως μια εκτίμηση της ευπάθειας της υποδομής από άποψη φυσικής ασφάλειας. Η δυνατότητα αποκατάστασης (recoverability) καλύπτει μερικώς την ανθεκτικότητα, δεδομένου ότι αναφέρεται στη δυνατότητα της υποδομής να ανακάμπτει μετά από διαταραχή. Η τρωτότητα (vulnerability) καλύπτει μέρος των πιθανών ευπαθειών υποδομής, αυτών που σχετίζονται με τρομοκρατικές επιθέσεις και πιο συγκεκριμένα με εκρήξεις και χημικές/βιολογικές απειλές.

Το κριτήριο συναίσθησης (espyability) αναφέρεται στη λειτουργία μιας υποδομής ως σύμβολο (π.χ. πολιτιστική περιοχή) με έμμεσες επιπτώσεις. Εντούτοις, δεν εξηγείται λεπτομερώς η ποσοτικοποίηση αυτού. Τέλος, η εφεδρικότητα (redundancy) αναφέρεται στις εναλλακτικές λύσεις που υπάρχουν για τον πόρο.

Ιδιαίτερο ενδιαφέρον παρουσιάζει ο τρόπος με τον οποίο εκτιμώνται οι αλληλεξαρτήσεις. Ο χρήστης έχει στη διάθεσή του μια κατηγοριοποίηση τομέων που επηρεάζονται από την απώλεια ενός πόρου. Αυτό που πρέπει να διευκρινιστεί αναλυτικά είναι σε ποιο επίπεδο καθορίζονται οι αλληλεξαρτήσεις. Πιθανότατα, η σχέση μεταξύ διάφορων πόρων σε διαφορετικούς τομείς πρέπει να είναι προκαθορισμένη. Επιπλέον δεν είναι σαφές ποιο είδος αλληλεξάρτησης περιλαμβάνεται στο εργαλείο (εικονική, φυσική, λειτουργική, γεωγραφική).

Το καθορισμένο από το χρήστη σύστημα αξιολόγησης επιτρέπει να συγκριθούν ανομοιογενή αντικείμενα και είναι χαρακτηριστικό ότι παρέχει ένα διατομεακό (cross-sectoral) εναρμονισμένο σύστημα μέτρησης για την εκτίμηση της σπουδαιότητας των διαφορετικών υποδομών. Λείπει ωστόσο μια προσέγγιση υψηλότερου επιπέδου ενώ η ανθεκτικότητα εξετάζεται μόνο μερικώς.

5.14 Μητρώο κινδύνων ασφάλειας QinetiQ

Το μητρώο κινδύνων ασφαλείας QinetiQ (Risk Registry) αναπτύχθηκε στο πλαίσιο ενός προγράμματος εφαρμοσμένης έρευνας για το Υπουργείο Άμυνας του Ηνωμένου Βασιλείου (Hopkinson, 2012). Είναι λύση που βασίζεται σε πιο γενικευμένο μοντέλο εκτίμησης επικινδυνότητας. Το μητρώο κινδύνων αναπτύχθηκε ως βάση δεδομένων Microsoft (MS) Access που υποστηρίζεται από σενάρια και στοιχεία της γλώσσας Perl. Το μητρώο κινδύνων είναι σε μορφή βάσης δεδομένων (π.χ. MS Access) για να

βοηθά το χρήστη να δημιουργήσει, να διαχειρίζεται επερωτήσεις και γενικά να συντηρεί το μητρώο μέσα από μια ποικιλία ηλεκτρονικών υποστηρικτικών εργαλείων.

Το μητρώο κινδύνων βασίζεται στους πόρους κρίσιμων υποδομών, που σημαίνει ότι κάθε κίνδυνος περιγράφεται στα πλαίσια των απειλών που τίθενται προς τους πόρους και τις επιπτώσεις που θα μπορούσε να έχει σε αυτούς. Ένας πόρος είναι ένα αφηρημένο εννοιολογικό αντικείμενο που ορίζεται ως: οτιδήποτε, φυσικό ή λογικό που επηρεάζει τις διαδικασίες στον τομέα ενδιαφέροντος. Ένας πόρος μπορεί επίσης να θεωρηθεί ως και «αντικείμενο» κάτι που έχει αξία (για το χρήστη, τον ιδιοκτήτη, το φορέα εκμετάλλευσης, κ.λπ.). Ένας πόρος μπορεί επίσης να είναι ένα σύνολο αποτελούμενο από τα παραπάνω και ως τέτοιος, ονομάζεται συλλογικός πόρος.

Συχνά, ζεύγη πόρων σχετίζονται, έτσι ώστε αν ένας πόρος πρόκειται να αποτύχει ή να καταστεί μη διαθέσιμος, η λειτουργία του δεύτερου πόρου μπορεί, κατά πάσα πιθανότητα, να είναι αισθητά μειωμένη. Η έννοια των σχέσεων ή των εξαρτήσεων μεταξύ των πόρων στα πλαίσια της ανάλυσης κινδύνων εισάγονται στο μητρώο κινδύνων ως μαθηματικές σχέσεις. Ορισμένες «πρότυπες» σχέσεις, όπως «contains», «depends on», «[in] the proximity of» είναι προκαθορισμένες στο μητρώο κινδύνων, και οι χρήστες μπορούν να ορίσουν πρόσθετες σχέσεις.

Το κύριο πλεονέκτημα του ορισμού της έννοιας των σχέσεων μεταξύ των πόρων μέσω μαθηματικών σχέσεων, είναι ότι καθιστούν δυνατή την υποστήριξη σημαντικών εργαλείων υποστήριξης που θα αναπτυχθούν για το μητρώο κινδύνων. Η δυσλειτουργία περιγράφεται από τη λειτουργική ανεπάρκεια των πόρων μεταξύ των άμεσα απειλούμενων (και επηρεασμένων) πόρων και των δευτερογενώς επηρεασμένων πόρων.

Η μέθοδος που ονομάστηκε «γραμματική περιγραφής των κινδύνων» (risk description grammar) αναπτύχθηκε για το μητρώο των κινδύνων. Είναι ένα απλό πλαίσιο για τον καθορισμό της φύσης ενός κινδύνου και επινοήθηκε με σκοπό να καταστούν οι περιγραφές των κινδύνων πιο αυστηρές και ακριβείς. Η γραμματική είναι μια «δομημένη φυσική γλώσσα» στην οποία οι προτάσεις σχηματίζονται με βάση συγκεκριμένα πρότυπα με (αγγλικές) προτάσεις φυσικής γλώσσας και σημασιολογία που αντιστοιχεί ακριβώς στο μοντέλο του κινδύνου. Το εργαλείο

μητρώου κινδύνων περιλαμβάνει έναν συντακτικό αναλυτή (parser) που ελέγχει τη σύνταξη των προτάσεων και εκτελεί περιορισμένη σημασιολογική ανάλυση.

5.15 Μέθοδος προγράμματος COUNTERACT (ενέργεια & μεταφορές - τρομοκρατία)

Η ομάδα COUNTERACT (Cluster Of User Networks in Transport and Energy Relating to Anti-terrorist ACTivities) στα πλαίσια της Ευρωπαϊκής Ένωσης ανέπτυξε μια γενική μέθοδος ασφάλειας για την αλυσίδα παραγωγής ενέργειας και τον τομέα μεταφορών προκειμένου να καλυφθούν και να ελαχιστοποιηθούν οι τρομοκρατικές απειλές (Kurowski et al., 2012). Επειδή η μέθοδος επικεντρώνεται αποκλειστικά σε τρομοκρατικές απειλές, χρησιμοποιεί ειδικά την ανθρώπινη πρόθεση για να εκτιμήσει κινδύνους, βάσει βλάβης (harm) και διαθεσιμότητας (availability). Παρόλο που η μέθοδος μπορεί να εφαρμοστεί σε διάφορα επίπεδα της ιεραρχίας, δεν παρέχει κανένα μηχανισμό μεταφοράς των αποτελεσμάτων εκτίμησης της επικινδυνότητας σε υψηλότερο (ιεραρχικά) επίπεδο.

Η μέθοδος αποτελείται από εννέα βήματα:

1. Πλήρης στήριξη της ανώτατης διοίκησης για τη διεξαγωγή της μελέτης.
2. Καθορισμός στόχου και ορίων μελέτης - ποιοι πόροι πρέπει να περιληφθούν στην εκτίμηση.
3. Σχεδιασμός του έργου σε σχέση με τη διαθεσιμότητα πόρων, πληροφοριών και χρόνου.
4. Συλλογή δεδομένων και λοιπών πληροφοριών.
5. Χαρακτηρισμός πόρων ως προς:
 - Επιπτώσεις και
 - Διαθεσιμότητα.
6. Δημιουργία πίνακα ελκυστικότητας πόρων (asset attractiveness matrix).
7. Αξιολόγηση και προτάσεις μέτρων για μείωση της ελκυστικότητας πόρων σύμφωνα με το κριτήριο ALARP (As Low As Reasonably Practicable).
8. Αναφορά.
9. Υλοποίηση και παρακολούθηση μέτρων που έχουν καθοριστεί.

Τα πλεονεκτήματα της μεθόδου συνίστανται στο ότι περιορίζει τα στοιχεία που λαμβάνονται υπόψη σε εκείνους τους πόρους που μπορούν να αποτελέσουν στόχο για

τρομοκρατικές ενέργειες όπως και λίστα ελέγχου με τις αναγκαίες πληροφορίες για ολοκλήρωση της μεθόδου και περιγραφή των ειδικών γνώσεων που απαιτούνται για να ληφθούν οι πληροφορίες αυτές.

5.16 Μέθοδος RAM-CAP plus (κρίσιμες υποδομές)

Η μέθοδος RAMCAP (Διαχείριση και ανάλυση επικινδυνότητας για την προστασία των κρίσιμων πόρων) αναπτύχθηκε από την ASME-ITI (American Society of Mechanical Engineers) το Σεπτέμβριο του 2003 (Reddy et al., 2011). Η συγκεκριμένη μέθοδος εκτίμησης επικινδυνότητας στοχεύει στη μείωση των τρομοκρατικών επιθέσεων. Το Φεβρουάριο του 2009, επεκτάθηκε για να συμπεριλάβει το σύνολο των κινδύνων και για αυτό το λόγο ονομάστηκε RAMCAP plus. Το αποτέλεσμα που προέκυψε είναι μια μέθοδος εκτίμησης και διαχείρισης επικινδυνότητας υψηλού επιπέδου που μπορεί να προσαρμοστεί για να χρησιμοποιηθεί σε διαφορετικούς τομείς. Διατίθενται γραπτές οδηγίες που διευκολύνουν την προσαρμογή της μεθόδου στις συγκεκριμένες ανάγκες του κάθε τομέα, για εφτά (7) συγκεκριμένους κρίσιμους τομείς. Για τον τομέα της ενέργειας, οι ακόλουθες εγκαταστάσεις χαρακτηρίζονται ιδιαίτερα κρίσιμες:

- Διυλιστήρια πετρελαίου.
- Σταθμοί υγρού φυσικού αερίου.
- Εργοστάσια πυρηνικής ενέργειας.
- Αποθήκευση και μεταφορά αποβλήτων από πυρηνικά εργοστάσια.
- Φράγματα και δεξαμενές.

Η μέθοδος προορίζεται να χρησιμοποιηθεί ευρέως από όλους τους διαχειριστές ασφάλειας των κρίσιμων υποδομών και στοχεύει να δώσει αποτελέσματα που θα επιτρέπουν τη σύγκριση παραγόντων κινδύνου εντός και μεταξύ διαφορετικών τομέων σε επίπεδο: α) πόρου, β) συστήματος, γ) περιφέρειας, δ) πολιτείας και ε) χώρας. Η μέθοδος περιλαμβάνει επτά διακριτά βήματα:

1. Ανάλυση χαρακτηριστικών πόρου.
2. Χαρακτηρισμός απειλής.
3. Ανάλυση συνεπειών.
4. Ανάλυση ευπάθειας.
5. Εκτίμηση απειλής.

6. Εκτίμηση επικινδυνότητας και ανθεκτικότητας.
7. Διαχείριση επικινδυνότητας και ανθεκτικότητας.

Το RAMCAP plus αντιμετωπίζει τα φυσικά αντικείμενα και το προσωπικό ως πόρους. Οι οργανωτικοί πόροι είναι δυνατόν να περιληφθούν σε ένα από αυτά τα αντικείμενα, κάτι που όμως δεν είναι σαφές. Η μέθοδος εξετάζει όλους τους τύπους απειλών και παρέχοντας αποδεκτά συστήματα μέτρησης πιθανοτήτων, ευπάθειας και επιδράσεων, υποστηρίζει τη σύγκριση των αποτελεσμάτων σε όλους τους τομείς και παρέχει λίστες ελέγχου για απειλές και επιδράσεις. Τα πλεονεκτήματα αυτής της μεθόδου είναι οι στατικές μετρήσεις και το γεγονός ότι δεν απευθύνεται σε συγκεκριμένο τομέα, αλλά υποστηρίζεται από γενικές κατευθύνσεις για κάθε υποδομή.

5.17 Μέθοδος ES-ISAC (τομέας ενέργειας)

Η συγκεκριμένη μέθοδος εκτίμησης της ευπάθειας (vulnerability) αναπτύχθηκε από το Υπουργείο Ενέργειας των ΗΠΑ το 2002 (Voronca, 2012). Μέρος της αποστολής της ήταν η ανάπτυξη και η εφαρμογή προγράμματος εκπαίδευσης και αντίληψης της ευπάθειας στον τομέα της ενέργειας. Το πρόγραμμα έχει σχεδιαστεί με σκοπό να αναπτύξει, να επαληθεύσει και να διαδώσει μεθόδους έρευνας και εκτίμησης επικινδυνότητας με αντίστοιχα εργαλεία που θα βοηθήσουν στην υλοποίηση, θα παράσχουν εκπαίδευση και τεχνική βοήθεια ενώ παράλληλα θα διασφαλίζουν τις ενέργειες για την ελαχιστοποίηση σημαντικών προβλημάτων. Η μέθοδος προορίζεται για ευρεία χρήση εντός του τομέα της ενέργειας στις ΗΠΑ.

Η μέθοδος εκτίμησης κινδύνων ES_ISAC αποτελείται από τρία βασικά στάδια και από ένα σύνολο βημάτων:

- Πριν την εκτίμηση (a-priori)
 - ο Καθορισμός στόχων και πεδίου εφαρμογής της εκτίμησης.
 - ο Καθορισμός διαδικασιών προστασίας πληροφοριών.
 - ο Εύρεση και κατάταξη κρίσιμων πόρων.
- Εκτίμηση
 - ο Ανάλυση αρχιτεκτονικής δικτύου.

- ο Εκτίμηση περιβάλλοντος απειλών.
- ο Διεξαγωγή ελέγχων διείσδυσης.
- ο Εκτίμηση φυσικής ασφάλειας.
- ο Ανάλυση φυσικών πόρων.
- ο Εκτίμηση ασφάλειας λειτουργιών.
- ο Εξέταση πολιτικών και διαδικασιών.
- ο Ανάλυση επιπτώσεων.
- ο Εκτίμηση αλληλεξάρτησης υποδομών.
- ο Εύρεση χαρακτηριστικών γνωρισμάτων κινδύνων.

- Μετά την εκτίμηση (a- posteriori)

- ο Ιεράρχηση οδηγιών αντιμετώπισης.
- ο Ανάπτυξη σχεδίου δράσης.
- ο Εφαρμογή διδαγμάτων και ορθών πρακτικών.
- ο Διεξαγωγή εκπαίδευσης.

Η μέθοδος ES-ISAC απευθύνεται σε φυσικούς πόρους, σε πόρους που σχετίζονται με την οργανωτική δομή και στις τεχνολογίες επικοινωνιών και πληροφορικής. Παρόλο που το προσωπικό αναφέρεται ως πόρος, δεν αντιμετωπίζεται ξεχωριστά. Μόνο οι ανθρωπογενείς απειλές ή τα κλιμακωτά συμβάντα αντιμετωπίζονται με αυτήν τη μέθοδο. Η μέθοδος ESISAC εστιάζει περισσότερο στην αναγνώριση των παραγόντων κινδύνου παρά στην αξιολόγησή τους, πράγμα που δυσχεραίνει τα αποτελέσματα της σύγκρισης. Οι λίστες ελέγχου για τις απειλές, την ευπάθεια και τα αποτελέσματα ενσωματώνονται στη μέθοδο εκτίμησης κινδύνου.

Τα πλεονεκτήματα αυτής της μεθόδου εκτίμησης επικινδυνότητας εντοπίζονται στη λίστα ελέγχου που παρέχεται. Η λίστα αποκαλύπτει ποιες πληροφορίες απαιτούνται για την ολοκλήρωση της μεθόδου εκτίμησης κινδύνων και από πού (από ποιες πηγές) μπορούν να εξαχθούν αυτές. Επιπλέον, περιλαμβάνεται μια λίστα ελέγχου (checklist) για την καταγραφή των πόρων.

6. Η Μέθοδος Magerit και το εργαλείο EAR/PILAR

6.1 Μέθοδος Magerit

Η μέθοδος MAGERIT (Crespo et al., 2006) αναπτύχθηκε το 1997 από το ανώτατο Ισπανικό συμβούλιο για την Ηλεκτρονική διακυβέρνηση (Consejo Superior de Administración Electrónica). Ο σκοπός της μεθόδου σχετίζεται άμεσα με τη γενικευμένη χρήση των ηλεκτρονικών μέσων. Τα μέσα αυτά δημιουργούν οφέλη, αλλά ταυτόχρονα υπόκεινται σε απειλές και κινδύνους που πρέπει να ελαχιστοποιηθούν με αντίμετρα. Με τον τρόπο αυτό, ενισχύεται η εμπιστοσύνη στη χρήση των μέσων. Αυτή τη στιγμή βρίσκεται στην τρίτη έκδοση με έτος θεώρησης το 2012.

Η μέθοδος Magerit αποσκοπεί στα εξής:

- Να αναδείξει την ύπαρξη απειλών, κινδύνων και την ανάγκη έγκαιρης αντιμετώπισής τους.
- Να προσφέρει μια συστηματική μέθοδο ανάλυσης των κινδύνων.
- Να υποβοηθήσει στην περιγραφή και το σχεδιασμό των κατάλληλων μέτρων ελέγχου της επικινδυνότητας.
- Να προετοιμάσει τον οργανισμό για μία διαδικασία αξιολόγησης (valuation), ελέγχου (auditing) και πιστοποίησης (certification).
- Να επιτύχει ομοιομορφία στις αναφορές που εμπειρίζουν τα ευρήματα και τα συμπεράσματα της ανάλυσης, προτείνοντας μια ενιαία δομή.

Το λογισμικό που υποστηρίζει τη μέθοδο Magerit αποτελεί αναπόσπαστο τμήμα της και ονομάζεται EAR/Pilar. Μέσω του εργαλείου αυτού παρακολουθείται η ορθή βήμα-προς-βήμα εφαρμογή της μεθόδου, ενώ αποθηκεύονται και ενημερώνονται όλα τα στοιχεία που συλλέγονται κατά την εφαρμογή της μεθόδου. Το εργαλείο διατέθηκε στην αγορά το 2004 και υποστηρίζεται από τον A.L.H.J.Mañas (Manas, 2009).

6.2 Περιγραφή Magerit

Τα βήματα της μεθόδου περιγράφονται σε 3 βιβλία (*MAGERIT - Methodology for Information Systems Risk Analysis and Management: Book I-The Method, Book II-The Elements, Book III-The Techniques*). Στο πρώτο περιγράφεται αναλυτικά η μέθοδος, στο δεύτερο οι κοινοί τύποι αγαθών, τα κριτήρια αξιολόγησης τους, οι τυπικές απειλές και οι βέλτιστες πρακτικές. Τέλος, στο τρίτο βιβλίο παρέχονται βέλτιστες πρακτικές και συμπληρωματικές πληροφορίες για την ανάλυση και

διαχείριση επικινδυνότητας.

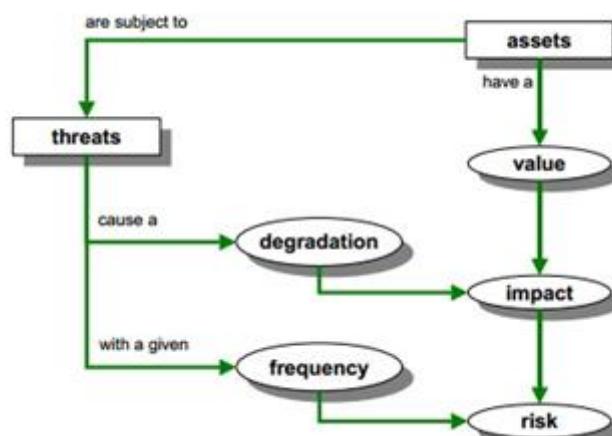
Κατά την έναρξη της μελέτης και κατά την πρώτη σύσκεψη της ομάδας μελέτης με τα καθ' ώλην αρμόδια στελέχη της εταιρίας θα πρέπει:

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

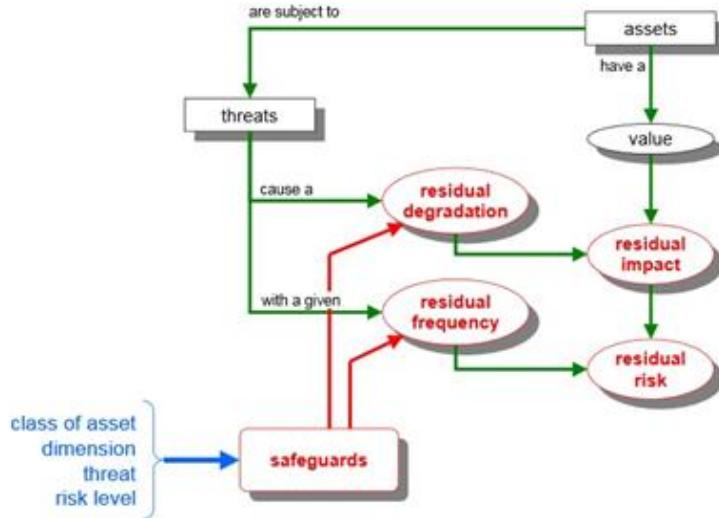
6.3 Βήματα Magerit

Για τον προσδιορισμό του κινδύνου, η μέθοδος ακολουθεί τα εξής βήματα:

- Καθορισμός των σχετικών αγαθών του οργανισμού, των σχέσεων μεταξύ τους και της αξίας τους (π.χ. ποια ζημιά/κόστος θα προκληθεί από την υποβάθμισή τους).
- Καθορισμός των απειλών στις οποίες είναι εκτεθειμένα τα εν λόγω αγαθά.
- Καθορισμός των μέσων προστασίας (safeguards) που υπάρχουν και πόσο αποτελεσματικά είναι έναντι του κινδύνου.
- Εκτίμηση της επίπτωσης (impact), που ορίζεται ως η ζημιά που μπορεί να συμβεί στο αγαθό ως αποτέλεσμα μιας απειλής.
- Εκτίμηση της επικινδυνότητας, που ορίζεται ως η σταθμισμένη επίπτωση στο ποσοστό εμφάνισης (ή την προσδοκία της εμφάνισης) της απειλής.



Εικόνα 4: Βήματα Magerit (χωρίς safeguards)



Εικόνα 5: Βήματα Magerit (με safeguards)

Για την καλύτερη οργάνωση των αποτελεσμάτων, τα βήματα 1, 2, 4 και 5 εκτελούνται πρώτα, παρακάμπτοντας το βήμα 3, έτσι ώστε αν δεν έχουν αναπτυχθεί μέτρα προστασίας οι οποιεσδήποτε τυχόν εκτιμήσεις των επιπτώσεων και των κινδύνων να είναι δυνητικές. Μόλις αναπτυχθεί αυτό το θεωρητικό σενάριο, τα μέτρα ασφάλειας λαμβάνονται υπόψη στο βήμα 3 παρέχοντας έτσι μία ρεαλιστική εκτίμηση της επίπτωσης των απειλών και του κίνδυνου. Στη συνέχεια, υπολογίζονται εκ νέου τα βήματα 4 και 5.

Τα 5 αυτά λειτουργικά βήματα μπορούν να ομαδοποιηθούν σε τρία βασικά στάδια:

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

Κάθε στάδιο εκτελείται σε συγκεκριμένα βήματα. Τα στάδια και τα βήματα αυτά παρουσιάζονται στη συνέχεια.

6.3.1. Στάδιο 1: Προετοιμασία και Προγραμματισμός Έργου

Η Magerit υλοποιεί ένα σύνολο εργασιών κατά την έναρξή της οι οποίες σχετίζονται με τη συλλογή της απαραίτητης πληροφορίας και το σχεδιασμό του έργου.

Βήμα 1: Αρχικά, πραγματοποιείται μελέτη σκοπιμότητας, κατά την οποία διερευνώνται τα προβλήματα που αντιμετωπίζει ο οργανισμός και τα πιθανά οφέλη

που θα προκύψουν από την πραγματοποίηση ενός έργου ανάλυσης και διαχείρισης επικινδυνότητας. Αποτέλεσμα είναι η δημιουργία μιας προκαταρκτικής έκθεσης, η οποία προτείνει τις ενέργειες προετοιμασίας για την διεξαγωγή του έργου. Περιέχει μια λίστα θεμάτων όπως τα βασικά επιχειρήματα, λίστα που αφορά θέματα της ασφάλειας των συστημάτων πληροφοριών (π.χ. στρατηγικό σχέδιο δράσης), μια πρώτη προσέγγιση του πεδίου στο οποίο λειτουργεί ο οργανισμός (π.χ. ανάγκες των μονάδων ή τμημάτων, κατευθύνσεις και τεχνικές διαχείρισης, οργανωτική δομή, τεχνικό περιβάλλον). Η έκθεση αυτή παρουσιάζεται στη διοίκηση του οργανισμού η οποία λαμβάνει την απόφαση έγκρισης του έργου, αλλαγής στόχων ή καθυστέρησής του.

Βήμα 2: Μετά το πέρας της μελέτης σκοπιμότητας ακολουθεί ο καθορισμός του πλαισίου αναφοράς του έργου. Προσδιορίζονται οι βραχυπρόθεσμοι και μακροπρόθεσμοι στόχοι του έργου καθώς και οι διάφοροι περιορισμοί (π.χ. γεωγραφικοί, χρονικοί, λειτουργικοί κ.ά.) και οι δυσκολίες που θα προκύψουν. Επιπλέον γίνεται εκτίμηση των πόρων που απαιτούνται για την υλοποίηση του έργου (ανθρώπινοι, χρονικοί, οικονομικοί).

Βήμα 3: Στη συνέχεια ακολουθεί ο προγραμματισμός του έργου. Σε αυτό το βήμα καθορίζεται το πλάνο των συνεντεύξεων που θα πραγματοποιηθούν για τη συλλογή πληροφοριών σχετικά με τον οργανισμό και τον τρόπο λειτουργίας του. Έπειτα, καθορίζεται ποια άτομα θα συμμετέχουν στη διαχείριση, υλοποίηση και συντήρηση του έργου και προσδιορίζονται τα καθήκοντά τους. Ορίζεται επίσης και η κατηγοριοποίηση της πληροφορίας που θα συλλεχθεί από τις συνεντεύξεις. Τέλος, παράγεται το χρονοδιάγραμμα του έργου.

Βήμα 4: Αφού ολοκληρωθούν οι παραπάνω δραστηριότητες, ακολουθεί η διαδικασία έναρξης του έργου. Σε αυτό το βήμα τροποποιούνται και συντάσσονται τα ερωτηματολόγια για τη συλλογή των απαραίτητων πληροφοριών, δημιουργείται ένας κατάλογος με τα αγαθά που πρέπει να προστατευθούν και προσδιορίζονται τα κριτήρια εκτίμησης των αγαθών και των απειλών. Επιπρόσθετα, γίνεται ανάθεση των πόρων που απαιτούνται για τη διεκπεραίωση του έργου, ενώ παράλληλα γνωστοποιείται ο σκοπός και το πλάνο του έργου στους συμμετέχοντες και στους άμεσα εμπλεκόμενους.

Οι εργασίες που περιγράφονται παραπάνω, ξεκινούν με ένα σύνολο συναντήσεων, συνεχίζουν με συνεντεύξεις και ολοκληρώνονται με τη συμπλήρωση ερωτηματολογίων. Η μέθοδος Magerit με το εργαλείο Pilar, παρέχει υψηλή ευελιξία και ένα ευέλικτο κορμό δημιουργίας ερωτηματολογίων. Η μέθοδος παρέχει οδηγίες για τις συνεντεύξεις και τις διαχωρίζει σε τρεις φάσεις. Η πρώτη φάση χαρακτηρίζεται από χαμηλής προτυποποίησης συνεντεύξεις, ενώ στη δεύτερη φάση και τρίτη φάση, οι συνεντεύξεις και τα ερωτηματολόγια παίρνουν μια πιο δομημένη και αυστηρή μορφή, ώστε να φτάσουμε στα τελικά αποτελέσματα. Το Pilar δίνει τη δυνατότητα ορισμού φάσεων για το έργο. Στο στάδιο της αποτίμησης της επικινδυνότητας, η κατάσταση του έργου αναπαριστάται σε κάθε μία από αυτές παράλληλα.

6.3.2. Στάδιο 2: Ανάλυση Επικινδυνότητας

Το στάδιο αυτό χωρίζεται σε 4 επιμέρους βήματα:

1. Αναγνώριση και Αποτίμηση Αγαθών,
2. Χαρακτηρισμός και Εκτίμηση Απειλών,
3. Χαρακτηρισμός Αντιμέτρων και
4. Εκτίμηση Επικινδυνότητας.

Βήμα 1: Αναγνώριση και Αποτίμηση Αγαθών.

Στο στάδιο αυτό, τα αγαθά αναγνωρίζονται σύμφωνα με τις συνεντεύξεις που προηγήθηκαν. Στη συνέχεια χωρίζονται σε 9 κατηγορίες, οι οποίες παρουσιάζονται στον παρακάτω πίνακα.

Κατηγορίες αγαθών	
Υπηρεσίες (Services)	Φυσικά Μέσα Αποθήκευσης (Media)
Δεδομένα/Πληροφορία (Data/Information)	Βοηθητικός Εξοπλισμός (Auxiliary equipment)
Εφαρμογές (Applications/Software)	Εγκαταστάσεις Εξοπλισμού (Installations)
Εξοπλισμός (Computer Equipment/Hardware)	Προσωπικό (Personel)
Δίκτυα Επικοινωνιών (Communication networks)	

Πίνακας 11: Κατηγοριοποίηση αγαθών στη μέθοδο Magerit

Στη Magerit και στο εργαλείο Pilar δε γίνεται διαχωρισμός υποκατηγοριών όπως γίνεται σε άλλες μεθόδους (όπως για παράδειγμα στην CRAMM), αλλά χρησιμοποιείται διαχωρισμός με στρώματα (layers), όπως τα αποκαλεί. Αυτό βοηθά στην αναγνώριση εξαρτήσεων και συσχετίσεων μεταξύ ομάδων αγαθών και διευκολύνει την πρόβλεψη για μια απειλή που αφορά κάποιο αγαθό χαμηλότερης προτεραιότητας. Πριν γίνει η αποτίμηση της αξίας των αγαθών, κατασκευάζεται ένα μοντέλο για κάθε αγαθό. Στη Magerit αυτό μπορεί να πραγματοποιηθεί και με χρήση XML και ονομάζεται “Μοντέλο Εξάρτησης Αγαθών” (Asset Dependency Model).

Η δημιουργία εξαρτήσεων μεταξύ των αγαθών είναι σημαντική πτυχή της μεθόδου. Πιο συγκεκριμένα, ένα "υψηλότερο αγαθό" λέγεται ότι εξαρτάται από το "χαμηλότερο αγαθό", όταν η εμφάνιση μιας απειλής στο χαμηλότερο αγαθό έχει επίπτωση στο υψηλότερο. Διαισθητικά, θα μπορούσαν να ερμηνευθούν τα χαμηλότερα αγαθά ως οι πυλώνες (pillar) που στηρίζουν την ασφάλεια των υψηλότερων αγαθών. Το χαρακτηριστικό αυτό της μεθόδου οδήγησε στην ονομασία του εργαλείου που υλοποιεί τη μέθοδο: το εργαλείο EAR/PILAR.

Αφού τα αγαθά αναγνωριστούν και κατηγοριοποιηθούν, η Magerit προχωρά στην αποτίμηση αυτών. Στο σημείο αυτό επιλέγεται προσωπικό το οποίο θεωρείται εξειδικευμένο ως προς τον τύπο του αγαθού. Για την αποφυγή μεγάλων αποκλίσεων στις εκτιμήσεις, γίνεται μια προσπάθεια σύγκλισης των διαφορετικών απόψεων μέσω της διαδικασίας Delphi. Η τεχνική Delphi βασίζεται στην έμμεση αλληλεπίδραση και στη δομημένη επικοινωνία μεταξύ εμπειρογνωμόνων. Ονομάζεται επίσης «επαναλαμβανόμενη συνέντευξη» με την έννοια ότι οι ίδιοι εμπειρογνώμονες απαντούν σε τουλάχιστον δύο ενότητες ερωτήσεων, που πρέπει να είναι σταδιακά περισσότερο δομημένες με βάση τα αποτελέσματα του προηγούμενου γύρου συνεντεύξεων. Αποτέλεσμα είναι η δημιουργία μιας αναφοράς, βάσει του κόστους που θα επιφέρει στην εταιρεία η πιθανή καταστροφή κάθε αγαθού. Στη συνέχεια τα σενάρια μεταφράζονται σε βαθμολογία, βάσει ενός συνόλου κανόνων. Κάθε κανόνας ακολουθεί μια κλίμακα, συνήθως από το μηδέν μέχρι το δέκα.

Βήμα 2: Χαρακτηρισμός και Εκτίμηση Απειλών.

Στο βήμα αυτό εντοπίζονται οι απειλές που αφορούν κάθε αγαθό και δημιουργείται ένας κατάλογος απειλών. Επίσης υπολογίζεται η συχνότητα με την οποία κάθε απειλή μπορεί να συμβεί για κάθε αγαθό και εκτιμάται η υποτίμηση/υποβάθμιση

(degradation) της αξίας ενός αγαθού μετά την πραγματοποίηση κάθε απειλής. Η συχνότητα προσθέτει μια επιπλέον διάσταση στην εξέταση της υποτίμησης/υποβάθμισης των αγαθών, καθώς μια απειλή μπορεί να έχει τρομερές συνέπειες, αλλά είναι πολύ απίθανο να συμβεί. Παράλληλα, μια άλλη απειλή μπορεί να έχει πολύ μικρές συνέπειες, αλλά να είναι τόσο συχνές ώστε να συσσωρεύονται σημαντικές ζημίες.

Οι απειλές ομαδοποιούνται σε τέσσερις κατηγορίες, όπως φαίνεται στον παρακάτω πίνακα.

Κατηγορίες αγαθών
Φυσικές καταστροφές
Καταστροφές βιομηχανικής προέλευσης
Λάθη ή Ακούσιες αποτυχίες
Ηθελημένες επιθέσεις

Πίνακας 12: Κατηγοριοποίηση απειλών στη μέθοδο Magerit

Η μέθοδος μπορεί να εκτελεστεί είτε με ποιοτικά είτε με ποσοτικά κριτήρια. Σε κάθε μοντέλο, η επίπτωση υπολογίζεται βάσει της τιμής του αγαθού σε πέντε διαστάσεις ή και λιγότερες, οι οποίες αναφέρονται στη συνέχεια. Στο σημείο αυτό σημαντική βοήθεια παρέχει το εργαλείο Pilar, αφού προσφέρει αυτοματοποιημένο υπολογισμό της πιθανότητας πραγμάτωσης μιας απειλής μέσα από διαφορετικές οπτικές γωνίες (πιθανότητα εμφάνισης, δυνητικότητα, ευκολία, επίπεδο, συχνότητα) και δίνει τη δυνατότητα εμπλουτισμού της υπάρχουσας βάσης του προσθέτοντας γνωστές τρωτότητες με τη μορφή αρχείων XML (CVE's). Οι ευπάθειες αυτές μπορούν να συνδεθούν με τα αντίστοιχα αγαθά που ορίστηκαν στην προηγούμενη φάση. Το Pilar, επίσης, συνυπολογίζει τις συσχετίσεις μεταξύ των αγαθών που αντιμετωπίζουν κοινή απειλή, τη συχνότητα εμφάνισης της απειλής και την υποτίμηση/υποβάθμιση (degradation) που μπορεί να προκύψει στα αγαθά, όπως αυτή ορίζεται από τη Magerit. Η υποτίμηση/υποβάθμιση μετρά τη ζημία που θα προκληθεί αν συμβεί ένα περιστατικό. Η υποτίμηση/υποβάθμιση συχνά περιγράφεται ως μέρος της αξίας του αγαθού και για τη μέτρησή της χρησιμοποιούνται ποιοτικές εκφράσεις. Η τρωτότητα προσδιορίζεται στη κλίμακα “Χαμηλή, “Μεσαία” ή Υψηλή”.

Βήμα 3: Χαρακτηρισμός Αντιμέτρων.

Στο βήμα αυτό πραγματοποιείται εντοπισμός των ήδη υπαρχόντων αντιμέτρων κάθε είδους, τα οποία προκύπτουν καθ' όλη τη διάρκεια της μελέτης ενώ εκτιμάται η αποτελεσματικότητά τους. Για την αξιολόγηση των αντίμετρων, η Magerit ορίζει τη

διεξαγωγή συνεντεύξεων και συναντήσεων με τα κατάλληλα άτομα, όπως ακριβώς ορίστηκαν στο βήμα 1. Τα αντίμετρα αποτιμώνται λαμβάνοντας υπόψη:

1. Την καταλληλότητά τους για το σκοπό που υλοποιήθηκαν.
2. Την ποιότητα της υλοποίησής τους.
3. Την εκπαίδευση των υπεύθυνων για τη διαμόρφωση και τη λειτουργία τους.
4. Την εκπαίδευση των χρηστών, εφόσον αυτοί έχουν κάποιο ενεργό ρόλο.
5. Την ύπαρξη μέτρων ελέγχου για τη μέτρηση της αποτελεσματικότητάς τους.
6. Την ύπαρξη διαδικασιών για τακτικές αναθεωρήσεις των αντιμέτρων αυτών.

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 αποτελεσματικότητά τους.

Βήμα 4: Εκτίμηση Επικινδυνότητας.

Η εκτίμηση αυτή προκύπτει από τον προσδιορισμό της ενδεχόμενης και εναπομένουσας επίπτωσης στην οποία το σύστημα υποβάλλεται. Παράλληλα, ταξινομούνται οι προτεραιότητες που αφορούν τα αγαθά ή τις ομάδες αγαθών, με σειρά επίπτωσης ή επικινδυνότητας. Σκοπός αυτού του βήματος είναι ο υπολογισμός της επίπτωσης της επικινδυνότητας και η ερμηνεία των αποτελεσμάτων. Η μέθοδος Magerit καθώς και το Pilar, υπολογίζει την απομένουσα (residual) συνολική επικινδυνότητα λαμβάνοντας υπόψη τη συσσωρευμένη (accumulated) και την αποκλίνουσα (deflected) επικινδυνότητα. Η επικινδυνότητα που υπολογίζεται για κάθε αγαθό αθροίζεται (aggregated) όταν πληρούνται συγκεκριμένα κριτήρια. Η κλίμακα που χρησιμοποιείται για την αποτίμηση τόσο της επικινδυνότητας όσο και της επίπτωσης παίρνει τιμές από το ένα μέχρι το εννέα. Για τον υπολογισμό της επικινδυνότητας μπορούν να χρησιμοποιηθούν προκαθορισμένοι πίνακες ή αλγορίθμική ανάλυση. Το εργαλείο Pilar που υποστηρίζει τη μέθοδο, είναι ικανό να την υπολογίσει και ποιοτικά και ποσοτικά.

6.3.3. Στάδιο 3: Διαχείριση Επικινδυνότητας

Η διαχείριση επικινδυνότητας μπορεί να χωριστεί σε 3 επιμέρους βήματα:

- Λήψη αποφάσεων,
- Προετοιμασία σχεδίου ασφάλειας και

- Υλοποίηση του σχεδίου ασφάλειας.

Βήμα 1: Λήψη Αποφάσεων.

Στόχος είναι η κατηγοριοποίηση της επικινδυνότητας σε μια κλίμακα (κρίσιμη, σοβαρή, αξιόλογη ή αποδεκτή). Σε αυτό το βήμα προσδιορίζεται η τιμή της επικινδυνότητας και ταξινομούνται οι επιπτώσεις σε μορφή αναφοράς, περιλαμβάνοντας οδηγίες για την αντιμετώπισή τους. Η διαδικασία αυτή είναι απαραίτητη για τη λήψη αποφάσεων που θα πραγματοποιηθεί από τη διοίκηση προκειμένου να αντιμετωπιστούν οι απειλές στις οποίες είναι εκτεθειμένο το σύστημα και να περιοριστούν οι επιπτώσεις τους. Για την κατηγοριοποίηση και αποτίμηση της επικινδυνότητας λαμβάνονται υπόψη διάφοροι παράγοντες από τη διοίκηση του οργανισμού, όπως για παράδειγμα η σοβαρότητα της επίπτωσης, οι νομικές υποχρεώσεις του οργανισμού, η επίπτωση στη δημόσια εικόνα του οργανισμού κ.ά.

Βήμα 2: Προετοιμασία σχεδίου ασφάλειας.

Σκοπός του βήματος αυτού είναι η δημιουργία του πλάνου ασφάλειας του οργανισμού. Για τη κατάρτιση ενός σχεδίου ασφάλειας θα πρέπει να ληφθούν υπόψη τα σενάρια εκείνα στα οποία οι επιπτώσεις και η επικινδυνότητα βρίσκονται σε κρίσιμο ή σοβαρό επίπεδο. Βάσει των σεναρίων αυτών, θα δημιουργηθεί ένα πλήθος προγραμμάτων ασφάλειας (π.χ. εκτίμηση κόστους, πλάνο αποδοχής, πλάνο λειτουργίας, πλάνο συντήρησης, πλάνο εκπαίδευσης, διαδικασίες ελέγχου απόδοσης και αποτελεσματικότητας) που θα παρέχουν τρόπους αντιμετώπισής τους. Ο τελικός στόχος είναι η υλοποίηση ή βελτίωση μιας σειράς αντιμέτρων τα οποία θα μειώσουν την επίπτωση και την επικινδυνότητα σε επίπεδα αποδεκτά από τη διοίκηση του οργανισμού. Αποτέλεσμα της διαδικασίας είναι η δημιουργία ενός τελικού σχεδίου το οποίο θα περιλαμβάνει και θα ενοποιεί όλες τις απαραίτητες ενέργειες, όπως αυτές ορίστηκαν στα επιμέρους σχέδια ασφάλειας που δημιουργήθηκαν.

Βήμα 3: Υλοποίηση του σχεδίου ασφάλειας.

Το βήμα αυτό περιλαμβάνει τις εργασίες που πρέπει να εκτελεστούν για κάθε πρόγραμμα ασφάλειας ξεχωριστά, με σκοπό την υλοποίηση και εφαρμογή του ενιαίου σχεδίου ασφάλειας που έχει καθοριστεί στο προηγούμενο βήμα. Αποτέλεσμα της εφαρμογής του είναι η υλοποίηση των καθορισμένων αντιμέτρων, η δημιουργία KPI'S (key performance indicators) για τη μέτρηση αποτελεσματικότητας, η

νιοθέτηση προτύπων καθώς και η δημιουργία ενημερωμένων μοντέλων επικινδυνότητας για τον οργανισμό.

Στάδιο	Βήματα σταδίου
1. Προετοιμασία και προγραμματισμός έργου (Preparation & Planning of implementation)	<i>Βήμα 1: Μελέτη σκοπιμότητας Βήμα 2: Καθορισμός πλαισίου αναφοράς Βήμα 3: Προγραμματισμός έργου Βήμα 4: Έναρξη έργου</i>
2. Ανάλυση επικινδυνότητας (Risk analysis)	<i>Βήμα 1: Αναγνώριση και Αποτίμηση Αγαθών Βήμα 2: Χαρακτηρισμός και Εκτίμηση Απειλών Βήμα 3: Χαρακτηρισμός Αντιμέτρων Βήμα 4: Εκτίμηση Επικινδυνότητας</i>
3. Διαχείριση επικινδυνότητας (Risk management)	<i>Βήμα 1: Λήψη αποφάσεων Βήμα 2: Προετοιμασία σχεδίου ασφάλειας Βήμα 3: Υλοποίηση σχεδίου ασφάλειας</i>

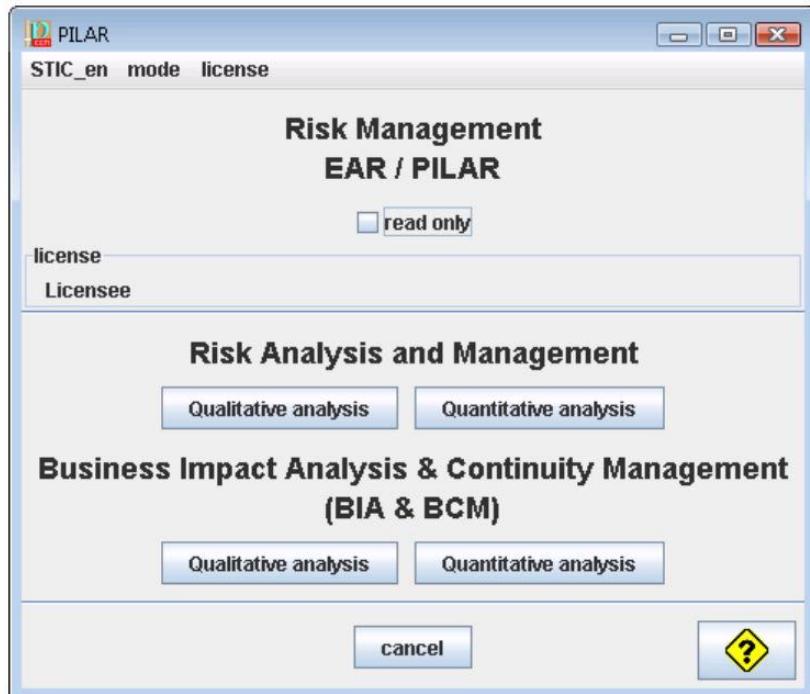
Πίνακας 13: Στάδια και βήματα της EAR/Pilar

6.4. Το Εργαλείο EAR/Pilar

Η μέθοδος Magerit υποστηρίζεται από το εργαλείο EAR/Pilar [EAR/Pilar, 2014]. Έχει σχεδιαστεί για την υποστήριξη της διαδικασίας διαχείρισης επικινδυνότητας σε μακροχρόνιες περιόδους, παρέχοντας αυξητική ανάλυση καθώς τα μέτρα προστασίας βελτιώνονται. Το εργαλείο Pilar έγινε διαθέσιμο το 2004 με την πρώτη επίσημη έκδοση (έκδοση 1.2) ενώ τώρα βρίσκεται στην έκδοση 5.4. Η Magerit και το Pilar καλύπτουν ένα μεγαλύτερο φάσμα προτύπων ISO. Τα πρότυπα αυτά είναι:

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

Κατά την αρχική οθόνη στου εργαλείου (Εικόνα 6) 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.



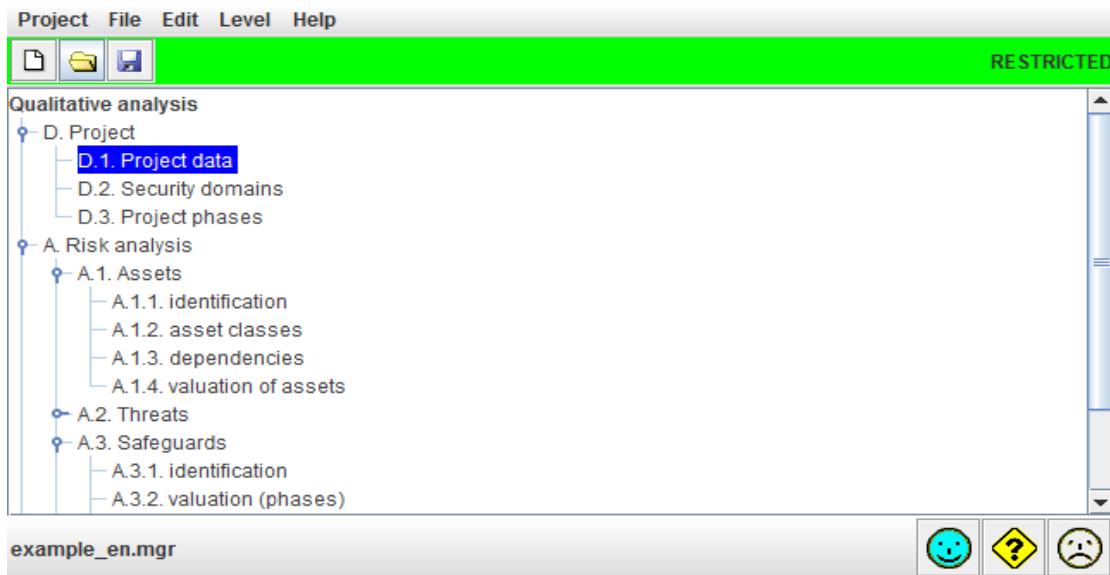
Εικόνα 6: Αρχική οθόνη εργαλείου

Πριν την έναρξη του έργου, στο Pilar ορίζονται διάφορες γενικές πληροφορίες για το έργο, όπως οι τομείς της ασφάλειας (security domains) και οι φάσεις του έργου. Οι τομείς ασφάλειας αποτελούν στην ουσία το πεδίο για το οποίο γίνεται η ανάλυση. Το εργαλείο επίσης παρέχει περισσότερη λεπτομέρεια στο χρήστη ανάλογα με το επίπεδο (level) που έχει επιλεγεί. Για παράδειγμα παρέχεται επιλογή των διαστάσεων ασφάλειας που θα χρησιμοποιηθούν στην αποτίμηση επικινδυνότητας, επιλογή των κλάσεων αγαθών που θα χρησιμοποιηθούν στην αναγνώριση αγαθών και επιλογή των κριτηρίων αποτίμησης των απειλών.

Επίσης παρουσιάζονται οι επιλογές που παρέχει το εργαλείο κατά την ποιοτική μελέτη επικινδυνότητας (Εικόνα 8), με τις επιλογές στο επίπεδο του ειδικού είναι πιο λεπτομερείς (Εικόνα 7). Για παράδειγμα κατά την περιγραφή του έργου παρέχονται 8 επιλογές στο επίπεδο του ειδικού, ενώ παρέχονται 3 επιλογές στο βασικό επίπεδο.



Εικόνα 7: Επιλογές στο επίπεδο του ειδικού



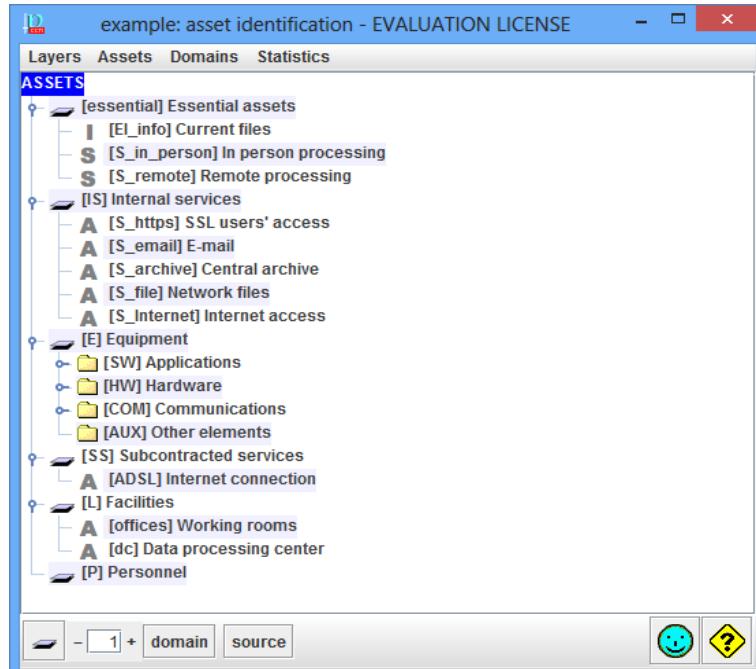
Εικόνα 8: Επιλογές στο βασικό επίπεδο

6.4.1. Λειτουργικά Βήματα: Αναγνώριση αγαθών

6.4.1.1. Κατηγοριοποίηση αγαθών

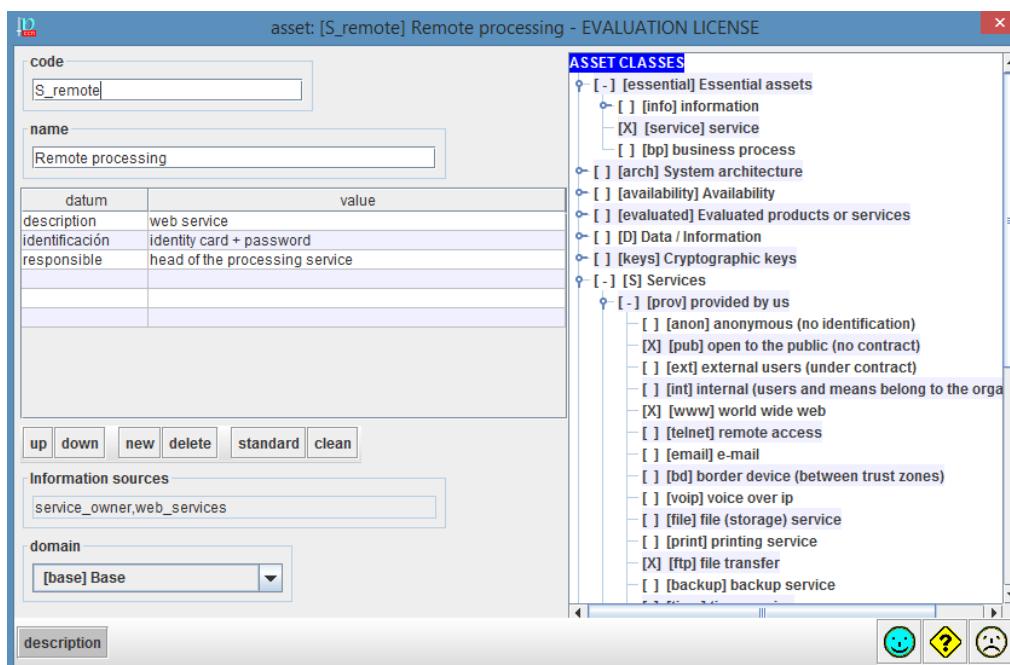
Στο εργαλείο Pilar γίνεται χρήση επιπέδων (layers) για το διαχωρισμό των αγαθών σε κατηγορίες και υποκατηγορίες. Αυτό βοηθάει στην αναγνώριση εξαρτήσεων και συσχετίσεων μεταξύ των διαφορετικών ομάδων αγαθών. Τα επίπεδα συνήθως ταυτίζονται με τις 9 κατηγορίες αγαθών, όπως αυτές ορίζονται από τη μέθοδο Magerit. Επίσης το Pilar δίνει τη δυνατότητα προσθήκης έτοιμων λιστών με τεχνολογικά προϊόντα (hardware και software) (CPE's) και την αντιστοιχία τους με αγαθά. Το εργαλείο παρέχει εύκολη επεξεργασία των επιπέδων, μέσω του μενού

εργασίας. Κάθε αγαθό προστίθεται εύκολα στη λίστα και αντιστοιχίζεται με το επίπεδο και με την κλάση που ανήκει (Εικόνα 9).



Εικόνα 9: Αναγνώριση Αγαθών

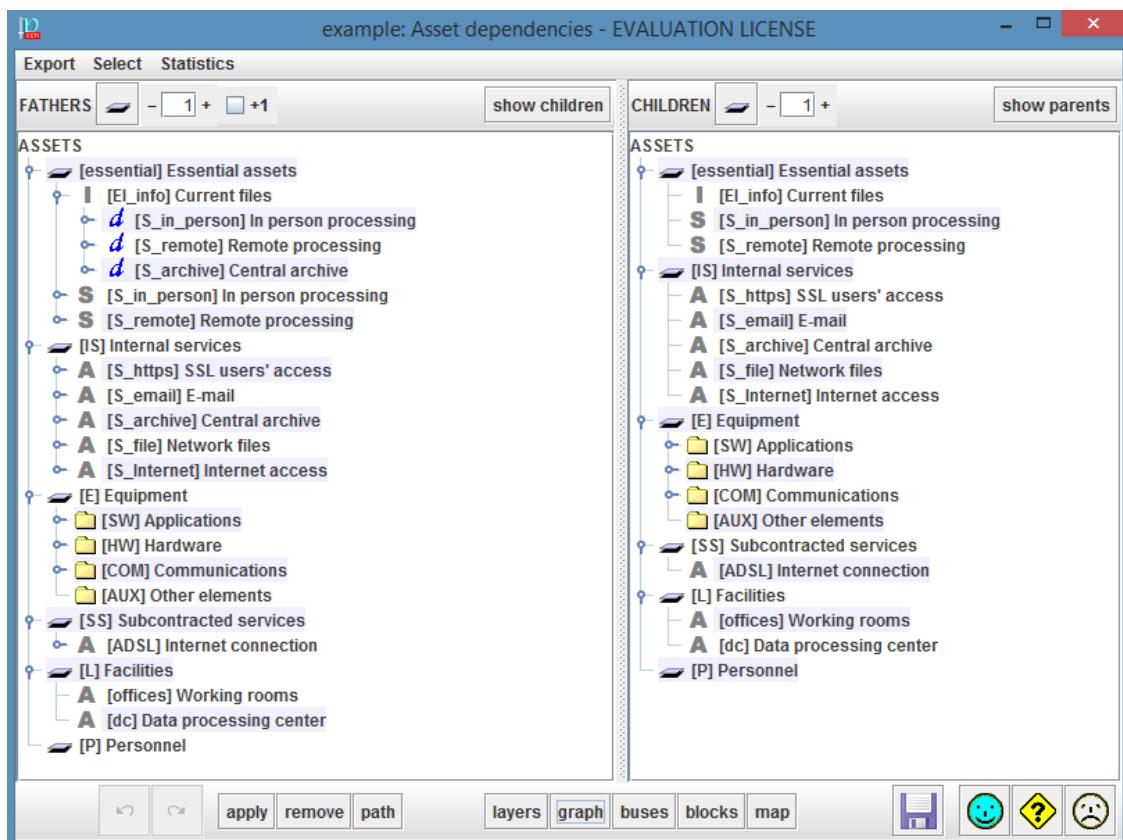
Το εργαλείο επίσης παρέχει τη δυνατότητα αντιστοίχισης ενός αγαθού με τις κατάλληλες κλάσεις στις οποίες ανήκει, σύμφωνα με την ανάλυση των συνεντεύξεων και των ερωτηματολογίων.



Εικόνα 10: Κατηγοριοποίηση αγαθών σε κλάσεις

6.4.1.2. Επεξεργασία Αγαθών

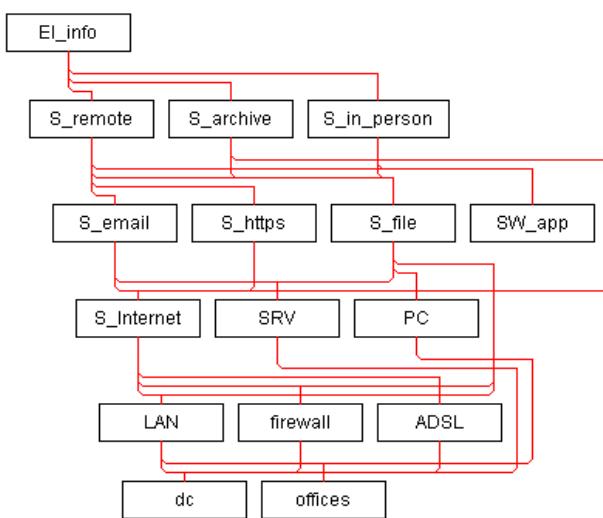
Πριν την αποτίμηση των αγαθών εκτελείται η δημιουργία του μοντέλου εξάρτησης αγαθών, το οποίο μπορεί να γίνει είτε μέσω του εργαλείου είτε μέσω της εισαγωγής ειδικά διαμορφωμένου XML αρχείου. Η αποτίμηση των αγαθών μέσω του εργαλείου μπορεί να γίνει είτε βάση του πεδίου στο οποίο ανήκει κάθε αγαθό (domain valuation) είτε αγαθό προς αγαθό (asset by asset valuation). Στην περίπτωση που επιλεγεί η αποτίμηση με βάση το πεδίο, οι εξαρτήσεις μπορούν να παραλειφθούν και η διαδικασία να συνεχιστεί απευθείας με την αποτίμηση αγαθών. Στην εικόνα 11, εμφανίζονται οι επιλογές για τη δημιουργία εξαρτήσεων μεταξύ των αγαθών.



Εικόνα 11: Αντιστοίχιση αγαθών με άλλα αγαθά για τη δημιουργία εξαρτήσεων

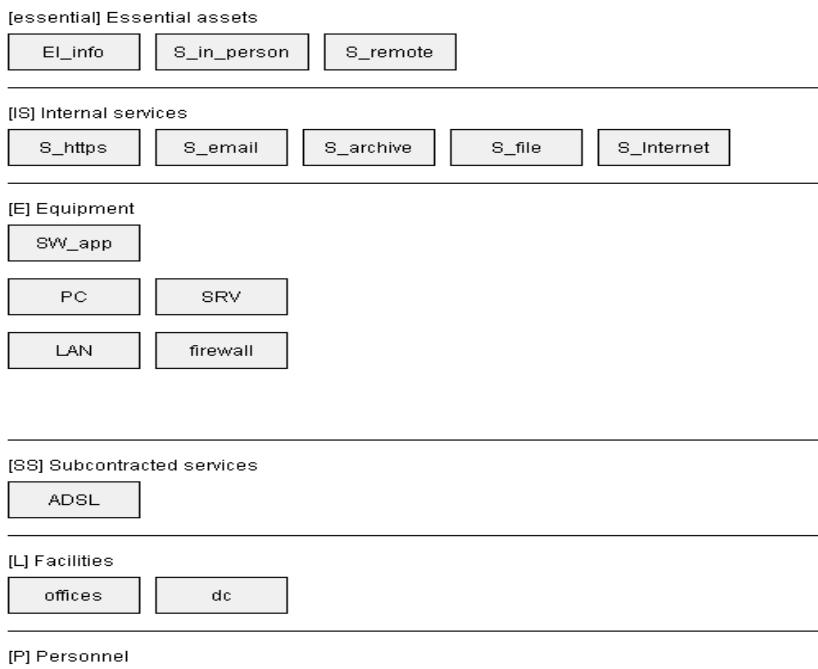
Το εργαλείο δύναται να παράξει αυτόματα διαγράμματα και στατιστικά όσο αφορά την εξάρτηση των αγαθών. Μερικά από τα διαγράμματα αυτά είναι το διάγραμμα συσχετίσεων αγαθών (Εικόνα 12) και ο χάρτης εξαρτήσεων (Εικόνα 13) κ.ά.

100%



Εικόνα 12: Διάγραμμα συσχετίσεων αγαθών

100%



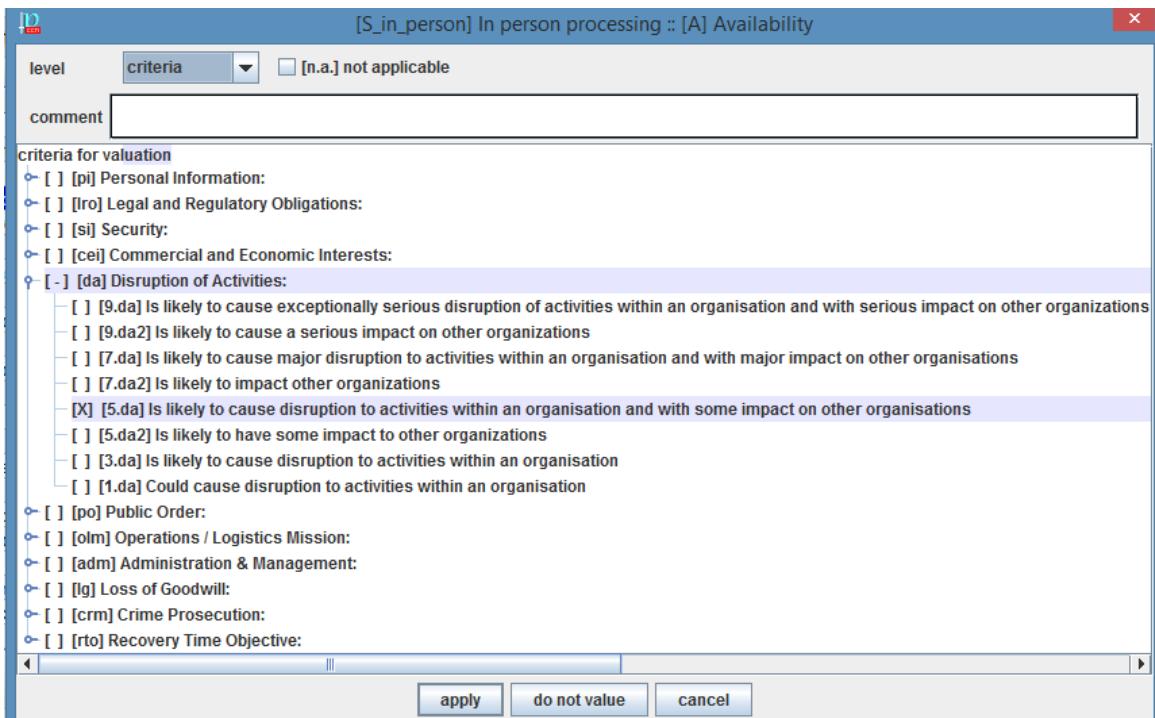
Εικόνα 13: Χάρτης εξαρτήσεων

6.4.2. Λειτουργικά Βήματα: Αποτίμηση αγαθών

Το εργαλείο Pilar αποτιμά κάθε αγαθό υπό το πρίσμα των πέντε διαστάσεων ασφάλειας (Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα, Απονομή Ευθυνών, Αυθεντικοποίηση). Επίσης στο Pilar, στην περίπτωση που δεν πραγματοποιηθεί λεπτομερής ανάλυση επικινδυνότητας, τότε η κλίμακα μπορεί να είναι από το μηδέν μέχρι το πέντε, ενώ η αξία κτίσης ή αντικατάστασης του αγαθού, ορίζεται στην επιλογή ποσοτικής ανάλυσης. Στην περίπτωση της ποιοτικής ανάλυσης, το εργαλείο μπορεί να αποδώσει αυτόματα συσσωρευμένη. Στην περίπτωση της ποσοτικής ανάλυσης δίδεται μια τιμή με βάση το κόστος (Εικόνα 14). Επίσης προσφέρεται η δυνατότητα να ορίσει ο χρήστης βαθμολογία, ή τιμή, μέσω μιας σειράς κριτηρίων (Εικόνα 15), διαφορετικών για κάθε αγαθό.

asset	[A]	[I]	[C]	[Auth]	[Acc]
ASSETS					
↳ [essential] Essential assets					
[EI_info] Current files	[5]	[6]	[5]	[5]	
[S_in_person] In person processing	[5]		[7]	[6]	
[S_remote] Remote processing	[3]		[7]	[6]	
↳ [IS] Internal services					
[S_https] SSL users' access					
[S_email] E-mail					
[S_archive] Central archive					
[S_file] Network files					
[S_Internet] Internet access					
↳ [E] Equipment					
[SW] Applications					
[HW] Hardware					
[COM] Communications					
[AUX] Other elements					
↳ [SS] Subcontracted services					
[ADSL] Internet connection					
↳ [L] Facilities					
[offices] Working rooms					
[dc] Data processing center					
↳ [P] Personnel					
-					

Εικόνα 14: Βαθμολόγηση αξίας αγαθών



Εικόνα 15: Σύνολο κριτηρίων αξιολόγησης αγαθών

6.4.3. Λειτουργικά Βήματα: Εκτίμηση απειλών

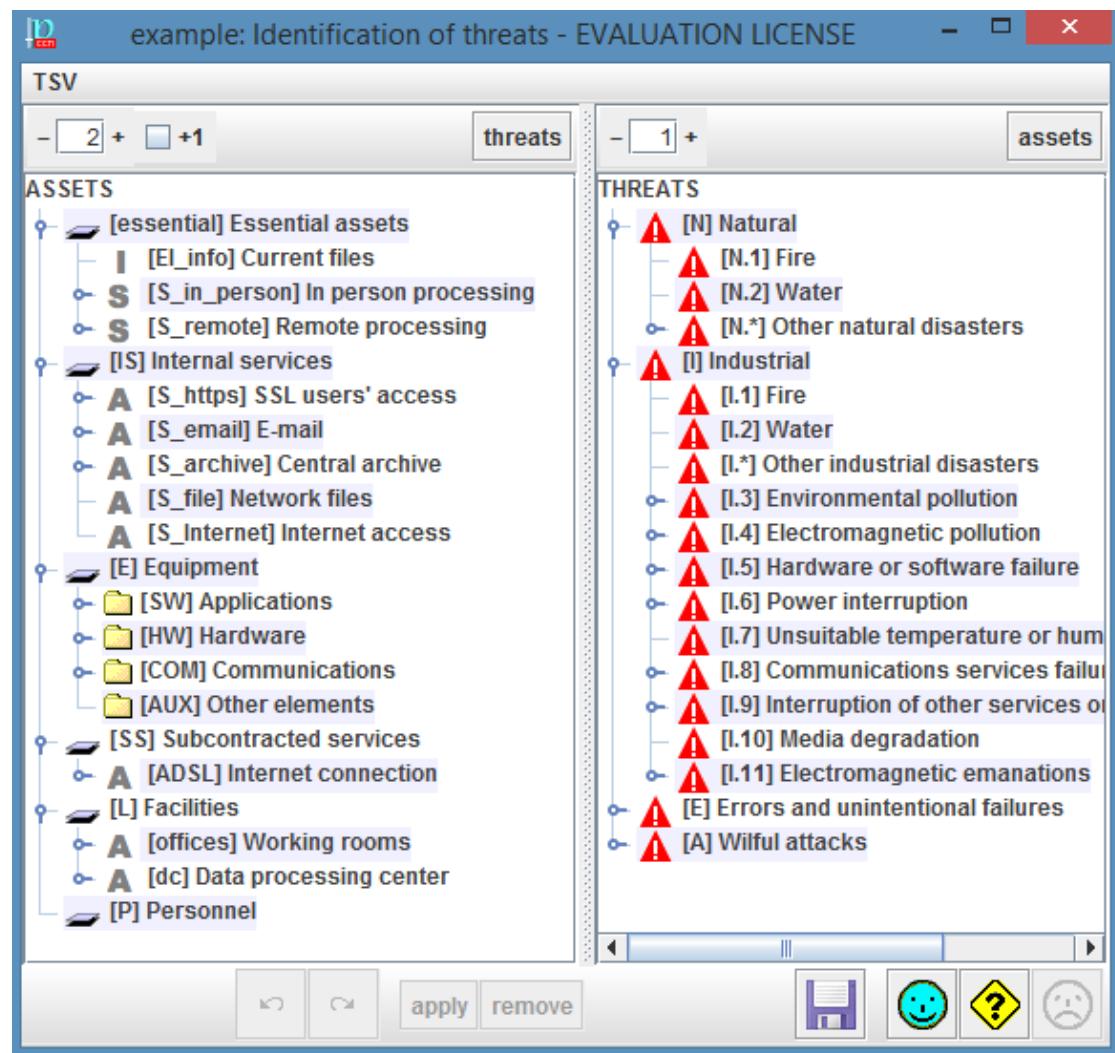
To Pilar δίνει τη δυνατότητα αυτόματης δημιουργίας ομάδων για τα αγαθά, καθώς και τη δυνατότητα τροποποίησης αυτών στη φάση της αναγνώρισης των αγαθών, κάνοντας έτσι πιο εύκολη την εισαγωγή τους. Οι κατηγορίες απειλών που περιέχονται είναι αρκετά ενημερωμένες, καθώς περιέχονται εξειδικευμένα είδη απειλών όπως το malware diffusion αλλά και πιο γενικού περιεχομένου όπως η κοινωνική μηχανική (social engineering). Τα εργαλείο ορίζει μια αρχική τιμή της επίπτωσης κάθε απειλής, την οποία ο χρήστης μπορεί να προσαρμόσει μετέπειτα. Το Pilar, ανάλογα με το είδος της ανάλυσης που έχει επιλεχθεί (ποιοτική ή ποσοτική), χρησιμοποιεί διαφορετικό μοντέλο αποτίμησης της επίπτωσης. Σε κάθε μοντέλο, η επίπτωση υπολογίζεται βάσει της τιμής του αγαθού στις πέντε διαστάσεις που προαναφέρθηκαν.

Επιπροσθέτως, το εργαλείο προσφέρει την εμφάνιση των πιθανοτήτων πραγμάτωσης μιας απειλής μέσα από διαφορετικές οπτικές γωνίες (πιθανότητα εμφάνισης, δυνητικότητα, ευκολία, επίπεδο, συχνότητα) και δίνει τη δυνατότητα εμπλουτισμού της υπάρχουσας βάσης του προσθέτοντάς γνωστές ευπάθειες με τη μορφή αρχείων XML (CVE's). Οι ευπάθειες αυτές μπορούν να συνδεθούν με τα αντίστοιχα αγαθά που ορίστηκαν στην προηγούμενη φάση. Το Pilar επίσης συνυπολογίζει τις συσχετίσεις μεταξύ των αγαθών με μία απειλή, τη συχνότητα εμφάνισης της απειλής

και την υποτίμηση/υποβάθμιση (degradation) που μπορεί να προκύψει στα αγαθά, όπως αυτή ορίζεται από τη Magerit.

6.4.3.1. Αναγνώριση Απειλών

Οι απειλές ταξινομούνται σε 4 κατηγορίες (όπως προαναφέρθηκε). Στην εικόνα 16 εμφανίζονται οι κατηγορίες αυτές και οι υποκατηγορίες τους.



Εικόνα 16: Κατηγοριοποίηση απειλών

6.4.3.2. Αποτίμηση Απειλών

Στο Pilar η τρωτότητα προσδιορίζεται με κλίμακα που περιέχει τους χαρακτηρισμούς “Χαμηλή, “Μεσαία” ή Υψηλή” (Εικόνα 17).

example: Valuation of threats - EVALUATION LICENSE

	asset	level	[A]	[I]	[C]	[Auth]	[Acc]
<input type="checkbox"/> ASSETS							
<input type="checkbox"/> [essential] Essential assets							
<input type="checkbox"/> [EL_info] Current files							
<input type="checkbox"/> S [S_in_person] In person processing			50%	50%	50%	100%	100%
<input type="checkbox"/> [E.1] User errors	M	10%	10%	10%			
<input type="checkbox"/> [E.2] System / Security administrator errors	M	20%	20%	20%			
<input type="checkbox"/> [E.15] Accidental alteration of the information	M		1%				
<input type="checkbox"/> [E.18] Destruction of information	M	10%					
<input type="checkbox"/> [E.19] Information leaks	M			10%			
<input type="checkbox"/> [E.24] System failure due to exhaustion of resources	H	50%					
<input type="checkbox"/> [A.5] Masquerading of identity	M		50%	50%	100%		
<input type="checkbox"/> [A.6] Abuse of access privileges	M	1%	10%	10%	100%		
<input type="checkbox"/> [A.7] Misuse	M	1%	10%	10%			
<input type="checkbox"/> [A.11] Unauthorised access	M		10%	50%	100%		
<input type="checkbox"/> [A.13] Repudiation (denial of actions)	H						100%
<input type="checkbox"/> [A.15] Deliberate alteration of information	H		50%				
<input type="checkbox"/> [A.18] Destruction of information	M	50%					
<input type="checkbox"/> [A.19] Disclosure of information	M			50%			
<input type="checkbox"/> [A.24] Denial of service	H	50%					
<input type="checkbox"/> [S_remote] Remote processing			50%	50%	50%	100%	100%
<input type="checkbox"/> [IS] Internal services							
<input type="checkbox"/> [E] Equipment							
<input type="checkbox"/> [SS] Subcontracted services							
<input type="checkbox"/> [L] Facilities							
<input type="checkbox"/> [P] Personnel							

Εικόνα 17: Αποτίμηση αγαθών

Επίσης, ορίζονται κάποιες προκαθορισμένες τιμές, σε αρχεία TSV (Threat Standard Values). Τα αρχεία αυτά είναι κατάλογοι με τις απειλές και τις τιμές τους για κάθε κατηγορία αγαθού. Η δυνατότητα προσθήκης TSV αρχείου μπορεί να γίνει είτε κατά την έναρξη του έργου είτε κατά τη φάση προσδιορισμού των απειλών. Η αποτίμηση των απειλών μπορεί να γίνει χειροκίνητα ή αυτόματα. Στην περίπτωση που αυτό γίνεται αυτόματα, χρησιμοποιούνται οι τιμές που ορίστηκαν στα αρχεία TSV.

Οι τρωτότητες βασίζονται στην κατανόηση των λειτουργιών και των δυνατοτήτων που είναι διαθέσιμες μέσα από το περιβάλλον του συστήματος. Πιο συγκριμένα, από τη στιγμή που έχει διαπιστωθεί ότι η απειλή μπορεί να βλάψει ένα αγαθό, η τρωτότητα πρέπει να εκτιμηθεί λαμβάνοντας υπόψη δύο πτυχές: την υποτίμηση/υποβάθμιση του αγαθού και τη συχνότητα της απειλής.

6.4.4. Λειτουργικά Βήματα: Εκτίμηση Επικινδυνότητας

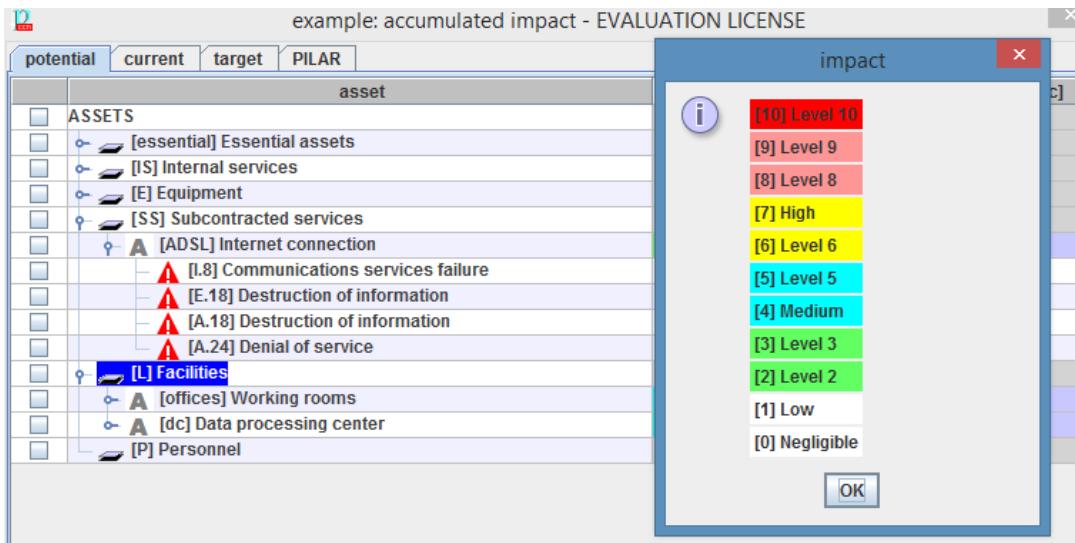
To Pilar υπολογίζει την απομένουσα (residual) συνολική επικινδυνότητα λαμβάνοντας υπόψη τη συσσωρευμένη (accumulated) και την αποκλίνουσα (deflected) επικινδυνότητα. Η επικινδυνότητα που υπολογίζεται για κάθε αγαθό αθροίζεται (aggregated) όταν πληρούνται συγκεκριμένα κριτήρια. Επίσης υπάρχει ξεχωριστή ενότητα για τις επιπτώσεις (Εικόνα 18) και την επικινδυνότητα (Εικόνα 19), στην οποία διαχωρίζονται οι συσσωρευμένες και οι αποκλίνουσες τιμές. Η κλίμακα που χρησιμοποιείται για την αποτίμηση τόσο της επικινδυνότητας όσο και της επίπτωσης παίρνει τιμές από το ένα μέχρι το εννέα και υπάρχει ο αντίστοιχος χρωματισμός (Εικόνα 20). Το εργαλείο είναι ικανό να υπολογίσει την επικινδυνότητα είτε με προκαθορισμένους πίνακες είτε με αλγορίθμική ανάλυση (ποιοτική και ποσοτική) που βασίζεται σε μαθηματικά μοντέλα. Είναι σημαντικό να τονιστεί πως το εργαλείο παρέχει εκτιμήσεις για την πιθανή και τρέχουσα επικινδυνότητα άλλα και τον επιθυμητό στόχο. Επίσης, δίνεται εκτίμηση του επιπέδου επικινδυνότητας μετά την εφαρμογή αντιμέτρων. Επιπλέον, παρέχει τη δυνατότητα ορισμού φάσεων, που βοηθούν στην παρακολούθηση της κατάστασης του έργου.

example: accumulated impact - EVALUATION LICENSE						
	asset	[A]	[I]	[C]	[Auth]	[Acc]
ASSETS		[5]	[7]	[6]	[7]	[6]
[essential] Essential assets		[4]	[4]	[5]	[7]	[6]
[IS] Internal services		[3]	[5]	[6]	[7]	
[E] Equipment		[5]	[7]	[6]	[7]	[6]
[SS] Subcontracted services		[3]				
[A] [ADSL] Internet connection		[3]				
[I.8] Communications services failure		[3]				
[E.18] Destruction of information		[0]				
[A.18] Destruction of information		[2]				
[A.24] Denial of service		[2]				
[L] Facilities		[5]	[4]	[5]		
[A] [offices] Working rooms		[5]	[2]	[5]		
[A] [dc] Data processing center		[5]	[4]	[5]		
[P] Personnel						

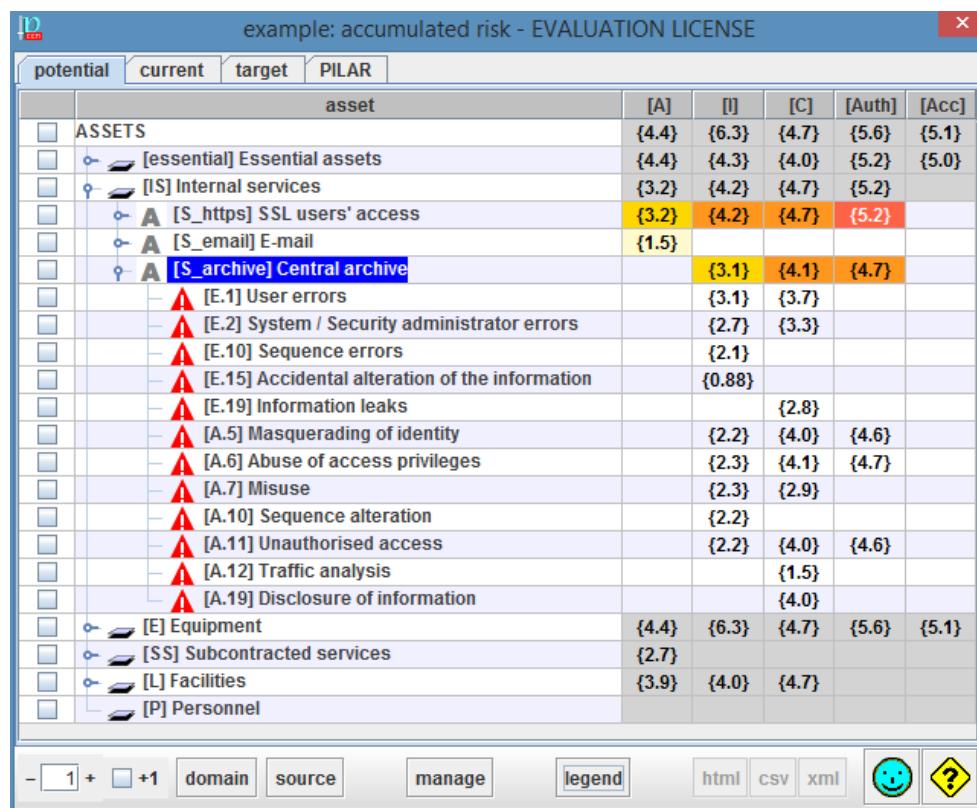
Buttons at the bottom:

- 1 + 1
- domain source
- manage
- legend
- html csv xml
- Smiley icon
- Help icon

Εικόνα 18: Παράδειγμα συσσωρευμένης επίπτωσης



Εικόνα 19: Επεξήγηση χρωμάτων αποτελεσμάτων στους πίνακες αποτίμησης επιπτώσεων



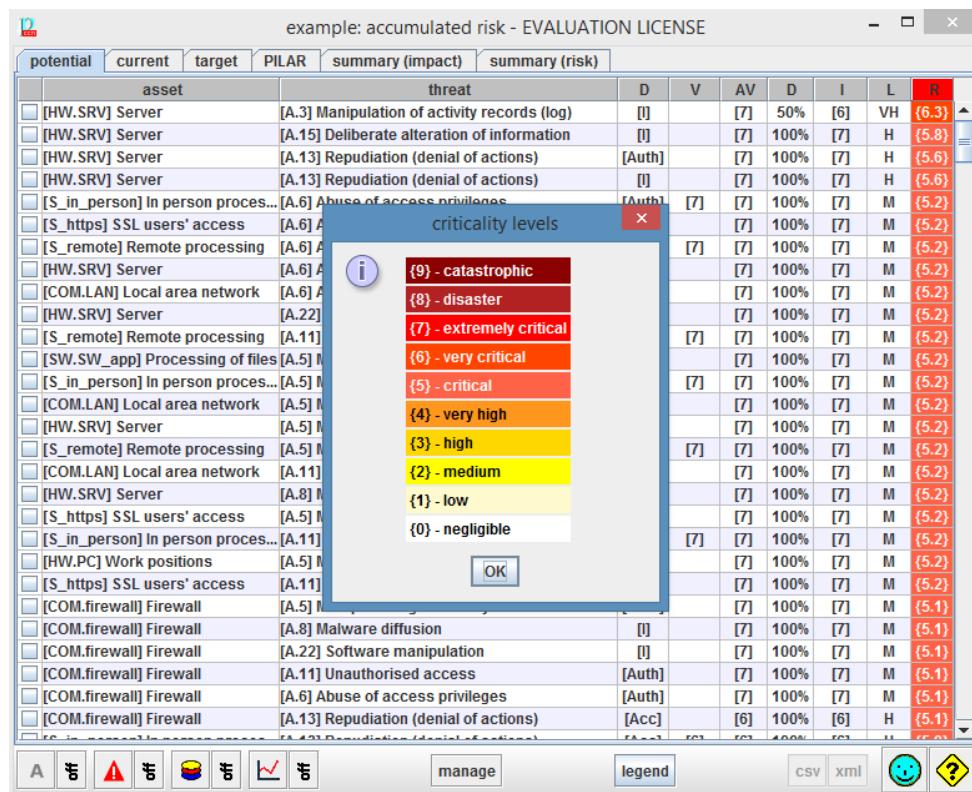
Εικόνα 20: Παράδειγμα συσσωρευμένης επικινδυνότητας

Στην εικόνα 21 παρουσιάζεται ένα παράδειγμα του πίνακα επικινδυνότητας που εξάγεται από τη μελέτη και επεξήγηση των χρωματισμών ανάλογα με την κρισιμότητα (Εικόνα 22).

example: accumulated risk - EVALUATION LICENSE

potential	current	target	PILAR	summary (impact)	summary (risk)	D	V	AV	D	I	L	R
asset	threat											
[HW.SRV] Server	[A.3] Manipulation of activity records (log)	[I]		[7]	50%	[6]	VH	(6.3)				
[HW.SRV] Server	[A.15] Deliberate alteration of information	[I]		[7]	100%	[7]	H	(5.8)				
[HW.SRV] Server	[A.13] Repudiation (denial of actions)	[Auth]		[7]	100%	[7]	H	(5.6)				
[HW.SRV] Server	[A.13] Repudiation (denial of actions)	[I]		[7]	100%	[7]	H	(5.6)				
[S_in_person] In person proces...	[A.6] Abuse of access privileges	[Auth]	[7]	[7]	100%	[7]	M	(5.2)				
[S_https] SSL users' access	[A.6] Abuse of access privileges	[Auth]	[7]	[7]	100%	[7]	M	(5.2)				
[S_remote] Remote processing	[A.6] Abuse of access privileges	[Auth]	[7]	[7]	100%	[7]	M	(5.2)				
[HW.SRV] Server	[A.6] Abuse of access privileges	[I]		[7]	100%	[7]	M	(5.2)				
[COM.LAN] Local area network	[A.6] Abuse of access privileges	[Auth]	[7]	100%	[7]	M	(5.2)					
[HW.SRV] Server	[A.22] Software manipulation	[I]		[7]	100%	[7]	M	(5.2)				
[S_remote] Remote processing	[A.11] Unauthorised access	[Auth]	[7]	[7]	100%	[7]	M	(5.2)				
[SW.SW_app] Processing of files	[A.5] Masquerading of identity	[Auth]	[7]	100%	[7]	M	(5.2)					
[S_in_person] In person proces...	[A.5] Masquerading of identity	[Auth]	[7]	[7]	100%	[7]	M	(5.2)				
[COM.LAN] Local area network	[A.5] Masquerading of identity	[Auth]	[7]	100%	[7]	M	(5.2)					
[HW.SRV] Server	[A.5] Masquerading of identity	[Auth]	[7]	100%	[7]	M	(5.2)					
[S_remote] Remote processing	[A.5] Masquerading of identity	[Auth]	[7]	[7]	100%	[7]	M	(5.2)				
[COM.LAN] Local area network	[A.11] Unauthorised access	[Auth]	[7]	100%	[7]	M	(5.2)					
[HW.SRV] Server	[A.8] Malware diffusion	[I]		[7]	100%	[7]	M	(5.2)				
[S_https] SSL users' access	[A.5] Masquerading of identity	[Auth]	[7]	100%	[7]	M	(5.2)					
[S_in_person] In person proces...	[A.11] Unauthorised access	[Auth]	[7]	[7]	100%	[7]	M	(5.2)				
[HW.PC] Work positions	[A.5] Masquerading of identity	[Auth]	[7]	100%	[7]	M	(5.2)					
[S_https] SSL users' access	[A.11] Unauthorised access	[Auth]	[7]	100%	[7]	M	(5.2)					
[COM.firewall] Firewall	[A.5] Masquerading of identity	[Auth]	[7]	100%	[7]	M	(5.1)					
[COM.firewall] Firewall	[A.8] Malware diffusion	[I]		[7]	100%	[7]	M	(5.1)				
[COM.firewall] Firewall	[A.22] Software manipulation	[I]		[7]	100%	[7]	M	(5.1)				
[COM.firewall] Firewall	[A.11] Unauthorised access	[Auth]	[7]	100%	[7]	M	(5.1)					
[COM.firewall] Firewall	[A.6] Abuse of access privileges	[Auth]	[7]	100%	[7]	M	(5.1)					
[COM.firewall] Firewall	[A.13] Repudiation (denial of actions)	[Acc]	[6]	100%	[6]	H	(5.1)					

Εικόνα 21: Παράδειγμα πίνακα επικινδυνότητας



Εικόνα 22: Επεξήγηση χρωματισμού ανάλογα με επίπεδο επικινδυνότητας

6.4.5. Λειτουργικά Βήματα: Προσδιορισμός προτεινόμενων αντιμέτρων

Το εργαλείο PILAR παρέχει λειτουργικές και όχι τεχνικές προδιαγραφές. Σε περίπτωση αντικρουόμενων αντιμέτρων (δηλαδή αντιμέτρων που εξυπηρετούν διαφορετικές ανάγκες) δεν προβλέπεται εσωτερικός μηχανισμός που να τα αποκλείει. Είναι ευθύνη του αναλυτή να επιλέξει ποιο θα προταθεί τελικά, λαμβάνοντας υπόψη τις εξαρτήσεις των αγαθών.

Τα αντίμετρα κατηγοριοποιούνται επίσης βάσει της αποτελεσματικότητάς τους. Για την αξιολόγηση κάθε αντίμετρου, το Pilar χρησιμοποιεί επίπεδα ωριμότητας (maturity levels), όπως ορίζονται από το Capability Maturity Model (CMM). Με τον όρο “επίπεδο ωριμότητας” ορίζεται η κατάσταση εφαρμογής των υπαρχόντων αντιμέτρων στις διάφορες φάσεις του έργου. Η κλίμακα αξιολόγησης που χρησιμοποιείται είναι από 0% (L0) μέχρι 100% (L5) (Εικόνα 23).

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 23: Κλίμακα αξιολόγησης αντιμέτρων

Επίσης στο Pilar χρησιμοποιείται διαχωρισμός των αντιμέτρων βάσει 4 πτυχών:

Κατηγορίες αντιμέτρων

M = Διοίκηση - Διαχείριση (Management)

Per = Πολιτικές προσωπικού (Personnel policies)

T = Τεχνικές Λύσεις (Technical Solutions)

Phy = Φυσική Ασφάλεια (Physical Security)

Πίνακας 14: Κριτήρια διαχωρισμού αντιμέτρων

Ακόμα, ορίζεται και ο τύπος προστασίας στον οποίο αναφέρεται κάθε αντίμετρο. Οι τύποι προστασίας διαχωρίζονται σε 10.

Tύποι αντιμέτρων

PR: prevention

DR: deterrence

EL: elimination

IM: impact minimization

CR: correction

RC: recovery

AD: administrative

AW: awareness

DC: detection

MN: monitoring

Πίνακας 15: Κριτήρια διαχωρισμού αντιμέτρων

Το εργαλείο κάνει χρήση μιας κλίμακας βαρύτητας από το μηδέν μέχρι το τρία, βάσει της οποίας εκτιμά τη σημαντικότητα ενός μέτρου. Για κάθε αντίμετρο, το Pilar εφαρμόζει και μία κλίμακα από το μηδέν μέχρι το δέκα, την οποία ονομάζει “Σύσταση” (Recommendation). Το “μηδέν” σημαίνει πως το αντίμετρο έχει σχετικά μικρή σημασία ενώ το “δέκα” πως συνιστάται η άμεση υλοποίησή του. Η κλίμακα αυτή χρησιμοποιείται σε συνδυασμό με τη βαρύτητα σημαντικότητας (Εικόνα 24) ώστε το εργαλείο να υποδείξει την προτεραιότητα υλοποίησης των μέτρων. Επίσης, διαθέτει επιλογή αυτόματης υπόδειξης των αντιμέτρων που θεωρούνται τα πιο κατάλληλα. Το βάρος σημαντικότητας κάθε κριτηρίου προτεραιότητας για τα αντίμετρα ορίζεται από το προφίλ ασφάλειας που έχει επιλεγεί.

	highest weight	Critical.
	high weight	Very important.
	normal weight	Important.
	low weight	Interesting.
	assurance: certified components	

Εικόνα 24: Σχετικό βάρος σημαντικότητας

Στην αναγνώριση των υπαρχόντων αντίμετρων, το εργαλείο προτείνει αυτόματα μια λίστα με αντίμετρα, τα οποία ο αναλυτής καλείται να επιλέξει εάν ισχύουν ή όχι (applicable, not applicable), ενώ παρέχεται και η δυνατότητα το ίδιο το εργαλείο να το προτείνει το ίδιο, δίνοντας παράλληλα και τιμές προτεραιότητας από Null έως 10 (Εικόνα 25). Αν το Pilar σημειώσει με γκρι χρώμα ένα αντίμετρο στη στήλη “recommended”, τότε αυτό θεωρείται ως μη αναγκαίο.

The screenshot shows a software application window titled "example: safeguards - EVALUATION LICENSE". The menu bar includes "Edit", "Expand", "Export", "View", and "Statistics". A toolbar at the top has icons for "Edit", "Expand", "Export", "View", and "Statistics". Below the menu is a table with the following columns: asp..., top, safeguard, doubts, source, comment, recommendation, on / off, and applies. The table lists various safeguards categorized under "SAFEGUARDS" and other sections like "PHYSICAL", "PERSONNEL", "CONTINUITY", "ORGANISATION", and "EXTERNAL RELATIONS". Each row contains a small icon representing the safeguard type (e.g., red umbrella for highest weight, green checkmark for recommended). The "recommendation" column shows numerical values ranging from 4 to 7. At the bottom of the table are buttons for "sources", "clear", "recommendation", and "only if ...". To the right of the table are several icons: a floppy disk, a smiley face, a question mark, and a sad face.

Εικόνα 25: Πρόταση αντιμέτρων

Τα αντίμετρα μεταφορτώνονται αυτόματα από τα προφίλ ασφάλειας που έχουν επιλεχθεί (Εικόνα 26).



Εικόνα 26: Προφίλ ασφάλειας

Το εργαλείο μπορεί να προσφέρει επιπλέον μέτρα προστασίας στη διοίκηση του οργανισμού (Εικόνα 27), τα οποία όμως δεν λαμβάνονται υπόψη στην αποτίμηση της επικινδυνότητας.

Edit Export Import		Information sources							
[base] Base		safeguard							
as...	top		do...	so...	co...	rec...	cur...	tar...	PIL...
		ADDITIONAL PROTECTION							
		⌚ [COM] Communication networks							
		⌚ [COM.wifi] WiFi							
		⌚ [es.cni.ccn.stic.406] STIC 406 - Wireless security (802.11)							
M		⌚ [G] Management recommendations					7	L0... L1 L3 L3...	
M		⌚ [1] evaluation mode					6	L1 L3 L4	
M		⌚ [2] evaluation mode					6	L1 L3 L4	
PER		⌚ [3] evaluation mode					6	L1 L3 L4	
M		⌚ [4] evaluation mode					7	L1 L3 L3...	
M		⌚ [5] evaluation mode					6	L1 L3 L4	
PHY		⌚ [6] evaluation mode					6	L1 L3 L4	
T		⌚ [7] evaluation mode					7	L1 L3 L4	
PHY		⌚ [7b] evaluation mode					7	L0 L3 L4	
T		⌚ [8] evaluation mode					6	L1 L3 L4	
M		⌚ [8b] evaluation mode					6	L1 L3 L4	
T		⌚ [T] Technical recommendations					7	-L2 -L3 L3...	

Below the table are buttons for 'sources', navigation arrows, a search bar ('operation'), and various icons for file operations and help.

Εικόνα 27: Πρόσθετα μέτρα στη διοίκηση του οργανισμού

Το εργαλείο παράγει εκτενείς αναφορές και προσφέρει τη δυνατότητα εποπτικής παρουσίασης με χρήση πινάκων (Εικόνα 28) και γραφημάτων.

example: Safeguard effectiveness - EVALUATION LICENSE

Information sources										
[base] Base		safeguard	doubts	source	commen...	recom...	current	target	PILAR	
asp...	top	SAFEGUARDS								
M	PR	o [H] General Protections				7		L0-L5	L3-L5	L2-L4
M	PR	o [D] Protection of Data / Information				7		L0-L5	L2-L5	L2-L4
M	EL	o [K] Cryptographic keys management				8		L1-L3	L2-L5	L2-L5
M	PR	o [S] Protection of Services				6		L0-L5	L3-L5	L2-L4
M	PR	o [SW] Protection of Software				7		L0-L5	L3-L5	L2-L4
M	PR	o [HW] Protection of Hardware				7		L0-L5	L0-L5	L2-L4
M	PR	o [COM] Protection of Communications				8		L0-L5	L2-L5	L2-L5
M	PR	o [IP] Interconnection points: connecting to other trust zones				5		L0-L2	L2-L5	L2-L3
M	PR	o [MP] Protection of Media				7		L2-L3	L3-L5	L2-L4
M	PR	o [AUX] Auxiliary Means				6		L0-L5	L1-L5	L2-L4
PHY	PR	o [L] Protection of the installations				7		L0-L5	L1-L5	L2-L4
PER	PR	o [PS] Personnel						L1	L5	n.a.
M	CR	o [H.IR] Incident management (ICT)				5		L0-L5	L2-L5	L2-L3
M	RC	o [BC] Business continuity (contingency)				5		L0-L3	L4-L5	L2-L3
M	AD	o [G] Organisation				6		L0-L5	L2-L5	L2-L4
M	AD	o [E] External Relations				5		L1-L5	L4-L5	L2-L3
M	AD	o [NEW] Acquisition / development				4		L0-L2	L5	L2-L3

Εικόνα 28: Παράδειγμα αποτίμησης αντιμέτρων ασφαλείας

Το εργαλείο μπορεί να κάνει εξαγωγή των αποτελεσμάτων της έκθεσης επικινδυνότητας σε αρχείο τύπου XML, RTF, HTML και CSV. Ειδικότερα, η παρουσίαση σε XML είναι πολύ σημαντική καθώς διευκολύνει την αναζήτηση των στοιχείων, όχι μόνο μέσω του διαδικτύου, αλλά και του σημασιολογικού ιστού. Τέλος, βοηθά στη διασύνδεση με άλλα εργαλεία που υποστηρίζουν την XML.

6.4.6. Το Εργαλείο EAR/Pilar και η Διαδικασία Συνέχισης Λειτουργίας

Το εργαλείο Pilar δύναται να υποστηρίξει και διαδικασίες για “συνέχιση της λειτουργίας” (business continuity) του οργανισμού. Η λειτουργία αυτή είναι ιδιαίτερα χρήσιμη όταν ο οργανισμός θέλει να ελέγξει την κατάστασή του, ώστε να διασφαλιστεί η συνεχής λειτουργία των υπηρεσιών του σε περίπτωση πραγμάτωσης μιας απειλής. Η ανάλυση των επιπτώσεων στην επιχειρηματική λειτουργία (*Business Impact Analysis - BIA*) προβλέπει τις συνέπειες της διακοπής της λειτουργίας των επιχειρήσεων και συγκεντρώνει τις πληροφορίες που απαιτούνται για την ανάπτυξη στρατηγικών ανάκαμψης.

Ο εντοπισμός και η αξιολόγηση των επιπτώσεων των καταστροφών στην επιχείρηση παρέχει τη βάση για επενδύσεις σε στρατηγικές ανάκαμψης, καθώς και τις επενδύσεις

σε στρατηγικές πρόληψης και μετριασμού ενδεχόμενων απωλειών από την πραγμάτωση απειλών.

Η διαδικασία μοιάζει με αυτήν που ακολουθείται σε ένα έργο ανάλυσης και αποτίμησης επικινδυνότητας, με τη διαφορά πως προστίθενται επιπλέον επιλογές στο εργαλείο.

Στο εγχειρίδιο του εργαλείου τονίζεται η σημασία των παραμέτρων “Χρόνος Ανάκαμψης Υπηρεσίας” (RTO – Recovery Time Objective) και “Σημείο ανάκαμψης” (RPO – Recovery Point Objective).

Στο RTO ορίζεται το άνω χρονικό όριο ανάκαμψης και στο RPO η αποδεκτή ποσότητα απώλειας πληροφορίας μετά από ένα περιστατικό. Το RTO είναι δύσκολο να οριστεί επακριβώς, και διακρίνεται σε 3 φάσεις:

- T1 = Το χρονικό διάστημα από την στιγμή που παύει η λειτουργία μιας υπηρεσίας μέχρι την στιγμή της ανίχνευσης του προβλήματος. Ο καθορισμός αυτής της χρονικής περιόδου είναι ο πιο δύσκολος, καθώς μια υπηρεσία ενδέχεται να παύσει την λειτουργία της σε χρονική στιγμή που δεν είναι άμεση η ανίχνευση του προβλήματος (π.χ. βραδινές ώρες).
- T2 = Το χρονικό διάστημα από τη στιγμή ανίχνευσης του προβλήματος μέχρι τη λήψη απόφασης για την εκκίνηση του σχεδίου ανάκαμψης.
- T3 = Το χρονικό διάστημα από τη λήψη της απόφασης μέχρι την πλήρη επαναφορά της υπηρεσίας. Η φάση αυτή σχετίζεται άμεσα με τις αποφάσεις διακυβέρνησης του οργανισμού. Ένα σύντομο χρονικό διάστημα για την άμεση επαναφορά της υπηρεσίας μπορεί να έχει υψηλό κόστος και συχνά απαιτείται η εύρεση του σημείου ισορροπίας μεταξύ κόστους και RTO.

Το RPO αποτελεί απόφαση που σχετίζεται με τη διοίκηση του οργανισμού. Οι εμπλεκόμενη με αυτό μηχανισμοί απαιτούν τη δημιουργία αυτοματοποιημένων αντιγράφων της υπηρεσίας, χωρίς την διακοπή της λειτουργίας της κύριας υπηρεσίας.

Το Pilar δεν παρέχει λειτουργικότητα σχετικά με το RPO. Διαχειρίζεται μόνο το χρόνο που απαιτείται για την ανάκαμψη από ένα αντίγραφο ασφάλειας (backup). Η συχνότητα δημιουργίας και η διαχείριση του αντιγράφου ασφάλειας είναι ζήτημα που αφορά τις πολιτικές κάθε οργανισμού. Αντίθετα με το RPO, το Pilar είναι αρκετά ευέλικτο όσο αφορά το RTO και βοηθά στον καθορισμό της τιμής του και στην ανάλυση του κατά πόσο τελικά το σύστημα επιτυγχάνει τους στόχους που έχουν τεθεί

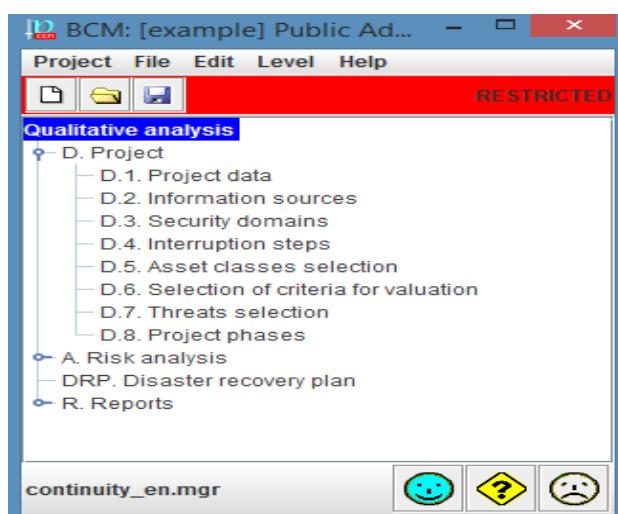
ή όχι. Το Pilar υπολογίζει την επίπτωση σε περίπτωση που το σύστημα επανέλθει μετά από το πέρας ενός χρονικού διαστήματος X. Αν η επίπτωση αυτή είναι αποδεκτή, τότε υπάρχει περιθώριο το RTO να πάρει μεγαλύτερη τιμή. Το επιθυμητό RTO επιλέγεται μελετώντας της αποτίμηση των υπηρεσιών του συστήματος στην ενότητα “Assets/ Valuation”. Ένα άνω όριο για το RTO μπορεί να εξαχθεί παρατηρώντας την κλιμάκωση στις επιπτώσεις. Για τον έλεγχο του κατά πόσο το σύστημα τηρεί το επιθυμητό RTO σε μια συγκεκριμένη χρονική φάση, το εργαλείο αναλύει την εναπομένουσα επίπτωση στην ενότητα “Backup/ aggregated”.

Σε περίπτωση προετοιμασίας του πλάνου ανάκαμψης μπορούν να χρησιμοποιηθούν τα εξής:

- (α) Το ίδιο RTO που χρησιμοποιήθηκε στον υπολογισμό της επίπτωσης,
- (β) οι αντικειμενικοί στόχοι ανάκαμψης,
- (γ) ευρετήριο με σειρά προτεραιότητας ανάλογα με το μέγεθος της καταστροφής.

6.4.6.1.Αρχικοποίηση Έργου

Η αρχικοποίηση του έργου στο εργαλείο Pilar παρουσιάζει μικρές διαφορές σε σχέση με το έργο ανάλυσης και αποτίμησης επικινδυνότητας. Οι περισσότερες επιλογές στο μενού προετοιμασίας του έργου παραμένουν ίδιες. Ωστόσο, στη διαδικασία προστίθεται η λειτουργία “Interruption Steps”, ενώ δεν υπάρχει πλέον η δυνατότητα επιλογής των διαστάσεων ασφάλειας.



Εικόνα 29: Αρχικό μενού για Επιχειρησιακή Συνέχεια

Τα “Interruption Steps” πρόκειται στην ουσία για τα χρονικά σημεία στα οποία θα εκτελεστεί ανάλυση της διακοπής της λειτουργίας του συστήματος. Το Pilar παρέχει ένα σύνολο προκαθορισμένων σημείων, αλλά δίνει την δυνατότητα προσθήκης νέων από το χρήστη. Επίσης, δίνει την επιλογή απόκρυψης ενός συγκεκριμένου σημείου από την ανάλυση, επιλέγοντας το on/off.



Εικόνα 30: Interruption Steps

6.4.6.2.Στάδιο Ανάλυσης Επικινδυνότητας

Αναγνώριση και Αποτίμηση Αγαθών και Απειλών

Αφότου οριστούν οι βασικές παράμετροι, ακολουθεί η διαδικασία αναγνώρισης και αποτίμησης των αγαθών. Η διαδικασία δεν παρουσιάζει καμία διαφορά από αυτή που εκτελείται στην ανάλυση και αποτίμηση επικινδυνότητας και οι επιλογές που παρουσιάζονται στο χρήστη είναι επίσης εφάμιλλες. Ωστόσο, αλλάζει η σειρά των εργασιών.

Αρχικά εκτελείται η αναγνώριση και αποτίμηση αγαθών με τον ίδιο τρόπο που εκτελείται και σε έργο ανάλυσης επικινδυνότητας. Η διαφορά έγκειται στο ότι πλέον δεν υπάρχει προσθήκη CPE αρχείων (προκατασκευασμένες λίστες με τεχνολογικά προϊόντα), καθώς διαφέρει ο σκοπός για τον οποίο γίνεται η ανάλυση. Έπειτα ακολουθεί η αναγνώριση και αποτίμηση απειλών, με την διαφορά πως δεν υπάρχει η επιλογή εισαγωγής CVE's.

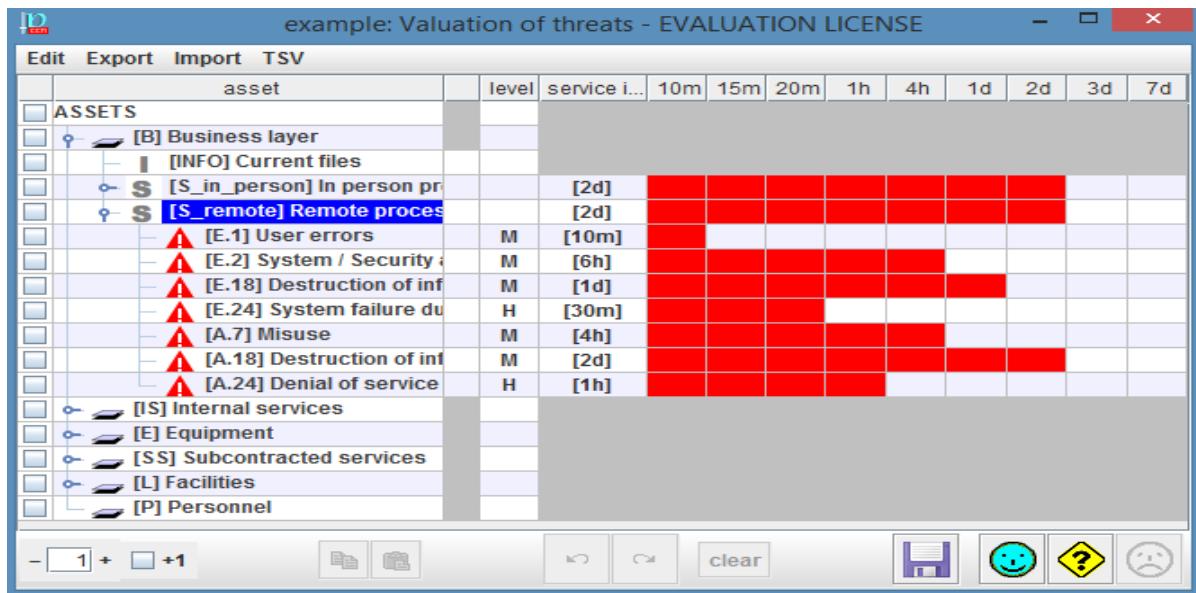
Η αποτίμηση των αγαθών και των απειλών γίνεται στα πλαίσια του χρονικού ορίου που έχει οριστεί κατά τη φάση προετοιμασίας του έργου και όχι υπό το πρίσμα των 5 πτυχών ασφάλειας. Η αποτίμηση αγαθών ανά πεδίο παρέχει ένα γρήγορο τρόπο αποτίμησης, κοινό για όλα τα αγαθά σε ένα πεδίο (domain). Χρησιμοποιώντας αυτή τη μέθοδο αποτίμησης, όλα τα αγαθά στο πεδίο λαμβάνουν τις ίδιες τιμές. Σε περίπτωση χρήσης της μεθόδου αποτίμησης, “αγαθό με αγαθό” (asset by asset)

απαιτείται η αντιστοίχηση των αγαθών και η δημιουργία των εξαρτήσεων κατά τη φάση της αναγνώρισης αγαθών.

Εικόνα 31: Αποτίμηση αγαθών ανά επίπεδο

Η αποτίμηση για κάθε Interruption phase γίνεται στην κλίμακα από 0 (αμελητέα) έως 10 (απολύτως κρίσιμη) ή ακολουθώντας τα κριτήρια από 0 έως 9. Η κλίμακα αποτυπώνει το πόσο κρίσιμο είναι να υπάρξει διακοπή της λειτουργίας του συγκεκριμένου αγαθού κατά τη συγκεκριμένη χρονική περίοδο.

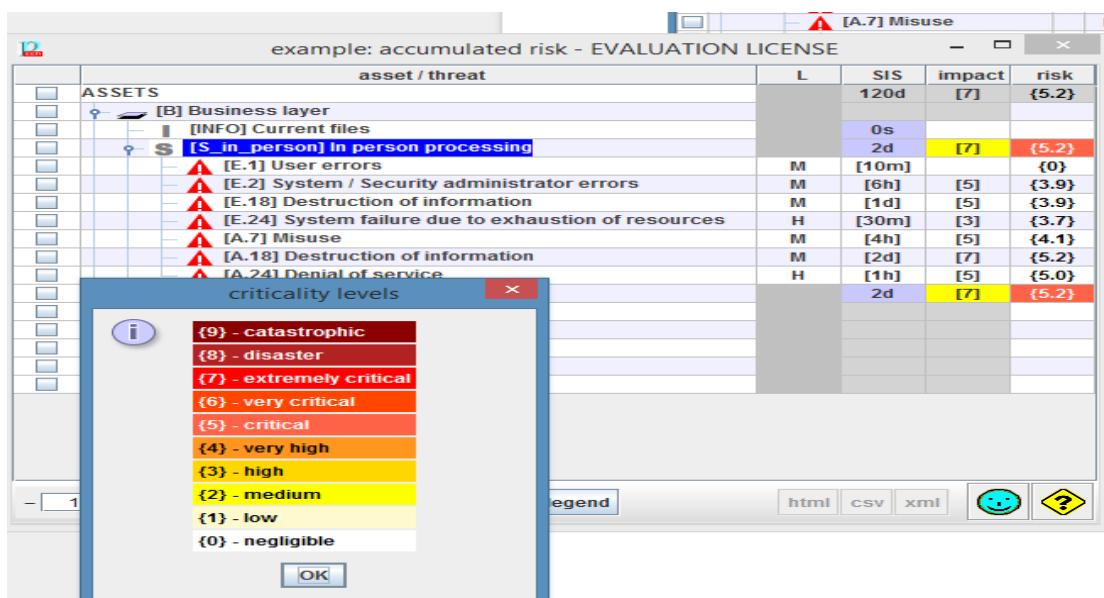
Η διαφορά στη διαδικασία αποτίμησης απειλών σε ένα έργο συνέχισης λειτουργίας από το έργο ανάλυσης και αποτίμησης επικινδυνότητας είναι πως στην πρώτη περίπτωση το Pilar υπολογίζει το χρονικό περιθώριο που η υπηρεσία ή το αγαθό δεν θα είναι διαθέσιμα και ανάλογα κρίνει την επίπτωση αυτή. Οι κλίμακες αποτίμησης παραμένουν ίδιες. Επίσης, παρέχεται γραφικά το χρονικό περιθώριο διακοπής της διαθεσιμότητας του αγαθού/υπηρεσίας (Εικόνα 32).



Εικόνα 32: Αποτίμηση απειλών

Αποτίμηση Επικινδυνότητας και Επιπτώσεων

Σε αυτό το βήμα το εργαλείο παρέχει δύο “παθητικές” (passive) οθόνες, οι οποίες δείχνουν τα αποτελέσματα σχετικά με την αποτίμηση για τις συσσωρευμένες και αποκλίνουσες τιμές επικινδυνότητας και επίπτωσης στο σύστημα (Εικόνα 33). Η κλίμακα αποτίμησης παραμένει από το 0 έως το 10.



Εικόνα 33: Παθητικές εικόνες (Συσσωρευμένη επικινδυνότητα)

Στον πίνακα που δημιουργεί το Pilar παρουσιάζεται η πιθανότητα απώλειας (L) της διαθεσιμότητας του αγαθού ή υπηρεσίας εξαιτίας μιας απειλής, το χρονικό περιθώριο

που θα επηρεαστεί το σύστημα (SIS) καθώς και οι τιμές της επίπτωσης και της επικινδυνότητας.

Εφεδρικός Εξοπλισμός

Στην περίπτωση ύπαρξης εφεδρικού εξοπλισμού για την αντικατάσταση ενός αγαθού ή υπηρεσίας, η επίπτωση περιορίζεται από το χρόνο που απαιτείται μέχρι την εκκίνηση λειτουργίας του εφεδρικού αυτού εξοπλισμού.

Το εργαλείο συλλέγει το χρόνο που απαιτείται για την έναρξη τέτοιου είδους εξοπλισμού σε κάθε φάση του έργου. Με μαύρο χρώμα σηματοδοτείται εξοπλισμός που είναι διαθέσιμος μόνο σε μία φάση, ενώ με κόκκινο χρώμα απεικονίζεται εξοπλισμός για τον οποίο δεν έχει οριστεί εφεδρικός ή κάποια τιμή. Αν σε μια φάση δεν οριστεί τιμή, το Pilar μεταβιβάζει την τιμή της προηγούμενης φάσης με κόκκινο.

The screenshot shows a software window titled "example: Backup equipment - EVALUATION L...". The main area is a table with three columns: "asset", "current", and "target". The table is organized by asset type under the heading "ASSETS".

asset	current	target
ASSETS		
[B] Business layer		
[INFO] Current files	[1d] /	[1d] /
[S_in_person] In person processing		
[S_remote] Remote processing		
[IS] Internal services		
[A] [email] E-mail	[4h] /	[4h] /
[A] [archive] Central historical archive	[10m] /	[10m] /
[technical] Technical Services, Auxiliary		
[E] Equipment		
[SS] Subcontracted services		
[L] Facilities		
[D] Personnel		
[]	- 1 +	aggregate
		CSV
		Smiley
		?
		Sad

Εικόνα 34: Παράδειγμα ορισμού εξοπλισμού

Επιλέγοντας ένα αγαθό, ο αναλυτής μπορεί να ορίσει το επίπεδο ωριμότητας καθώς και το χρονικό διάστημα που απαιτείται για να εγκατασταθεί ο εφεδρικός εξοπλισμός του. Το Pilar επίσης συναθροίζει τις τιμές (με την επιλογή “Aggregate”) και εμφανίζει στο χρήστη αποτιμήσεις όλων των αγαθών λαμβάνοντας υπόψη το μεγαλύτερο χρόνο αποκατάστασης σε περιπτώσεις που δεν έχει δηλωθεί εφεδρικός εξοπλισμός, διαφορετικά υπολογίζει με βάση το συντομότερο χρόνο.

Προσδιορισμός προτεινόμενων αντιμέτρων

To Pilar ακολουθεί την ίδια διαδικασία όπως αυτή πραγματοποιείται σε ένα έργο ανάλυσης και αποτίμησης επικινδυνότητας.

Εκτίμηση Εναπομένουσας Επικινδυνότητας

Έπειτα από τον προσδιορισμό των αντιμέτρων ακολουθεί το βήμα υπολογισμού της εναπομένουσας επικινδυνότητας. Ομοίως με το βήμα αποτίμησης επικινδυνότητας και επιπτώσεων παρουσιάζονται οι πίνακες με τις συσσωρευμένες και αποκλίνουσες τιμές της εναπομένουσας επικινδυνότητας στο σύστημα. Το εργαλείο όμως παρέχει στο βήμα αυτό χωριστούς πίνακες για την επικινδυνότητα και για την επίπτωση καθώς και ένα συγκεντρωτικό.

6.4.6.3.Στάδιο Πλάνου Ανάκαμψης Λειτουργίας

Αφού ολοκληρωθεί το στάδιο της ανάλυσης επικινδυνότητας και των επιπτώσεων, ακολουθεί η προετοιμασία του πλάνου ανάκαμψης από καταστροφή. Το εργαλείο βιοηθά στη δημιουργία ενός τέτοιου πλάνου, αλλά δε λαμβάνει υπόψη τα αντίμετρα, καθώς στηρίζεται στην υπόθεση πως όλα λειτουργούν βάσει του αρχικού σχεδίου. Μέσω του εργαλείου μπορούν να αποδοθούν τιμές από τους χαρακτηρισμούς “διαθέσιμο”, “στόχος” και “απαιτούμενο”. Ρυθμίζοντας τον επιθυμητό χρόνο ανάκαμψης για κάθε αγαθό, το εργαλείο επιλέγει αυτόμata το χρονικό διάστημα που το αγαθό θα είναι και πάλι διαθέσιμο με βάση τα δεδομένα που εισήχθηκαν στα προηγούμενα βήματα.



Εικόνα 35: Πλάνο Ανάκαμψης Λειτουργίας

Τέλος το εργαλείο μπορεί να παράξει διάφορα γραφήματα για χρήση στις αναφορές που θα παραδοθούν στη διοίκηση του οργανισμού.

7. Αξιολόγηση μεθόδων

Οι μέθοδοι μελέτης και διαχείρισης της επικινδυνότητας μπορούν να αξιολογηθούν βάσει κριτηρίων. Ωστόσο, δεν υπάρχει κοινό πλαίσιο που να υπαγορεύει ποια ακριβώς κριτήρια μπορούν να χρησιμοποιηθούν. Ωστόσο είναι η αδήριτη η ανάγκη αξιολόγησης των υπαρχουσών μεθόδων, ώστε να καθοριστεί ποιες είναι καταλληλότερες για κάθε οργανισμό και για τις ιδιαίτερες ανάγκες του.

7.1 Τεχνικές αξιολόγησης της ανάλυσης επικινδυνότητας

Οι τεχνικές για την αξιολόγησης της ανάλυσης επικινδυνότητας είναι διάφορες και η εφαρμογή τους ποικίλει. Ωστόσο, μπορούν να ταξινομηθούν με διάφορα κριτήρια, όπως το χρονοδιάγραμμα, τον τρόπο διεξαγωγής και τον σκοπό τους.

Έτσι, έχουμε τις εξής τρεις κατηγορίες (Bourguignon et al., 2002) σχετικά με το χρόνο διεξαγωγής τους:

Η εκ των προτέρων αξιολόγηση (Ex ante evaluation) πραγματοποιείται πριν από την εφαρμογή μιας παρέμβασης, αλλά χρειάζεται να προγραμματιστεί, δηλαδή να καθοριστεί με κάποιο βαθμό λεπτομέρειας. Μια εκ των προτέρων αξιολόγηση επιτρέπει την αξιολόγηση της καταλληλότητας και της συνοχής της δράσης, διότι τα πορίσματά της λαμβάνονται υπόψη προτού ληφθούν οι τελικές αποφάσεις. Επίσης, επιτρέπει την εκτίμηση τυχόν προβλημάτων κατά τη φάση της ανάπτυξης, το κατά πόσον η στρατηγική και οι στόχοι είναι συναφείς, εάν υπάρχει ασυμφωνία μεταξύ τους και αν η επιθυμητή επίδραση είναι ρεαλιστική.

Η προσωρινή αξιολόγηση (Ad interim evaluation) καλύπτει το σύνολο του χρονικού ορίζοντα εφαρμογής μιας παρέμβασης και δεδομένου ότι λαμβάνει χώρα κατά τη διάρκεια της παρακολούθησης των εκροών και των αποτελεσμάτων, συχνά συγχέεται με την εν λόγω δραστηριότητα, ακόμα κι αν είναι ξεχωριστές. Η αξιολόγηση αυτή αποτελείται από μια σειρά λεπτομερών μελετών, δεδομένου ότι περιλαμβάνει περαιτέρω ανάλυση σχετικά με τα θέματα αποτίμησης που προκύπτουν κατά την υλοποίηση. Επιτρέπει μια συνεπή και αποτελεσματική συνεργασία μεταξύ του υπεύθυνου αξιολόγησης και του προσώπου που διαχειρίζεται και εκτελεί την παρέμβαση, και ως εκ τούτου εξάγει καλύτερα και πιο κατάλληλα συμπεράσματα και προτάσεις.

Η εκ των υστέρων αξιολόγηση (Ex post evaluation) δεν πραγματοποιείται πριν από τον τερματισμό της παρέμβασης και μετά από ένα εύλογο χρονικό διάστημα. Επιδιώκει να εκτιμήσει την αποδοτικότητα και την αποτελεσματικότητα μιας παρέμβασης, προκειμένου να προσδιοριστούν οι παράγοντες της επιτυχίας ή της αποτυχίας, να εκτιμήσει τη βιωσιμότητα των αποτελεσμάτων και των επιπτώσεων και να εξάγει συμπεράσματα που μπορούν να γενικευτούν και σε άλλες παρεμβάσεις. Για το λόγο αυτό, η εκ των υστέρων αξιολόγηση πρέπει να διεξάγεται καθυστερημένα σε σχέση με το πέρας της υλοποίησης και προσανατολίζεται περισσότερο προς μελλοντικές παρόμοιες λύσεις αντί εκείνης που αξιολογείται.

Η αξιολόγηση μπορεί επίσης να διενεργείται από ανθρώπους εντός ή εκτός του οργανισμού που αναπτύσσει την λύση, με αποτέλεσμα να έχουμε δύο ξεχωριστούς **τύπους κατηγοριοποίησης της αξιολόγησης** (Bloom & Milkovich, 1998):

Εσωτερική αξιολόγηση πραγματοποιείται από οργανισμούς, ομάδες ή κοινότητες που εμπλέκονται άμεσα στην υλοποίηση της παρέμβασης. Χρησιμοποιείται συνήθως σε συνδυασμό με άλλες μορφές εξωτερικής αξιολόγησης και είναι χρήσιμο να επιτρέπεται σε εκείνους που συμμετέχουν στην εκτέλεση να βελτιώνουν τις επιδόσεις τους και να προσαρμόζουν τα προγράμματα που βρίσκονται σε εξέλιξη.

Εξωτερική αξιολόγηση διενεργείται από εξωτερικούς ειδικούς που δεν εργάζονται εντός του οργανισμού που είναι υπεύθυνος για το αντικείμενο της αξιολόγησης και οι οποίοι δεν έχουν προσωπικό, οικονομικό ή άμεσο ενδιαφέρον για το αντικείμενο. Οι εξωτερικές αξιολογήσεις εγγυώνται μια περισσότερο κριτική και αμερόληπτη εκτίμηση του υπό αξιολόγηση αντικειμένου από ό, τι είναι δυνατόν να επιτύχει μια εσωτερική αξιολόγηση, αλλά από την άλλη πλευρά, η εσωτερική αξιολόγηση επιτρέπει βαθύτερη και ταχύτερη πρόσβαση στην πληροφορία καθώς και μια ευρύτερη γνώση του υπό αξιολόγηση αντικειμένου.

Επιπλέον, η αξιολόγηση αυτή μπορεί να έχει περαιτέρω διαβάθμιση, ανάλογα με τον **σκοπό της** (Bloom, 1971):

- **Η διαμορφωτική αξιολόγηση** (Formative evaluation) χρησιμοποιείται για τη στήριξη των φορέων, όπως των διευθυντών και των ατόμων που ενδιαφέρονται άμεσα και εμπλέκονται, βοηθώντας τους να βελτιώνουν τις αποφάσεις και τις δραστηριότητές τους γενικότερα. Εφαρμόζεται κυρίως κατά τη διάρκεια της

υλοποίησης μιας παρέμβασης και ως εκ τούτου, έχει σαν στόχο να εκτιμήσει την αποτελεσματικότητα και τη σημασία της.

- Η **αθροιστική αξιολόγηση** (Summative evaluation) αφορά τον προσδιορισμό της αποτελεσματικότητας της παρέμβασης. Πραγματοποιείται προς όφελος των εξωτερικών παρατηρητών ή των φορέων λήψης αποφάσεων (που δεν εμπλέκονται άμεσα στην ανάπτυξη της παρέμβασης). Αθροιστική αξιολόγηση γίνεται, για παράδειγμα, για λόγους υπευθυνότητας, για την υποβολή εκθέσεων σχετικά με τα αποτελέσματα της έρευνας ή έξοδα που τα δικαιολογούν.

Η αξιολόγηση, ως γενική εκτίμηση, μπορεί να αναλυθεί σε τέσσερις διακριτές φάσεις:

1. Τη **φάση διάρθρωσης** κατά την οποία αναγνωρίζονται τα κριτήρια επιτυχίας, οι δείκτες, οι απορίες, οι πηγές δεδομένων και τα επίπεδα-στόχοι. Αυτό το βήμα εξασφαλίζει ότι η μέθοδος αξιολόγησης υλοποιείται σύμφωνα με αναγνωρισμένες μεθόδους συλλογής δεδομένων, παρέχοντας έτσι μια βάση για τον καθορισμό των απαιτούμενων πληροφοριών και την αξιολόγηση της απόδοσης των παρεμβάσεων. Η φάση της διάρθρωσης παρέχει συνήθως μια έκθεση που αναδεικνύει την επιχειρησιακή στρατηγική για την αξιολόγηση.
2. Η **φάση συλλογής δεδομένων** είναι η συλλογή ποιοτικών ή/και ποσοτικών στοιχείων. Ως εκ τούτου, αναγνωρίζει πληροφορίες, γνωμοδοτήσεις και αντιλήψεις.
3. Η **φάση της ανάλυσης δεδομένων** αφορά την αναθεώρηση των δεδομένων που συλλέγονται κατά την προηγούμενη φάση με τη χρήση διαφόρων εργαλείων και τεχνικών, όπως η ανάλυση μιας έρευνας, μιας συνέντευξης και ούτω καθεξής.
4. Η **φάση της διατύπωσης αποφάσεων** αποτελεί το τελικό στάδιο της αξιολόγησης. Η φάση αυτή εξετάζει την παρέμβαση σε σχέση με συγκεκριμένα κριτήρια.

Ανάλογα με τις φάσεις της διαδικασίας αξιολόγησης, χρησιμοποιούνται διαφορετικά εργαλεία και τεχνικές, όπως (Gupta, 2011)):

- Παρακολούθηση.
- Ανάλυση SWOT (strengths – weaknesses – opportunities – threats).
- Ερωτηματολόγιο.

- Μελέτες περιπτώσεων.
- Αναλυτικά μοντέλα.
- Διαβουλεύσεις από επιτροπές ειδικών.
- Ανάλυση κόστους-οφέλους.
- Πολυκριτηριακή ανάλυση.

Λαμβάνοντας υπόψη τις τεχνικές διαβουλεύσεις με τις οποίες εξάγονται οι γνωμοδοτήσεις, διατίθεται ένας αρκετά μεγάλος αριθμός επιλογών (Pickard, 2013):

Συνέντευξη (ή πρόσωπο με πρόσωπο): Συνήθως οι συνεντεύξεις βασίζονται σε διεξοδικές ή και διαπροσωπικές συζητήσεις, ώστε να συγκεντρωθούν συγκεκριμένες πληροφορίες σχετικά με επιμέρους ζητήματα. Η τεχνική της συνέντευξης χρησιμοποιείται για τη συλλογή ποιοτικών πληροφοριών και απόψεων των ανθρώπων που συμμετέχουν σε ένα συγκεκριμένο πρόγραμμα ή σχέδιο, στο πλαίσιο του ή το αποτέλεσμα ή τις επιπτώσεις του. Διακρίνονται διάφορες μορφές ομιλίας, κάθε μία από τις οποίες έχει διαφορετικό σκοπό: μια άτυπη συνέντευξη, μια ημιδομημένη συνέντευξη που κατευθύνεται και μια δομημένη συνέντευξη (η αυστηρότερη προσέγγιση) (Landoll & Landoll, 2005).

Ομάδες εστίασης (focus groups): αυτές είναι οι συνεντεύξεις/συζητήσεις που στοχεύουν σε μια ομοιογενή ομάδα ατόμων που αποτελείται από έναν αριθμό ανθρώπων (συνήθως από 6 έως 12) των οποίων η προσοχή εστιάζεται σε ένα συγκεκριμένο θέμα που έχει διερευνηθεί σε βάθος. Ο συντονιστής κατευθύνει και οδηγεί τη συζήτηση μεταξύ των συμμετεχόντων και διευκολύνει την αλληλεπίδραση. Η τεχνική αυτή εφαρμόζεται συνήθως με μια ήπια προσέγγιση ποιοτικής αξιολόγησης, δηλαδή όταν είναι σκόπιμο να χρησιμοποιούνται οι εκτιμήσεις, κρίσεις, απόψεις που εκφράζονται από ειδικούς επαγγελματίες, και οι χρήστες/πελάτες να συγκεντρώνουν διαφορετικές απόψεις σχετικά με ένα θέμα, μια διαδικασία, ένα αποτέλεσμα, ένα προϊόν κ.λπ. (Peltier, 2005).

Τεχνική Delphi: σε αντίθεση με την ομάδα εστίασης όπου οι εμπειρογνώμονες καλούνται να ανταποκριθούν από κοινού στις ερωτήσεις που εκπονήθηκαν από το διαμεσολαβητή για τους στόχους της διαβούλευσης, η τεχνική Delphi βασίζεται στην έμμεση αλληλεπίδραση και στη δομημένη επικοινωνία μεταξύ εμπειρογνωμόνων. Ονομάζεται επίσης «επαναλαμβανόμενη συνέντευξη» με την έννοια ότι οι ίδιοι εμπειρογνώμονες απαντούν σε τουλάχιστον δύο ενότητες ερωτήσεων, που πρέπει να

είναι σταδιακά περισσότερο δομημένες με βάση τα αποτελέσματα του προηγούμενου γύρου συνεντεύξεων. Σε σύγκριση με την ομάδα εστίασης, η τεχνική αυτή είναι περισσότερο χρονοβόρα, αλλά είναι οπωσδήποτε ευκολότερο οι εμπειρογνώμονες να οργανώνονται έτσι ώστε να πραγματοποιούν μία κάθε φορά, ενώ η ομάδα εστίασης πρέπει να συντάσσεται στην ίδια θέση, την ίδια ώρα και για τον ίδιο χρόνο (Wang, 2005).

Τεχνική ονομαστικών ομάδων (nominal groups): Η τεχνική αυτή διαφέρει από την τεχνική Delphi, καθώς οι εμπειρογνώμονες βρίσκονται στο ίδιο μέρος την ίδια χρονική στιγμή, και συνήθως δεν αλληλεπιδρούν άμεσα μεταξύ τους, αλλά πάντα μέσω του ερευνητή που συλλέγει και επεξεργάζεται περιοδικά τις μαρτυρίες που δίνονται, προφορικά ή γραπτά. Η τεχνική αυτή απαιτεί από τους εμπειρογνώμονες που συμμετέχουν να γνωρίζουν τις απαντήσεις που δόθηκαν από άλλους συμμετέχοντες και να εκφράζουν τις απόψεις τους ή να κάνουν προσθήκες, αλλά μόνο με τη σειρά τους, χωρίς να απαντούν απευθείας στο συντάκτη της παρέμβασης (Potter et al., 2004).

Καταιγισμός ιδεών (brainstorming): αυτή είναι μια από τις πολλές μη ομαδικές τεχνικές που αναπτύχθηκαν για την αξιολόγηση και που επικεντρώνεται ιδιαίτερα προς τη διευκόλυνση της δημιουργικότητας και της παραγωγής νέων ιδεών. Η παραδοσιακή εκδοχή του καταιγισμού ιδεών περιλαμβάνει μια ομάδα ανθρώπων, που είναι καλύτερο να καθοδηγείται από έναν συντονιστή. Η ομάδα καλείται να παράγει νέες ιδέες και όχι παρατηρήσεις πάνω σε παλιές, ανεξάρτητα από την αξία τους (Akintoye et al., 2001).

Όπως είναι αναμενόμενο οι τεχνικές αυτές έχουν πολλούς περιορισμούς και μειονεκτήματα. Ωστόσο, κοινά προβλήματα που ανακύπτουν κατά τη διάρκεια της αξιολόγησης, ανεξάρτητα από την κάθε μεμονωμένη τεχνική που χρησιμοποιείται είναι: η έλλειψη δεδομένων, απλοϊκή ή υποκειμενική ταξινόμηση δεδομένων, συλλογή ασήμαντων πληροφοριών ή πληροφοριών που δεν μπορούν να χρησιμοποιηθούν για γενικεύσεις, μεροληπτικές ή αναξιόπιστες απαντήσεις, λάθη στην επιλογή των εμπλεκόμενων συμμετεχόντων, αυθαίρετη επιλογή πληροφοριών, ασάφεια αποτελεσμάτων κ.λπ.

Αυτός είναι ο λόγος που συγκεκριμένα προβλήματα τα οποία συνδέονται με κάποιο είδος αξιολόγησης θα μπορούσαν να μετριαστούν με τη χρήση σύνθετης ανάλυσης. Ωστόσο, παρά τα πλεονεκτήματά της, η πολυκριτιριακή αξιολόγηση απαιτεί σχολαστική προετοιμασία για να αναλύσει σωστά τα δεδομένα. Πιο συγκεκριμένα, συχνά παρατηρείται έλλειψη στα διαθέσιμα δεδομένα για τη σύγκριση μεγεθών όπως η πιθανοφάνεια εκτιμήσεων σε σχέση με τη συχνότητά τους σε βάθος χρόνου. Επιπλέον, εξαιτίας της σπανιότητας των περιστατικών ασφάλειας, ακόμη και τα πιο συχνά εμφανιζόμενα γεγονότα θα απαιτούσαν πολύ μεγάλη περίοδο δειγματοληψίας, προκειμένου να συγκεντρωθούν επαρκείς εμφανίσεις και, συνεπώς, να εκτιμηθεί με στατιστικά αποδεκτή ακρίβεια η σχετική συχνότητά τους. Ως εκ τούτου, η μόνη βιώσιμη στρατηγική για την εκτίμηση της συνολικής αποτελεσματικότητας του εργαλείου είναι η εκμετάλλευση της εμπειρίας μιας σημαντικής ομάδας τελικών χρηστών και η αξιολόγησή της με βάση (Kiker, et al., 2005):

- Τη διαισθητικότητα (intuitiveness): πώς οι εκτιμήσεις που παράγονται από το προτεινόμενο μοντέλο εκτίμησης επικινδυνότητας ταιριάζουν με εκείνες των τελικών χρηστών ή δείχνουν αναμενόμενες/λογικές.
- Τη χρηστικότητα: ευκολία χρήσης, χρησιμότητα αποτελέσματος.

7.2 Βιβλιογραφική ανασκόπηση κριτηρίων αξιολόγησης μεθόδων και εργαλείων

Τα κριτήρια επιλογής μεθόδων ανάλυσης επικινδυνότητας, δεν έχουν προτυποποιηθεί. Ωστόσο, πρόκειται για ένα συστατικό ζωτικής σημασίας για την επιλογή της κατάλληλης μεθόδου ανάλυσης επικινδυνότητας. Χωρίς τα μέσα για τη σύγκριση των μεθόδων, τόσο η σύγκριση όσο και η επιλογή γίνονται αυθαίρετες. Η επιλογή μιας ακατάλληλης μεθόδου ή εργαλείου θα μπορούσε να οδηγήσει σε υπερβολική αύξηση των πόρων και γενικά υπερβολικές δαπάνες.

Οι Fischhoff et al. (1981) προσπάθησαν να ορίσουν κριτήρια αξιολόγησης για τις μεθόδους ανάλυσης επικινδυνότητας στις κοινωνικές επιστήμες. Ήταν σε θέση να ταξινομήσουν τις μεθόδους ανάλυσης επικινδυνότητας σε τρεις ομάδες ανάλογα με τον τρόπο ανάλυσης: 1) τυπική ανάλυση, 2) bootstrapping (είδος στατιστικής ανάλυσης) και 3) την επαγγελματική κρίση. Τα κριτήρια που εφαρμόζονται είναι υποκειμενικά και ορίζονται ποιοτικά (Fischhoff et al., 1981).

Η τυπική ανάλυση περιλαμβάνει μια ευρεία συλλογή τυποποιημένων εργαλείων και μεθόδων λήψης αποφάσεων, συμπεριλαμβανομένης της ανάλυσης των αποφάσεων και κόστους-οφέλους (Merkhofer, 1983). Η υπόθεση σε αυτή την προσέγγιση είναι ότι οι «πνευματικές τεχνολογίες» μπορούν να χρησιμοποιηθούν για να βοηθήσουν στην αντιμετώπιση προβλημάτων που δημιουργούνται από φυσικές τεχνολογίες (Fischhoff et al., 1981). Η προσέγγιση bootstrapping ουσιαστικά περιλαμβάνει τον εντοπισμό και τη συνέχιση των πολιτικών που έχουν εξελιχθεί με την πάροδο του χρόνου. Υπάρχουν προβλήματα, ωστόσο, καθώς η προσέγγιση αυτή αντικατοπτρίζει την προκατάληψη πως ό,τι ίσχυε ακριβώς στο παρελθόν ήταν και εξακολουθεί να είναι σωστό (Mooney, & Duval, 1993). Η επαγγελματική κρίση ενός εμπειρογνώμονα, είναι η απόφαση τεχνικών εμπειρογνωμόνων, που είναι γνώστες του τομέα και λαμβάνουν κρίσιμες αποφάσεις (Fischhoff et al., 1981).

Μια άλλη προσπάθεια έχει γίνει από τον Merkhofer το 1985 για την αξιολόγηση μεθόδων διαχείρισης του κοινωνικού κινδύνου. Ο Merkhofer κατηγοριοποιεί τα κριτήρια για την αξιολόγηση σε εσωτερικά (που αφορούν τον τομέα της ανάλυσης) ή εξωτερικά (που σχετίζονται με τις σκέψεις και τους περιορισμούς εκτός του πλαισίου της ανάλυσης). Στο πλαίσιο αυτής της ταξινόμησης των σκέψεων για μια συγκεκριμένη μέθοδο, ο Merkhofer ορίζει συγκεκριμένα κριτήρια, όπως λογική ορθότητα (logical soundness), πληρότητα (completeness), ακρίβεια (accuracy), πρακτικότητα (practicality) και αποδοχή (acceptability). Κάθε κριτήριο χρησιμοποιείται για να βοηθήσει τον αναλυτή στον καθορισμό της πιο κατάλληλης μεθόδου για τη δεδομένη κατάσταση. Η ερμηνεία της έννοιας ή του βαθμού εφαρμογής για κάθε κριτήριο και πάλι επαφίεται στην κρίση του αναλυτή (Merkhofer, 1987). Η λογική ορθότητα εξασφαλίζει ότι η αξιολόγηση της επικινδυνότητας μπορεί να τεκμηριωθεί από τη θεωρία και ότι η εφαρμογή της δεν παραβιάζει θεμελιώδεις παραδοχές. Η πληρότητα εξασφαλίζει ότι εξετάζονται όλες οι σχετικές πτυχές της επικινδυνότητας και δεν υπάρχουν σημαντικές παραλείψεις. Η ακρίβεια δείχνει ότι η μέθοδος είναι απαλλαγμένη από πιθανές προκαταλήψεις και είναι ευαίσθητη σε υποθέσεις που δεν έχουν ή δεν μπορούν να ελεγχθούν. Η πρακτικότητα εξασφαλίζει ότι η ανάλυση μπορεί να γίνει σε πραγματικά προβλήματα χρησιμοποιώντας διαθέσιμους πόρους και πληροφορίες. Η αποδοχή περιλαμβάνει τη συμμόρφωση με πρότυπα και διαδικασίες και την εύκολη κατανόηση από τους χρήστες.

Το πλαίσιο του Katzke (1988) αποτελεί μία οργανωμένη προσπάθεια για την κατηγοριοποίηση των μεθόδων ανάλυσης επικινδυνότητας. Περιλαμβάνει περιγραφή των στοιχείων που σχετίζονται με την ανάλυση επικινδυνότητας καθώς και τις συσχετίσεις μεταξύ τους (Mayerfeld, 1989). Αναφερόμενος στο πλαίσιο Katzke, ο Browne κάνει μια κριτική θεώρηση και αναφέρει ότι ένα από τα στοιχεία που δεν περιλαμβάνονται στο πλαίσιο είναι μια έκθεση κριτηρίων. Σύμφωνα με τα κριτήρια αυτά, ένας οργανισμός ή ένας αναλυτής θα πρέπει να δημιουργήσει, να εμπλουτίσει ή να αξιολογήσει μια μέθοδο ως εργαλείο ανάλυσης επικινδυνότητας. Πιο συγκεκριμένα, προτείνει μια σειρά κριτηρίων όπως το εύρος και το βάθος της ανάλυσης, το κόστος, η ακρίβεια των αποτελεσμάτων, η επαναληψιμότητα και η αναγνωρισιμότητα της μεθόδου, τα οποία πρέπει να είναι σαφή και ρητά (Browne, 1989).

Οι Olle et al. (1988) πρότειναν ότι μία μέθοδος ανάλυσης επικινδυνότητας θα πρέπει κατά προτίμηση να πληροί τα ακόλουθα κριτήρια:

1. Να περιλαμβάνει διαδοχικά και αυστηρά καθορισμένα βήματα.
2. Το αποτέλεσμα σε καθένα από τα στάδια να εξυπηρετεί ένα συγκεκριμένο σκοπό και να παράγει καλά προσδιορισμένα αποτελέσματα.
3. Το αποτέλεσμα σε κάθε βήμα να μπορεί να επικυρωθεί από ανεξάρτητους ελεγκτές.
4. Οι πόροι που χρησιμοποιούνται σε κάθε βήμα να είναι περιορισμένοι.
5. Η τεχνογνωσία που απαιτείται για την εκτέλεση κάθε βήματος να είναι ομοιογενής και να χρειάζεται περιορισμένος αριθμός εμπειρογνωμόνων διαφόρων ειδικοτήτων.
6. Η αλληλουχία των βημάτων να μπορεί να επαναληφθεί αρχής γενομένης από οποιοδήποτε από τα ενδιάμεσα προϊόντα για τη βελτίωση του συνολικού και του τελικού αποτελέσματος.

Στη συνέχεια, στην έρευνα των Garrabrant et al. (1990) εμφανίζεται η μέθοδος CERTS η οποία αποτελείται από 7 κριτήρια: συνοχή (consistency), χρηστικότητα (usability), προσαρμοστικότητα (adaptability), σκοπιμότητα (feasibility), πληρότητα (completeness), εγκυρότητα (validity) και αξιοπιστία (credibility). Κάθε κριτήριο μπορεί περιλαμβάνει δύο έως τέσσερα χαρακτηριστικά σύμφωνα με τα οποία μπορεί να αξιολογηθεί.

Ο Lichtenstein (1996) πρότεινε 17 κριτήρια, τα οποία πρέπει να ληφθούν υπόψη κατά την επιλογή της κατάλληλης μεθόδου ανάλυσης επικινδυνότητας. Η έρευνα βασίστηκε σε μεγάλο βαθμό σε εκείνη των Garrabrant et al. (1990) και ενσωμάτωσε πέντε από τα επτά κριτήρια τα οποία είχαν προταθεί. Στη συνέχεια, τα αρχικά 17 κριτήρια ομαδοποιήθηκαν και προέκυψαν τα παρακάτω (Lichtenstein, 1996):

1. Χαρακτηριστικά Μεθόδου: Κόστος, Απαίτηση για συμφωνία διοίκησης και αναλυτών, Ευελιξία, Πολυπλοκότητα, Πληρότητα, Συνέπεια, Ευκολία χρήσης, Σκοπιμότητα, Εγκυρότητα, Αξιοπιστία, Υποστήριξη από κατάλληλο λογισμικό.
2. Χαρακτηριστικά Οργανισμού: Επίπεδο επικινδυνότητας, Μέγεθος, Κουλτούρα ασφάλειας, Εξωτερικές απαιτήσεις, Οργανωσιακή δομή.

Οι Kitchenham et al. (1997) προτείνουν με τη μέθοδο DESMET τα παρακάτω κριτήρια για την αξιολόγηση των μεθόδων και των εργαλείων που χρησιμοποιούνται από πληροφοριακά συστήματα. Σύμφωνα με τη μέθοδο αυτή, τα κριτήρια που χρησιμοποιούνται είναι:

1. Το πλαίσιο της αξιολόγησης.
2. Η φύση της αναμενόμενης επίδρασης της μεθόδου ή του εργαλείου.
3. Η φύση του αντικειμένου/οργανισμού που αξιολογείται.
4. Η έκταση της επίδρασης της μεθόδου ή του εργαλείου.
5. Η ωριμότητα της μεθόδου ή του εργαλείου.
6. Η καμπύλη εκμάθησης που σχετίζεται με τη μέθοδο/εργαλείο.
7. Η ικανότητα οριοθέτησης του οργανισμού που υφίσταται την αξιολόγηση.

Ο Craft (1998) ορίζει ένα πλαίσιο που επικεντρώνεται στις διάφορες δραστηριότητες που μπορούν να εκτελεστούν κατά τη διάρκεια του κύκλου ζωής της ανάλυσης και διαχείρισης της επικινδυνότητας. Αυτά τα βασικά χαρακτηριστικά συνοψίζονται στα εξής: κατανόηση του συστήματος, δημιουργία κλίματος ασφάλειας, κατανόηση των τρωτών σημείων, αναγνώριση των κινδύνων και των απειλών, αξιολόγηση του συστήματος, κατάταξη των ευρημάτων της αξιολόγησης και διαφύλαξη του συστήματος.

Σε έρευνα που πραγματοποιήθηκε το 2004 από τους Bornman και Labuschagne τα κριτήρια κατηγοριοποιούνται σε τρεις ομάδες: *Κίνδυνοι*, *Διοίκηση* και *Διαδικασίες*. Για παράδειγμα στην ομάδα των «Κινδύνων» εξετάζεται το είδος, το επίπεδο

αποδοχής και το σχέδιο αντιμετώπισης. Οι Campell και Stamp (2004) χρησιμοποίησαν έναν άλλο τρόπο κατηγοριοποίησης που επιτρέπει τη σύγκριση των μεθόδων και την επιλογή της βέλτιστης. Πιο συγκεκριμένα, πρότειναν έναν πίνακα 3x3 που διαχωρίζει τις μεθόδους ανάλογα με την προσέγγισή τους σε χρονικές, λειτουργικές και υπολογιστικές και ανάλογα με το επίπεδο τους σε αφηρημένες, μεσαίου επιπέδου και συμπαγείς (concrete).

Οι Vorster και Labuschagne (2005) ορίζουν ένα πλαίσιο που συγκρίνει μεθόδους ανάλυσης επικινδυνότητας σύμφωνα με 5 κριτήρια που κλιμακώνονται ανάλογα με τη σημασία τους. Τα κριτήρια περιλαμβάνουν: προσέγγιση με αγαθά (ανάλυση επικινδυνότητας που πραγματοποιείται σε μοναδικό αγαθό ή σε ομάδα αγαθών), το επίπεδο της προετοιμασίας που χρειάζεται πριν από την εφαρμογή της μεθόδου, το είδος του προσωπικού που εμπλέκεται (υπάλληλοι του οργανισμού ή εξωτερικοί εμπειρογνώμονες), τους μαθηματικούς τύπους που χρησιμοποιούνται για τον υπολογισμό των κινδύνων καθώς και τα σχετικά και απόλυτα αποτελέσματα της αξιολόγησης.

Σε μία διαφορετική προσέγγιση, οι Niekerk και Labuschagne (2006) συγκρίνουν μεθόδους επικινδυνότητας σύμφωνα με τα στάδια στα οποία υλοποιούνται. Την ίδια χρονιά, η πολιτική αξιολόγησης που προτείνει ο DANIDA (2006) περιλαμβάνει τα ακόλουθα βασικά χαρακτηριστικά:

1. Χρησιμότητα: οι πληροφορίες που παράγονται από τη διαδικασία αξιολόγησης πρέπει να βελτιώσουν το θέμα υπό σχεδίαση καθώς και τις μελλοντικές του εξελίξεις.
2. Αντικειμενικότητα και αξιοπιστία: τα αποτελέσματα της αξιολόγησης πρέπει να είναι επαληθεύσιμα και αμερόληπτα και πρέπει να παρουσιάζουν τα πλεονεκτήματα και τις αδυναμίες με ισορροπημένο τρόπο. Η αξιολόγηση πραγματοποιείται από έναν εταίρο που δεν συμμετέχει στην υλοποίηση της δραστηριότητας, προκειμένου να αποφευχθεί η σύγκρουση συμφερόντων και η συνολική αντικειμενικότητα.
3. Ακρίβεια: όλες οι σχετικές πτυχές πρέπει να καλύπτονται και τα δεδομένα πρέπει να είναι όσο το δυνατόν ακριβέστερα.
4. Διαφάνεια: σκεπτικό αξιολόγησης, πόροι, διαδικασίες και κριτήρια πρέπει να παρουσιάζονται με σαφήνεια και να εξηγούνται.

5. Σκοπιμότητα: όλοι οι πόροι που απαιτούνται πρέπει να είναι διαθέσιμοι και όλες οι διαδικασίες και οι μέθοδοι πρέπει να είναι εφικτές.

Ο οργανισμός ENISA (2006) έχει αναπτύξει ένα «Αρχείο καταγραφής της εκτίμησης επικινδυνότητας και των μεθόδων διαχείρισης της επικινδυνότητας». Κατά την καταγραφή αυτή ακολουθήθηκε η παρακάτω προσέγγιση: αναγνώριση των διαφόρων σταδίων της αξιολόγησης και διαχείρισης της επικινδυνότητας, αναφορά σε οδηγίες της Ευρωπαϊκής Ένωσης και στους ορισμούς ISO, δημιουργία καταλόγου προϊόντων (μέθοδοι και πρότυπα) που σχετίζονται με τη μελέτη επικινδυνότητας και καθορισμός συγκεκριμένων ιδιοτήτων των «προϊόντων», έτσι ώστε να διευκολυνθεί τυχόν σύγκριση. Τα κριτήρια που έχουν ορίσει είναι: γενικές πληροφορίες που συνθέτουν την «ταυτότητα» της μεθόδου ή του εργαλείου (π.χ. κύκλος ζωής, τιμή, υποστηριζόμενες γλώσσες κ.ά.), έκταση πεδίου (άδειες, πιστοποιήσεις, καταλληλότητα για οργανισμούς κ.ά.) και η γνώμη των χρηστών (δεξιότητες, υποστήριξη, ωριμότητα μεθόδου κ.ά.) (ENISA, 2006).

Οι Syalim et al. (2009) κατηγοριοποιούν τις μεθόδους ανάλογα με τα βήματα που ακολουθούν κατά την ανάλυση επικινδυνότητας, με το περιεχόμενο της μεθόδου και την αντίστοιχη τεκμηρίωση που τη συνοδεύει.

Για την αξιολόγηση των μεθόδων και των εργαλείων ανάλυσης επικινδυνότητας, οι Sajko et al. (2010) έχουν αναπτύξει ένα μοντέλο κριτηρίων που χρησιμοποιεί Analytic Hierarchy Process (AHP). Πιο συγκεκριμένα, κριτήριο αποτελεί η υποστήριξη των διαδικασιών της μεθόδου είτε είναι μεθοδική (παροχή μετρικών, αντικειμενικότητα, ακρίβεια, ευελιξία, ακεραιότητα) είτε μέσω του λογισμικού (διεπαφή χρήστη, καταλληλότητα εξοπλισμού κ.ά.). Άλλα κριτήρια είναι οι απαιτούμενοι πόροι (πληροφορίες, άνθρωποι, χρήματα, χρόνος) και τα κίνητρα και οι στόχοι της μεθόδου.

Όταν στη διαδικασία ανάλυσης επικινδυνότητας εμπλέκονται και προσωπικά δεδομένα, τότε απαιτούνται περαιτέρω κριτήρια αξιολόγησης. Στη συγκεκριμένη περίπτωση, οι μέθοδοι πρέπει να λαμβάνουν υπόψη τους και κινδύνους που σχετίζονται με τη συλλογή, χρήση, προστασία και γνωστοποίηση των προσωπικών πληροφοριών. Ο Borking (2010) για λογαριασμό του Center for Democracy & Technology διατύπωσε ένα σύνολο κριτηρίων για την προστασία των προσωπικών δεδομένων για τη διαχείριση ταυτότητας στην ψηφιακή εποχή. Τα κριτήρια αυτά

επίσης μπορούν να χρησιμοποιηθούν για την αξιολόγηση και τη σύγκριση μεθόδων. Μερικά από τα κριτήρια αυτά είναι: η ανωνυμία, η διαφάνεια, η ποιότητα των δεδομένων, η αναλογικότητα, η χρήση των πληροφοριών ανάλογα με το σκοπό, τα δικαιώματα του υποκειμένου των δεδομένων, η λογοδοσία κ.ά. (Abie & Borking 2012).

Το 2011, ο Smojver προτείνει μία μέθοδο σύμφωνα με την Analytic Hierarchy Process (AHP) και με τα κριτήρια που πρότεινε ο ENISA (2006), η οποία περιλαμβάνει 5 βασικά κριτήρια που αναλύονται σε 17 περαιτέρω υπο-κριτήρια. Τα βασικά κριτήρια είναι: *πεδίο της έρευνας* (method scope), *ευκολία χρήσης*, *ωριμότητα της μεθόδου*, *στόχος της μεθόδου* (target audience). Η ανάλυση στα 17 κριτήρια είναι ιδιαίτερα εκτενής και βοηθάει στη δημιουργία ολοκληρωμένου πλαισίου αξιολόγησης και στην καταγραφή των χαρακτηριστικών κάθε μεθόδου. Το μοντέλο επιτρέπει διαφανή και αντικειμενική σύγκριση των διαφόρων μεθόδων και ο συγγραφέας καταλήγει στο συμπέρασμα ότι το μοντέλο επιτρέπει την επιλογή της βέλτιστης μεθόδου που ταιριάζει περισσότερο με τις ανάγκες του συγκεκριμένου οργανισμού που αξιολογείται.

Σε έρευνα που πραγματοποιήθηκε το 2014 από την Eskisabel σχετικά με τις μεθόδους μελέτης επικινδυνότητας και την εφαρμογή τους σε νοσοκομεία, ιδιαίτερη βαρύτητα δόθηκε στις τεχνικές ιδιαιτερότητες και ανάγκες του οργανισμού υπό εξέταση. Παρόλο που βασίστηκε στη μέθοδο των Vorster και Labuschagne (2005), παρουσιάζει διαφοροποίηση λόγω του προσανατολισμού της στο επιχειρησιακό περιβάλλον και του πρωταρχικού ρόλου που εκείνο διαδραματίζει κατά την επιλογή της βέλτιστης μεθόδου. Γίνεται, επομένως, σαφές ότι η καταλληλότητα της μεθόδου είναι άμεσα συνδεδεμένη με τις απαιτήσεις του οργανισμού και η σύγκριση πρέπει να λαμβάνει υπόψη και αυτόν τον παράγοντα.

7.3 Ομαδοποίηση κριτηρίων αξιολόγησης μεθόδων επικινδυνότητας

Από τη βιβλιογραφική ανασκόπηση παρατηρούμε ότι δεν υπάρχουν αυστηρώς καθορισμένα κριτήρια για την αξιολόγηση της καταλληλότητας των μεθόδων επικινδυνότητας. Επίσης κάποιοι ερευνητές αναφέρονται με διαφορετικό όνομα σε κριτήρια που έχουν ίδια ερμηνεία. Στη συνέχεια περιγράφονται τα κριτήρια και ο

ορισμός τους, ενώ εμφανίζονται οι ονομασίες και οι μορφές με τις οποίες εντοπίστηκαν σε διαφορετικές έρευνες.

7.3.1 Λογική ορθότητα

Η μέθοδος πρέπει να βασίζεται σε αναγνωρισμένα στατιστικά μοντέλα (π.χ. μέθοδος Bayes) προκειμένου να εξασφαλίζεται η αντικειμενικότητα και να υπάρχει επαρκής πολυπλοκότητα. Επίσης τα στάδια που ακολουθεί η μέθοδος και ο τρόπος ανάλυσης πρέπει να πληρούν τα πρότυπα και να μπορούν να επαναληφθούν χωρίς να αυξάνεται η πολυπλοκότητα της μεθόδου . Πιο συγκεκριμένα, για την κάλυψη της επαναληψιμότητας, η αλληλουχία των βημάτων μπορεί να επαναληφθεί αρχής γενομένης από οποιοδήποτε από τα ενδιάμεσα προϊόντα για τη βελτίωση του συνολικού και του τελικού αποτελέσματος. Τα κριτήρια τα οποία ομαδοποιούνται υπό το γενικό όρο «Λογική Ορθότητα» είναι τα παρακάτω:

Λογική ορθότητα (Merkhofer, 1985), Τρόπος ανάλυσης (Fischhoff et al., 1981; Vorster και Labuschagne, 2005; Niekerk και Labuschagne, 2006, Katzke, 1988; Campell και Stamp, 2004), Επαναληψιμότητα (Browne, 1989), Κύκλος ζωής και διαδικασίες (Olle et al., 1988; Craft et al., 1998; Syalim et al., 2009; ENISA, 2006), Συνοχή (Garrabrant et al., 1990), Πολυπλοκότητα (Lichtenstein, 1996; Vorster και Labuschagne, 2005).

7.3.2 Εγκυρότητα

Η εγκυρότητα περιλαμβάνει την πληρότητα και την ακρίβεια. Πιο συγκεκριμένα, πληρότητα είναι η παροχή ολοκληρωμένης κάλυψης όλων των εκτιμήσεων της διαχείρισης κινδύνου. Η ιδιότητα της ακρίβειας εξασφαλίζει ότι όλες οι σχετικές πτυχές που αξιολογούνται και εκτιμώνται πρέπει να καλύπτονται και τα δεδομένα πρέπει να είναι όσο το δυνατόν πιο κοντά στην πραγματικότητα. Τα κριτήρια τα οποία ομαδοποιούνται υπό το γενικό όρο «Εγκυρότητα» είναι τα παρακάτω:

Εγκυρότητα (Lichtenstein, 1996), Πληρότητα (Merkhofer, 1985; Garrabrant et al., 1990; Lichtenstein, 1996), Ακρίβεια (Merkhofer, 1985; Browne, 1989; Danida 2006;

Sajko et al., 2010), Ακεραιότητα (Sajko et al., 2010), Βάθος και εύρος ανάλυσης (Browne, 1989).

7.3.3 Αποδοχή

Η αποδοχή των χρηστών συνίσταται στη συμμετοχή κατά τη διαδικασία της ανάλυσης επικινδυνότητας αλλά και στην κατανόηση των προβλημάτων ασφάλειας και των επιπτώσεων που μπορεί να έχουν. Επίσης απαιτείται να είναι ώριμη η μέθοδος. Σύμφωνα με τους Paulk, Curtis et al. (1993) ώριμη μπορεί να χαρακτηρισθεί μία μέθοδος που είναι: επαναλήψιμη (repeatable), καθορισμένη (defined), διαχειριζόμενη (managed) και βελτιστοποιούμενη (optimising). Η ιδιότητα της ωριμότητας της μεθόδου περιλαμβάνει την εξάπλωση της χρήσης της μεθόδου (π.χ. πόσο καιρό υπάρχει η μέθοδος, πόσο συχνά ενημερώνεται και τη γεωγραφική εξάπλωση της χρήσης), ευθυγράμμιση με τα πρότυπα που σχετίζονται με την ασφάλεια των πληροφοριών (π.χ. ISO 27001, ISO 15408, ISO 17799 ISO 13335, ISO 21827, NIST SP 800-30) και τη δυνατότητα πιστοποίησης των οργανισμών και του προσωπικού τους. Τα κριτήρια τα οποία ομαδοποιούνται υπό το γενικό όρο «Αποδοχή» είναι τα παρακάτω:

Αποδοχή (Merkhofer, 1985; Lichtenstein, 1996), Αναγνωρισμότητα (Browne, 1989), Ωριμότητα (Kitchenham et al., 1997; ENISA, 2006; Smoijver, 2011), Ευθυγράμμιση με πιστοποιήσεις και πρότυπα (ENISA, 2006).

7.3.4 Πόροι

Οι πόροι περιλαμβάνουν πόσο σημαντικές είναι οι δαπάνες που σχετίζονται με τη μέθοδο. Πιο συγκεκριμένα, περιλαμβάνονται δαπάνες που αφορούν την προετοιμασία για την εφαρμογή της μεθόδου, καθαυτή την εφαρμογή της (implementation costs), καθώς και δαπάνες που σχετίζονται με την απόδοσή της (performance costs). Επίσης πόροι θεωρούνται οι άνθρωποι που ασχολούνται με τη μελέτη επικινδυνότητας είτε από την πλευρά του οργανισμού, είτε από την πλευρά των αναλυτών. Οι οικονομικές δαπάνες αλλά και ο χρόνος που απαιτούνται, αποτελούν επίσης σημαντικούς πόρους. Τέλος, οι πληροφορίες που αξιολογούνται βάσει των μεθόδων αλλά και η ποιότητα των δεδομένων αποτελούν σημαντικές εισροές στη διαδικασία της μελέτης, επομένως

κατηγοριοποιούνται ως πόροι (Das & Teng, 1998). Τα κριτήρια τα οποία ομαδοποιούνται υπό το γενικό όρο «Πόροι» είναι τα παρακάτω:

Πόροι (Olle et al., 1988), Κόστος (Browne, 1989; Lichtenstein, 1996; ENISA, 2006), Άνθρωποι (Olle et al., 1988; Vorster και Labuschagne, 2005; Sajko et al., 2010), Χρήματα (Sajko et al., 2010), Χρόνος (Sajko et al., 2010), Πληροφορία και ποιότητα δεδομένων (Vorster και Labuschagne, 2005; Sajko et al., 2010; Borking, 2010).

7.3.5 Χρησιμότητα

Σύμφωνα με το κριτήριο αυτό, αξιολογείται η χρησιμότητα της μεθόδου, δηλαδή οι εφαρμογές που έχει και οι συνέπειές της. Πιο συγκεκριμένα, σύμφωνα με τη χρηστικότητα, οι πληροφορίες που παράγονται από τη διαδικασία αξιολόγησης πρέπει να βελτιώσουν το θέμα υπό σχεδίαση καθώς και τις μελλοντικές του εξελίξεις. Παράλληλα, η μέθοδος πρέπει να έχει πρακτική εφαρμογή και να μη μένει σε θεωρητικό πλαίσιο. Γίνεται, επίσης, σαφές ότι η καταλληλότητα της μεθόδου είναι άμεσα συνδεδεμένη με τις απαιτήσεις του οργανισμού και η σύγκριση πρέπει να λαμβάνει υπόψη και αυτόν τον παράγοντα. Η έννοια του οργανισμού-στόχου αναφέρεται στο γεγονός ότι οι μέθοδοι μπορεί να περιέχουν υψηλού επιπέδου γενικές κατευθυντήριες γραμμές για τη διαδικασία διαχείρισης του κινδύνου (δηλαδή πληροφορίες σε επίπεδο διαχείρισης), επιχειρησιακές κατευθυντήριες γραμμές σχετικά με το πώς να εφαρμοστεί και να εκτελεστεί η διαδικασία διαχείρισης του κινδύνου (δηλαδή πληροφορίες σε επιχειρησιακό επίπεδο) ή / και πολύ λεπτομερείς τεχνικές κατευθυντήριες γραμμές ανάλογα με τη φύση (μέγεθος, κουλτούρα κ.ά.) και την κρισιμότητα του οργανισμού (Karolak και Karolak,, 1995). Τα κριτήρια τα οποία ομαδοποιούνται υπό το γενικό όρο «Χρησιμότητα» είναι τα παρακάτω:

Χρησιμότητα (Danida, 2006), Χρηστικότητα (Garrabrant et al., 1990), Πρακτικότητα (Merkhofer, 1985), Συνέπειες και επιδράσεις (Kitchenham et al., 1997; Craft et al., 1998), Κίνητρα και στόχοι (Sajko et al., 2010; Borking, 2010), Εξεταζόμενος οργανισμός (Lichtenstein, 1996; Kitchenham et al., 1997; Craft et al., 1998; Smojver, 2011; Eskisabel, 2014), Σκοπιμότητα (Olle et al., 1988; Garrabrant et al., 1990; Danida, 2006).

7.3.6 Αξιοπιστία

Τα αποτελέσματα της αξιολόγησης πρέπει να είναι επαληθεύσιμα και αμερόληπτα και πρέπει να παρουσιάζουν τα πλεονεκτήματα και τις αδυναμίες με ισορροπημένο τρόπο. Η αξιολόγηση πραγματοποιείται από αναλυτές που δεν συμμετέχουν στην υλοποίηση της δραστηριότητας, προκειμένου να αποφευχθεί η σύγκρουση συμφερόντων και να επιτευχθεί συνολική αντικειμενικότητα. Παράλληλα, μέσω της αναλογικότητας, πρέπει να εξασφαλίζεται ότι η χρήση των πληροφοριών γίνεται ανάλογα με το σκοπό και τα δικαιώματα του υποκειμένου των δεδομένων. Τα κριτήρια τα οποία ομαδοποιούνται υπό το γενικό όρο «Χρησιμότητα» είναι τα παρακάτω:

Αξιοπιστία (Garraibrants et al., 1990; Lichtenstein, 1996; Danida, 2006), Επικύρωση αποτελέσματος (Olle et al., 1988), Αντικειμενικότητα (Danida, 2006; Sajko et al., 2010), Αναλογικότητα (Borking, 2010), Λογοδοσία (Borking, 2010).

7.3.7 Ευκολία Χρήσης

Η ευκολία χρήσης αναλύεται στα εξής χαρακτηριστικά: ευκολία εκμάθησης (learnability), ευκολία κατανόησης (understandability) και ευκολία λειτουργίας του (operability) (ISO/IEC 9126). Επίσης περιλαμβάνεται το επίπεδο των δεξιοτήτων που απαιτούνται για την εφαρμογή, τη χρήση και τη συντήρηση της μεθόδου, το πόσο ευέλικτη είναι και αν προσαρμόζεται στις αλλαγές και επικαιροποιείται συχνά (updates). Σημαντική θεωρείται και η υποστήριξη από κατάλληλο εργαλείο λογισμικού που ακολουθεί την αντίστοιχη μέθοδο. Σύμφωνα με τη διαφάνεια που πρέπει να διέπει τις μεθόδους μελέτης επικινδυνότητας, το σκεπτικό αξιολόγησης, οι πόροι και οι διαδικασίες πρέπει να παρουσιάζονται με σαφήνεια και να εξηγούνται. Τα κριτήρια τα οποία ομαδοποιούνται υπό το γενικό όρο «Ευκολία Χρήσης» είναι τα παρακάτω:

Ευκολία χρήσης (Lichtenstein, 1996; Smoijver, 2011), Προσαρμοστικότητα (Garraibrants et al., 1990), Υποστήριξη από λογισμικό (Lichtenstein, 1996; ENISA 2006; Sajko et al., 2010), Εκμάθηση (Kitchenham et al., 1997), Τεκμηρίωση (Syalim et al., 2009), Ευελιξία (Lichtenstein, 1996; Sajko et al., 2010), Διαφάνεια (Danida, 2006; Borking, 2010).

7.4 Συνοπτικός πίνακας κριτηρίων

Στη συνέχεια παρουσιάζονται συνοπτικά τα παραπάνω κριτήρια και οι έρευνες στις οποίες εντοπίστηκαν. Πιο συγκεκριμένα, στον οριζόντιο άξονα απεικονίζονται οι έρευνες, ενώ στον κάθετο έχουμε τα κριτήρια. Όταν ένα από τα κριτήρια εμφανίζεται στην έρευνα απεικονίζεται με ένα «X».

	Κριτήριο						
	Λογική ορθότητα	Εγκυρότητα	Αποδοχή	Πόροι	Χρησιμότητα	Αξιοποιεία	Ευκολία χρήσης
Έρευνα	Borking			X	X	X	X
	Browne	X	X	X			
	Campell	X					
	Craft	X			X		
	Danida		X		X	X	X
	ENISA	X		X			X
	Eskisabel				X		
	Fischhoff	X					
	Garrabrant	X	X		X	X	X
	Katzke	X					
	Kitchenham			X	X		X
	Lichtenstein	X	X	X	X	X	X
	Merkhofer	X	X	X	X		
	Niekerk	X					
	Olle	X			X	X	X
	Sajko		X		X	X	X
	Smajver			X	X		X
	Syalim	X					X
	Vorster	X		X			

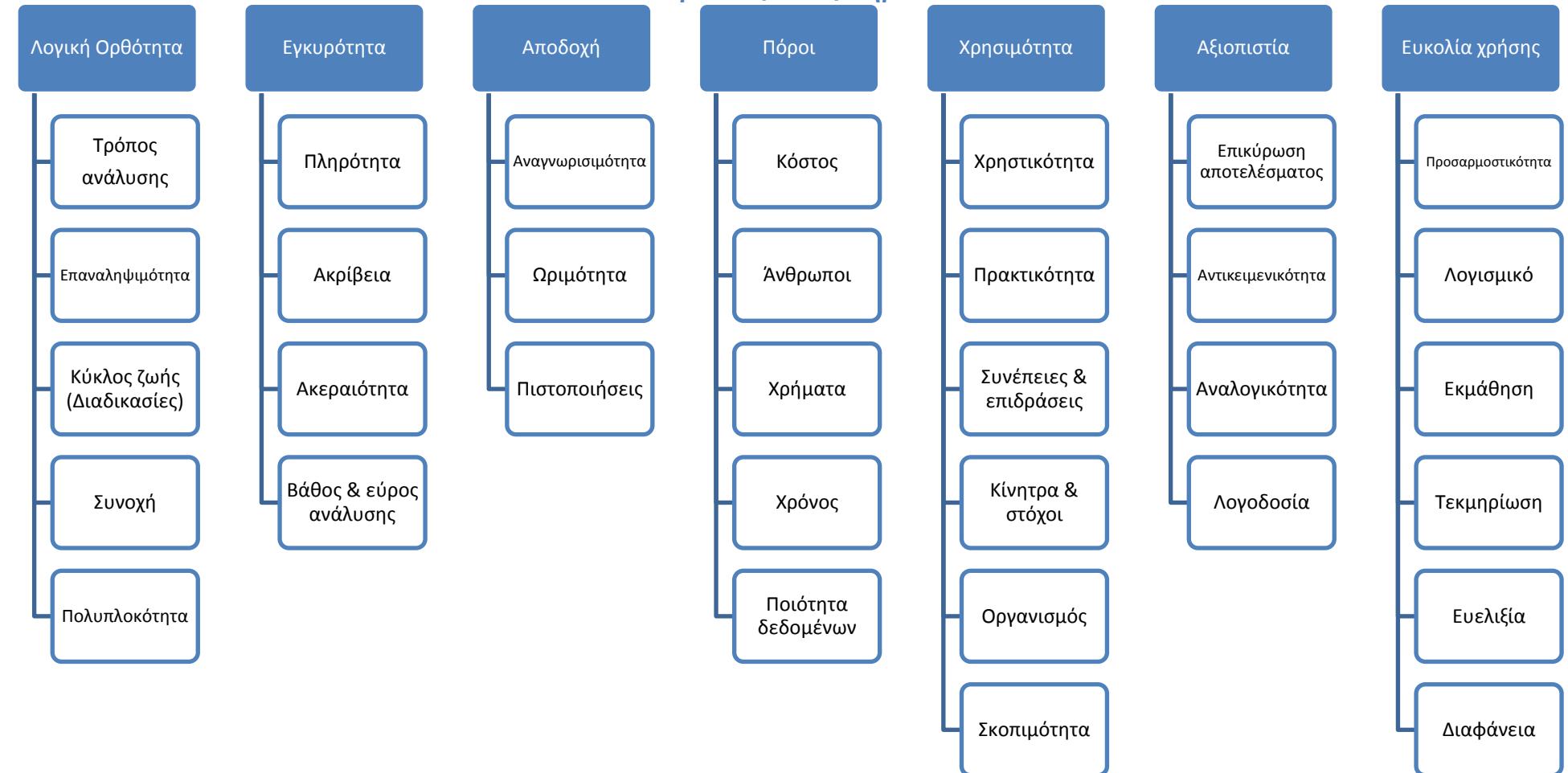
Πίνακας 16: Εμφάνιση κριτηρίων σε έρευνες

7.5 Προτεινόμενα κριτήρια

Στην ενότητα αυτή παρουσιάζονται συγκεντρωτικά τα κριτήρια που προέκυψαν από την έρευνα και την ομαδοποίηση. Στο επίπεδο 1 έχουμε το γενικό κριτήριο, ενώ στο επίπεδο 2 έχουμε τα υποκριτήρια που περιλαμβάνονται σε αυτό.

Κριτήρια επιλογής μεθόδου ανάλυσης επικινδυνότητας

Εικόνα 36: Προτεινόμενα κριτήρια



7.6 Επιλογή μεθόδου βάσει AHP (Advanced Hierachal Process)

Η μέθοδος της αναλυτικής ιεράρχησης (AHP) έχει χρησιμοποιηθεί σε ένα μεγάλο εύρος προβλημάτων όπως (Subramanian, & Ramanathan, 2012):

- Επιλογή μεταξύ εναλλακτικών λύσεων σε περιβάλλοντα με πολλαπλούς στόχους.
- Κατανομή πόρων σε ανεπάρκεια (scarce resources).
- Προβλέψεις.

Αν και το εύρος της μεθόδου είναι αρκετά μεγάλο, η θεμελίωση της αναλυτικής ιεράρχησης πάνω σε αξιώματα, ουσιαστικά οριοθετεί και περιορίζει το περιβάλλον του προβλήματος προς επίλυση, καθιστώντας έτσι πιο εύκολη και αντικειμενική την επιλογή της καταλληλότερης λύσης. Η μέθοδος βασίζεται στην πολύ καλά ορισμένη μαθηματική δομή των συνεπών πινάκων (consistent matrices) και την ικανότητα των χαρακτηριστικών διανυσμάτων τους (eigenvectors) να παράγουν αληθείς ή με πολύ καλή προσέγγιση σχετικές βαρύτητες.

Η κύρια χρήση της μεθόδου της αναλυτικής ιεράρχησης είναι η επίλυση προβλημάτων επιλογής μέσα σε ένα πολυκριτηριακό περιβάλλον. Υπό αυτήν την έννοια, η μεθοδολογία εμπεριέχει συγκρίσεις μεταξύ των κριτηρίων και των εναλλακτικών επιλογών με ένα τρόπο που επιτρέπει τις ανά ζεύγη συγκρίσεις (pair wise comparisons). Η μέθοδος μετατρέπει τις προσωπικές προτιμήσεις και κρίσεις σε βαρύτητες βαθμονομημένης κλίμακας, οι οποίες στη συνέχεια μετατρέπονται σε αθροιστικές γραμμικές βαρύτητες για τις συσχετιζόμενες εναλλακτικές επιλογές. Αυτές οι προκύπτουσες βαρύτητες χρησιμοποιούνται για να κατατάξουν τις διάφορες εναλλακτικές επιλογές και έτσι υποβοηθούν το σύστημα λήψης αποφάσεων στο να πάρει τη σωστή απόφαση ή να προβλέψει με μεγαλύτερη ακρίβεια κάποιο αποτέλεσμα (Sipahi & Timor, 2010).

7.6.1 Αρχές και αξιώματα της AHP

Η μέθοδος AHP εμπεριέχει τρεις βασικές αρχές (Saaty, 1977). Αυτές είναι:

1. Αποδόμηση (Decomposition).
2. Συγκριτικές κρίσεις (Comparative Judgments).

3. Ιεραρχική αποδόμηση ή σύνθεση προτεραιοτήτων (Hierarchic Composition or Synthesis of Priorities).

Η αρχή της αποδόμησης επιτρέπει σε ένα σύνθετο πρόβλημα να δομηθεί σε μια ιεραρχία κατηγοριών, υποκατηγοριών κ.λπ. Η αρχή των συγκριτικών κρίσεων επιτρέπει την πραγματοποίηση συγκρίσεων ανά ζεύγη όλων των δυνατών συνδυασμών των στοιχείων μιας ομάδας ή υποομάδας σε σχέση με το στοιχείο ή την ομάδα του αμέσως προηγουμένου επιπέδου. Αυτές οι συγκρίσεις ανά ζεύγη χρησιμοποιούνται για να εξαχθούν οι «τοπικές» βαρύτητες των στοιχείων της ομάδας σε σχέση με το ανώτερο επίπεδο της ιεραρχίας. Η αρχή της ιεραρχικής αποδόμησης ή σύνθεσης, επιτρέπει τον πολλαπλασιασμό των «τοπικών» προτεραιοτήτων των στοιχείων μιας ομάδας με την ολική (global) βαρύτητα του ανωτέρου επιπέδου, παράγοντας έτσι ολικές βαρύτητες σε ολόκληρη την ιεραρχία.

Όσον αφορά στα αξιώματα πάνω στα οποία η AHP στηρίζεται, αυτά είναι τα εξής σύμφωνα με τους Forman and Gass (1999):

1. Αξίωμα της αμοιβαιότητας (reciprocal axiom).
2. Αξίωμα της ομοιογένειας (homogeneity axiom).
3. Αξίωμα της σύνθεσης (synthesis axiom).

Το αξίωμα της αμοιβαιότητας υπονοεί ότι αν $P_c(A,B)$ είναι μία σύγκριση ανά ζεύγη των στοιχείων A και B σε σχέση με το στοιχείο C του ανωτέρου επιπέδου, παριστάνοντας το πόσες φορές περισσότερο το στοιχείο A κατέχει μια ιδιότητα σε σχέση με το στοιχείο B, τότε θα πρέπει να ισχύει ότι $P_c(B,A) = 1 / P_c(A,B)$. Για παράδειγμα, αν το A είναι πέντε φορές μεγαλύτερο από το B, τότε το B είναι το ένα πέμπτο του μεγέθους του A.

Κατά το αξίωμα της ομοιογένειας, τα στοιχεία τα οποία συγκρίνονται δεν θα πρέπει να διαφέρουν κατά πολύ όσον αφορά στις ιδιότητες στις οποίες γίνεται η σύγκριση. Αν κάτι τέτοιο δεν εφαρμόζεται, τότε τα λάθη στις κρίσεις μπορεί να είναι πολύ μεγάλα. Όταν δομείται επομένως μια ιεραρχία, θα πρέπει να δίνεται ιδιαίτερη προσοχή κατά την ταξινόμηση των στοιχείων ώστε αυτά να μην διαφέρουν πολύ όταν βρίσκονται μαζί μέσα σε μια ομάδα.

Το αξίωμα της σύνθεσης αναφέρει ότι οι βαρύτητες των στοιχείων σε μια ιεραρχία δεν εξαρτώνται από στοιχεία κατωτέρων επιπέδων. Αυτό το αξίωμα είναι απαραίτητο για να μπορέσει να εφαρμοστεί η αρχή της ιεραρχικής σύνθεσης. Το τρίτο αξίωμα

της σύνθεσης πάντως, απαιτεί προσεκτική εξέταση καθότι είναι σύνηθες να παραβιάζεται. Σε προβλήματα επιλογής είναι δυνατόν η επιλογή των εναλλακτικών να εξαρτάται από στοιχεία υψηλότερου επιπέδου, ενώ ταυτόχρονα η σημαντικότητα των στοιχείων αυτών να εξαρτάται ταυτόχρονα από τις εναλλακτικές. Όταν υπάρχει τέτοιου είδους εξάρτηση, το αξίωμα της σύνθεσης δεν είναι εφαρμόσιμο.

7.6.2 Μετρήσεις και Αναλογικές Κλίμακες στην AHP

Η AHP παρέχει έναν απλό και προηγμένο τρόπο μέτρησης αντικειμενικών αλλά και υποκειμενικών παραγόντων. Αυτό επιτυγχάνεται μέσω της διεξαγωγής συγκρίσεων ανά ζεύγη, οι οποίες παράγουν αδιάστατες αναλογικές προτεραιότητες. Ο λήπτης της απόφασης ερωτάται για να καταθέσει τις εκτιμήσεις του σχετικά με τη σχετική σημαντικότητα, προτίμηση, ή πιθανότητα (ανάλογα με το αν αξιολογούνται αντίστοιχα κριτήρια, εναλλακτικές ή σενάρια). Οι εκτιμήσεις αυτές μπορούν να γίνουν αριθμητικά, γραφικά ή λεκτικά. Πέραν του πλεονεκτήματος της παραγωγής αδιάστατων αναλογικών προτεραιοτήτων σε περιπτώσεις όπου δεν υπάρχει κλίμακα, οι σχετικές εκτιμήσεις τείνουν να είναι πιο ακριβείς από τις απόλυτες εκτιμήσεις (Saaty, 1977).

7.6.3 Αναλογικές κλίμακες, αριθμητικές και γραφικές συγκρίσεις ανά ζεύγη

Η μέθοδος AHP έχει προκαλέσει πλήθος ερωτήσεων σχετικά με το αν όντως παράγει προτεραιότητες τα μέτρα των οποίων είναι αναλογικά. Μια διαστηματική κλίμακα (interval scale) ορίζεται ως η κλίμακα η οποία ακολουθεί την εξίσωση της μορφής $y=ax+b$, ενώ η αναλογική κλίμακα ακολουθεί τη μορφή της εξίσωσης $y=ax$. Λόγω του ότι δεν υπάρχει το μέρος b στην εξίσωση, λέγεται ότι η αναλογική κλίμακα έχει ένα «καθαρό» μηδέν (Forman and Gass, 1999). Η αμφισβήτηση σχετικά με την αναλογικότητα έγκειται στο ότι δεν υπάρχει πουθενά το μηδέν, ούτε στις συγκρίσεις μεταξύ των στοιχείων των επιπέδων ούτε και στις τελικές προτεραιότητες που προκύπτουν. Αυτό όμως συμβαίνει λόγω του ότι οι συγκρίσεις είναι σχετικές και όχι απόλυτες και αυτός είναι ο μόνος τρόπος για την ύπαρξη αντικειμενικών συγκρίσεων.

Για να γίνει περισσότερο κατανοητή η έννοια της αναλογικής κλίμακας εξετάζεται το εξής παράδειγμα. Έστω ότι ζητείται να βρεθεί το σχετικό βάρος του αντικειμένου i σε σχέση με το αντικείμενο j . Τα δύο αυτά αντικείμενα είτε θα έχουν το ίδιο βάρος

(δηλαδή ο λόγος των βαρών τους θα είναι 1) είτε το αντικείμενο i θα είναι x φορές πιο βαρύ από το αντικείμενο j. Αντιστρόφως το αντικείμενο j θα είναι 1/x φορές πιο βαρύ από το αντικείμενο i. Σε αυτό το σημείο ορίζεται ως a_{ij} το αποτέλεσμα αυτής της σύγκρισης.

Για N τέτοια αντικείμενα, ο παρατηρητής θα εξήγαγε παρόμοια αποτελέσματα από τις συγκρίσεις και έτσι θα προέκυπτε ένας πίνακας ζευγωτών συγκρίσεων $A = (a_{ij})$, στον οποίο θα ισχύει ότι $a_{ii} = 1$ και $a_{ij} = 1/a_{ji}$. Εδώ θα πρέπει να σημειωθεί ότι αρκεί να συμπληρωθούν μόνο τα $N(N-1)/2$ στοιχεία του πίνακα που βρίσκονται πάνω από τη διαγώνιο, λόγω της συμμετρικής ιδιότητας του πίνακα. Για τον πίνακα A, η AHP χρησιμοποιεί το κανονικοποιημένο χαρακτηριστικό διάνυσμα (eigenvector) (Saaty, 1977). Λόγω του ότι ήδη κάθε μία σύγκριση ανά ζεύγη αποτελεί μια αναλογία, οι προκύπτουσες προτεραιότητες θα είναι επίσης αναλογικές. Ο Forman (1993) διενήργησε πειράματα τα οποία απέδειξαν ότι οι προκύπτουσες αναλογικές βαρύτητες είναι πιο ακριβείς από ότι οι μεμονωμένες συγκρίσεις.

Αριθμητικές και γραφικές διαδικασίες μπορούν να χρησιμοποιηθούν για να εξαχθούν κρίσεις κατά τη σύγκριση δύο στοιχείων. Έτσι μπορούν να εξαχθούν κρίσεις π.χ. για το σχετικό μέγεθος γεωμετρικών σχημάτων, τη σχετική φωτεινότητα αντικειμένων, τη σχετική σημαντικότητα στόχων, ή τη σχετική προτίμηση εναλλακτικών σε σχέση με κάποιο δεδομένο στόχο. Ενώ οι κρίσεις αυτές είναι υποκειμενικές, τα αποτελέσματα που θα προέκυψαν από συγκρίσεις μεγεθών, μπορούν να θεωρηθούν ως αντικειμενικά λόγω των ιδιοτήτων που συγκρίνονται. Όμως δεν υπάρχουν αντικειμενικά μέτρα για την σύγκριση της σημαντικότητας δύο στόχων ή της προτίμησης δύο εναλλακτικών. Παρόλα αυτά, είναι απαραίτητη η ύπαρξη αναλογικών μέτρων που να μετρούν αντικειμενικά τη σημαντικότητα και τις προτιμήσεις κατά τη λήψη αποφάσεων και την κατανομή πόρων. Η μέθοδος AHP είναι σε θέση να παράγει τέτοιου είδους μέτρα.

7.6.4 Φραστικές συγκρίσεις ανά ζεύγη

Η θεμελιώδης κλίμακα συγκρίσεων που αρχικά προτάθηκε από τον Saaty (1977) για τη μέθοδο AHP αποτελούνταν από τις λέξεις «ίσο», «ασθενές», «δυνατό», «πολύ δυνατό» και «απόλυτο» (η λέξη «ασθενές» αντικαταστάθηκε αργότερα από τη λέξη «μέτριο» και η λέξη «απόλυτο» από τη λέξη «ακραίο»). Βασισμένος σε εμπειρική

έρευνα, ο Saaty πρότεινε την αντιστοίχηση αυτών των λέξεων με τους αριθμούς 1,3,5,7,9 αντίστοιχα. Οι ενδιάμεσοι ακέραιοι 2,4,6,8, χρησιμοποιούνταν για να δηλώσουν ενδιάμεσες καταστάσεις.

Έτσι, για παράδειγμα, το 6 βρίσκεται κάπου μεταξύ του «δυνατό» και «πολύ δυνατό». Η αντιστοίχηση αυτή παρουσιάζεται στην Εικόνα 37. Σε αντίθεση με τις αριθμητικές και γραφικές διαδικασίες, οι φραστικές συγκρίσεις δεν αποτελούν διαστηματικά (interval) ή αναλογικά (ratio) μέτρα, αλλά μόνο βαθμωτά (ordinal) μέτρα. Η θεμελιώδης αυτή φραστική κλίμακα είναι βαθμωτή λόγω του ότι τα διαστήματα που υπάρχουν μεταξύ των φράσεων δεν είναι απαραίτητα ίσα. Αυτό για παράδειγμα σημαίνει ότι η απόσταση από το «δυνατό» στο «πολύ δυνατό» να είναι πολύ μικρότερη απ' ότι η απόσταση από το «πολύ δυνατό» στο «ακραίο».

Ένταση της Σχετικής Σημασίας	Ορισμός	Ερμηνεία
1	Ίση βαρύτητα	Δυο συνεισφέρουν εξίσου στον στόχο.
3	Μέτρια βαρύτητα του ενός στοιχείου ως προς ένα άλλο	Η εμπειρία και η κρίση ευνοούν ελαφρώς μια δραστηριότητα έναντι της άλλης.
5	Σημαντική βαρύτητα του ενός στοιχείου ως προς ένα άλλο	Η εμπειρία και η κρίση ευνοούν σημαντικά μια δραστηριότητα έναντι της άλλης
7	Εκδηλωμένη βαρύτητα	Μια δραστηριότητα ευνοείται ισχυρά και η κυριαρχία της εκδηλώνεται στην πράξη.
9	Μέγιστη βαρύτητα	Οι λόγοι που ευνοούν τη μια δραστηριότητα έναντι της άλλης είναι τους υψηλότερου δυνατού βαθμού επιβεβαίωσης.
2, 4, 6, 8	Ενδιάμεσες τιμές ανάμεσα σε δύο παρακείμενες κρίσεις	Όταν απαιτείται συμβιβασμός.
Αντίστροφοι των παραπάνω μη-μηδενικών αριθμών	Αν σε μια δραστηριότητα αντιστοιχίζεται ένας από τους παραπάνω αριθμούς, όταν αυτή συγκρίνεται με μια δεύτερη δραστηριότητα, τότε η δεύτερη έχει την αντίστροφη τιμή όταν συγκρίνεται με την πρώτη.	
Ρητοί αριθμοί	Αναλογίες που προκύπτουν από την κλίμακα	Αν επιβαλλόταν η συνέπεια λαμβάνοντας η αριθμητικές τιμές για το σχηματισμό του πίνακα.

Εικόνα 37: Θεμελιώδης κλίμακα συγκρίσεων

Παρά το γεγονός όμως ότι αυτή η βαθμωτή κλίμακα που χρησιμοποιείται για την εξαγωγή των κρίσεων αποτελεί ένα βαθμωτό μέτρο, η εμπειρική έρευνα του Saaty (1977) έδειξε ότι το κύριο χαρακτηριστικό διάνυσμα που προκύπτει από ένα πίνακα φραστικών συγκρίσεων συχνά δίνει προτεραιότητες που προσεγγίζουν τις

πραγματικές προτεραιότητες που παράγονται από αναλογικές συγκρίσεις μετρήσιμων στοιχείων. Αυτό συμβαίνει διότι όπως οι Wind & Saaty (1980), απέδειξαν μαθηματικά, ο υπολογισμός του χαρακτηριστικού διανύσματος έχει μια εξομαλυντική επίδραση. Έτσι, αν υπάρχει αρκετή ποικιλία και πλεονάζοντα στοιχεία στην ιεραρχία, τα λάθη κατά την κρίση, όπως αυτά που υπεισέρχονται όταν χρησιμοποιείται η βαθμωτή κλίμακα, μειώνονται δραστικά.

Επιπλέον μπορεί να δειχθεί ότι για ένα πίνακα ζευγωτών συγκρίσεων $A = (a_{ij})$, αν είναι συνεπής (consistent), που σημαίνει ότι $a_{ij} = a_{ik}a_{kj}$, τότε οι συνιστώσες του χαρακτηριστικού διανύσματος δίνουν τις πραγματικές και αληθινές προτεραιότητες των στοιχείων που συγκρίνονται (Mirkin, 1979; Saaty, 1986). Αν πάλι δεν υπάρχει συνέπεια στον πίνακα ζευγωτών συγκρίσεων, η ανάλυση των λαθών δείχνει ότι το χαρακτηριστικό διάνυσμα δίνει βαρύτητες οι οποίες εξακολουθούν να είναι κοντά στις πραγματικές τιμές με αποδεκτή ακρίβεια, υπό την προϋπόθεση βέβαια ότι ο λήπτης των αποφάσεων δεν διενεργεί τυχαίες συγκρίσεις (Saaty, 1986).

7.6.5 Στάθμιση κριτηρίων/ εναλλακτικών επιλογών

Η μέθοδος AHP διαθέτει τρεις τεχνικές εξαγωγής συμπερασμάτων όσον αφορά στον καθορισμό της σχετικής σημαντικότητας μεταξύ διαφόρων κριτηρίων ή εναλλακτικών επιλογών, τη λεκτική, την αριθμητική και την γραφική. Οι συγκρίσεις γίνονται πάντα ανά ζεύγη. Για παράδειγμα, κατά τη σύγκριση δύο κριτηρίων όπως το κόστος και η επίδοση, κατά τη λεκτική τεχνική, ένα πιθανό αποτέλεσμα μιας τέτοιας σύγκρισης θα μπορούσε να εκφραστεί με το ότι «η επίδοση είναι αρκετά πιο σημαντική από το κόστος». Κατά την αριθμητική τεχνική όμως θα μπορούσε αυτή η σύγκριση να απαντηθεί με το ότι «η επίδοση είναι 2,5 φορές πιο σημαντική από το κόστος».

7.6.6 Αξιολόγηση κριτηρίων με AHP (παράδειγμα)

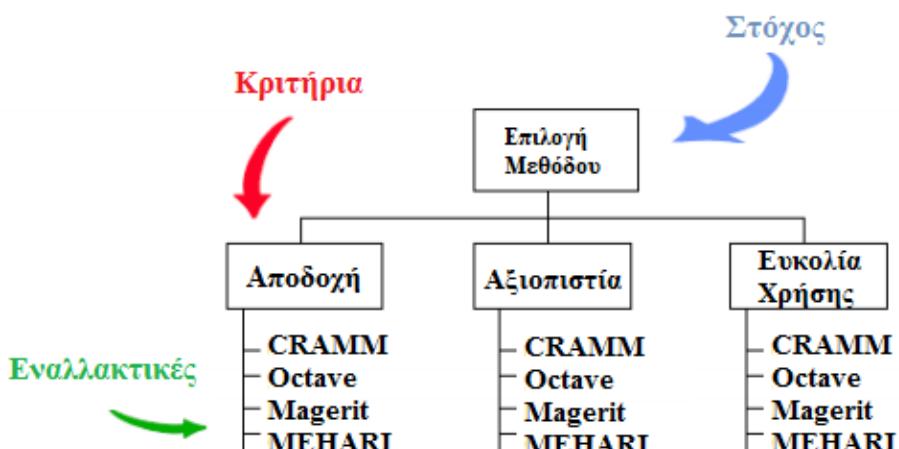
Για την καλύτερη κατανόηση της μεθόδου της AHP θα επιχειρηθεί η ανάπτυξη ενός παραδείγματος μαζί με τα στάδια που εμπεριέχονται μέχρι την τελική απόφαση. Τα εξής τρία ερωτήματα που θα πρέπει να απαντηθούν είναι:

1. Ποιος είναι ο αντικειμενικός στόχος (objective).

2. Ποια είναι τα κριτήρια της απόφασης (criteria).
3. Ποιες είναι οι διαθέσιμες εναλλακτικές επιλογές (alternatives).

Το παράδειγμα θα δομηθεί πάνω στην υπόθεση ότι ο λήπτης της απόφασης επιθυμεί να αποφασίσει ποια μέθοδο επικινδυνότητας θα πρέπει να διαλέξει. Ορίζεται έτσι με αυτόν τον τρόπο ο αντικειμενικός στόχος, ο οποίος είναι η επιλογή μεθόδου επικινδυνότητας. Στη συνέχεια ορίζονται τα κριτήρια πάνω στα οποία θα βασιστεί αυτή η απόφαση. Ο λήπτης της απόφασης, παραδείγματος χάρη, να χρησιμοποιήσει τρία κριτήρια: την αποδοχή, την αξιοπιστία και την ευκολία χρήσης. Πρέπει να τονιστεί ότι η επιλογή των κριτηρίων έγκειται αποκλειστικά στην υποκειμενική αντίληψη του λήπτη της απόφασης σχετικά με το ποια κριτήρια θεωρεί ως πλέον σημαντικά. Τέλος, γίνεται η υπόθεση ότι οι διαθέσιμες εναλλακτικές επιλογές μεθόδων ανάλυσης επικινδυνότητας είναι: CRAMM, Octave, Magerit, Mehari.

Έχοντας απαντήσει λοιπόν στα τρία αυτά ερωτήματα, χτίζεται αυτομάτως η ιεραρχία της απόφασης η οποία απεικονίζεται διαγραμματικά στην Εικόνα 38.



Εικόνα 38: Ιεραρχία απόφασης

Στο επόμενο βήμα θα πρέπει να γίνει η κατηγοριοποίηση των κριτηρίων με βάση την σπουδαιότητά τους. Εκφράζονται λοιπόν κάποιες κρίσεις σχετικά με την σχετική σημαντικότητα των κριτηρίων μεταξύ τους και οι συγκρίσεις αυτές γίνονται ανά ζεύγη (pair wise comparisons). Έτσι, υποθέτουμε στο παράδειγμα ότι:

- Η αξιοπιστία είναι δύο (2) φορές πιο σημαντική από την αποδοχή.
- Η αποδοχή είναι τρεις (3) φορές πιο σημαντική από την ευκολία χρήσης.
- Η αξιοπιστία είναι τέσσερις (4) φορές πιο σημαντική από την ευκολία χρήσης.

Με βάση την αναλογική κλίμακα του Saaty (1977), η οποία έχει εύρος από το 1 έως το 9 είναι εφικτό να έχουμε τον πρώτο πίνακα των κριτηρίων. Ο πίνακας αυτός είναι συμμετρικός και η διαγώνιος του αποτελείται από μονάδες.

	Αποδοχή	Αξιοπιστία	Ευκολία Χρήσης
Αποδοχή	1/1	1/2	3/1
Αξιοπιστία	2/1	1/1	4/1
Ευκολία Χρήσης	1/3	1/4	1/1

Μετατρέπουμε τα κλάσματα σε δεκαδικούς αριθμούς και ο πίνακας αποκτά την ακόλουθη μορφή:

$$\begin{bmatrix} 1,000 & 0,500 & 3,000 \\ 2,000 & 1,000 & 4,000 \\ 0,333 & 0,250 & 1,000 \end{bmatrix}$$

Στο πρώτο βήμα θα πρέπει να υπολογιστούν οι σχετικές προτεραιότητες των κριτηρίων. Το ζητούμενο είναι ο υπολογισμός του χαρακτηριστικού διανύσματος (eigenvector) το οποίο θα δώσει την κατάταξη αυτών των κριτηρίων. Οι υπολογισμοί που θα ακολουθήσουν απαιτούν στοιχειώδεις γνώσεις άλγεβρας πινάκων. Έτσι, συνεχίζοντας με την ανάπτυξη του παραδείγματος εκτελούμε τετραγωνισμό του πίνακα των συγκρίσεων.

$$\begin{bmatrix} 1,000 & 0,500 & 3,000 \\ 2,000 & 1,000 & 4,000 \\ 0,333 & 0,250 & 1,000 \end{bmatrix} * \begin{bmatrix} 1,000 & 0,500 & 3,000 \\ 2,000 & 1,000 & 4,000 \\ 0,333 & 0,250 & 1,000 \end{bmatrix} = \begin{bmatrix} 3,000 & 1,750 & 8,000 \\ 5,333 & 3,000 & 14,000 \\ 1,166 & 0,666 & 3,000 \end{bmatrix}$$

Στη συνέχεια προσθέτουμε τις σειρές των πινάκων και αθροίζουμε τα σύνολα των σειρών.

$$\begin{bmatrix} 3,000 + & 1,750 + & 8,000 \\ 5,333 + & 3,000 + & 14,000 \\ 1,166 + & 0,666 + & 3,000 \end{bmatrix} = \begin{bmatrix} 12,750 \\ 22,333 \\ 4,833 \end{bmatrix}$$

Το σύνολο των αθροισμάτων των σειρών προκύπτει ίσο με 39,916.

Με βάση αυτό το σύνολο κανονικοποιούνται τα αθροίσματα των σειρών και έτσι προκύπτει το χαρακτηριστικό διάνυσμα. Έτσι, το διάνυσμα προκύπτει από τις διαιρέσεις:

$$12,750/39,916=0,3194$$

$$22.333/39,916=0,5595$$

$$4,833/39,916=0,1211$$

Και είναι το εξής:

$$\begin{bmatrix} 0,3194 \\ 0,5595 \\ 0,1211 \end{bmatrix}$$

Η διαδικασία αυτή θα πρέπει να επαναληφθεί έως ότου το προκύπτον χαρακτηριστικό διάνυσμα δεν αλλάζει. Για την καλύτερη κατανόηση θα επιχειρηθεί ακόμα μία επανάληψη της διαδικασίας. Έτσι, τετραγωνίζοντας τον πίνακα του προηγούμενου βήματος έχουμε τα εξής:

$$\begin{bmatrix} 3,000 & 1,750 & 8,000 \\ 5,333 & 3,000 & 14,000 \\ 1,166 & 0,666 & 3,000 \end{bmatrix} * \begin{bmatrix} 3,000 & 1,750 & 8,000 \\ 5,333 & 3,000 & 14,000 \\ 1,166 & 0,666 & 3,000 \end{bmatrix} = \begin{bmatrix} 27,6653 & 15,8330 & 72,4984 \\ 48,3311 & 27,6662 & 126,6642 \\ 10,5547 & 6,0414 & 27,6653 \end{bmatrix}$$

Αθροίζοντας τις σειρές του πίνακα και στη συνέχεια παίρνοντας το σύνολο που προκύπτει, κανονικοποιούμε τα αθροίσματα και προκύπτει το νέο χαρακτηριστικό διάνυσμα της μορφής:

$$\begin{bmatrix} 0,3196 \\ 0,5584 \\ 0,1220 \end{bmatrix}$$

Η διαφορά του νέου διανύσματος από το προηγούμενο είναι πολύ μικρή, επομένως κρατάμε το χαρακτηριστικό διάνυσμα που έχει προκύψει, το οποίο απεικονίζει τη σχετική κατάταξη των κριτηρίων ως εξής.

Αποδοχή	$0,3196$
Αξιοπιστία	$0,5584$
Ευκολία	$0,1220$
Χρήσης	

Το διάνυσμα αυτό καταδεικνύει ότι η αξιοπιστία είναι το πιο σημαντικό κριτήριο και δίνει επίσης και τις σχετικές αποστάσεις μεταξύ των κριτηρίων.

Στη συνέχεια χρειάζεται η συλλογή των κρίσεων σε σχέση με κάθε κριτήριο ξεχωριστά και σύμφωνα με τις διαθέσιμες εναλλακτικές επιλογές. Έτσι, αφού γίνουν οι απαραίτητες συγκρίσεις ανά ζεύγη, προκύπτουν τρεις συμμετρικοί πίνακες συγκρίσεων για κάθε ένα από τα τρία κριτήρια.

Οι συγκρίσεις ανά ζεύγη θα παρασταθούν ενδεικτικά για το κριτήριο: *Αποδοχή*.

	Cramm	Octave	Magerit	Mehari
Cramm	$1/1$	$1/4$	$4/1$	$1/6$
Octave	$4/1$	$1/1$	$4/1$	$1/4$
Magerit	$1/4$	$1/4$	$1/1$	$1/5$
Mehari	$6/1$	$4/1$	$5/1$	$1/1$

Εφαρμόζοντας ακριβώς την ίδια μεθοδολογία είναι δυνατόν να εξαχθούν τα χαρακτηριστικά διανύσματα για το κριτήριο αυτό. Οι τιμές που προκύπτουν μετά την κανονικοποίηση είναι:

Cramm	$0,1160$
Octave	$0,2470$
Magerit	$0,0600$
Mehari	$0,5770$

Η κανονικοποίηση δίνει και την σχετική κατάταξη των μεθόδων με βάση το κριτήριο της αποδοχής.

8. Σύγκριση CRAMM και MAGERIT

Για την αξιολόγηση μεθόδων και εργαλείων που σχετίζονται με την ανάλυση επικινδυνότητας δεν υπάρχουν σαφώς ορισμένα κριτήρια. Για τη συγκεκριμένη εργασία επιλέχθηκαν τα κριτήρια που εφαρμόζονται από τον Lichtenstein (1996).

8.1 Χαρακτηριστικά Μεθόδου

Κάθε μέθοδος παρουσιάζει ιδιαίτερα χαρακτηριστικά βάσει των οποίων μπορεί να προκύψει αξιολόγηση και να συγκριθεί με αντίστοιχες μεθόδους.

8.1.1 Κόστος

8.1.1.1 Κόστος αγοράς και εφαρμογής

Για το εργαλείο CRAMM που υλοποιεί την αντίστοιχη μέθοδο υπάρχουν δύο διαθέσιμες εκδόσεις: η «Express» (κόστος: 1.850 ευρώ συν 300 ευρώ για ετήσια άδεια) και η «Expert» (κόστος: 3.600 ευρώ συν 1.100 ευρώ για ετήσια άδεια). Για το εργαλείο CRAMM Expert η εταιρεία συνιστά τριήμερο πρόγραμμα εκμάθησης (κόστος: 1.450 ευρώ).

Το εργαλείο PILAR που υλοποιεί τη μέθοδο MAGERIT προσφέρεται σε τέσσερις εκδόσεις: Η πλήρης έκδοση με κόστος 1500 ευρώ, το microPilar που έχει κόστος 250 ευρώ και κάθε πρόσθετο προφίλ αξιολόγησης 150 ευρώ και τέλος η έκδοση basic με κόστος 500 ευρώ. Οι τελευταίες δύο εκδόσεις προσφέρουν μόνο ποιοτική ανάλυση. Η τέταρτη έκδοση που προσφέρεται παρέχει δυνατότητες προσαρμογής και εξατομίκευσης του εργαλείου στις εκάστοτε ανάγκες του οργανισμού και κοστίζει 3.000 ευρώ. Παράλληλα, υπάρχει πακέτο αγοράς της βάσης δεδομένων και υποστήριξης του Pilar με κόστος 500 ευρώ και πρόγραμμα εκμάθησης με κόστος 4.000 ευρώ.

8.1.1.2 Χρόνος συλλογής δεδομένων

Και στις δύο μεθόδους παρουσιάζεται εκτενής χρήση ερωτηματολογίων και συνεντεύξεων με κρίσιμες ομάδες ενδιαφέροντος. Στην περίπτωση του εργαλείου CRAMM οι ερωτήσεις είναι προκαθορισμένες με αποτέλεσμα να μειώνεται ο χρόνος

προετοιμασίας για τη διεξαγωγή της μελέτης. Στην περίπτωση του εργαλείου PILAR παρέχεται η επιλογή δημιουργίας ερωτηματολογίου από τον αναλυτή (Crespo et al., 2006), γεγονός που συντελεί στην καλύτερη προσαρμογή της ανάλυσης στις απαιτήσεις του αξιολογούμενου οργανισμού, αλλά αυξάνει το χρόνο προετοιμασίας. Παράλληλα, ελλοχεύει ο κίνδυνος να μην έχει εξετασθεί κάποια παράμετρος λόγω παράλεψης του αναλυτή, με αποτέλεσμα να απαιτείται στη συνέχεια περαιτέρω συλλογή δεδομένων.

8.1.1.3 Χρόνος εκτίμησης επικινδυνότητας

Ο χρόνος εκτίμησης επικινδυνότητας κυμαίνεται ανάλογα με πολλές παραμέτρους, όπως το μέγεθος του οργανισμού και το πλήθος των διαστάσεων που πρέπει να εξετασθούν. Ωστόσο, η ανάλυση επικινδυνότητας σε ένα μεγάλο οργανισμό (τελικό στάδιο προσδιορισμού αντιμέτρων) μπορεί να διαρκέσει αρκετές ώρες για το εργαλείο CRAMM. Για το εργαλείο PILAR δε βρέθηκε εκτιμώμενος χρόνος παρουσίασης των αποτελεσμάτων.

8.1.2 Απαίτηση για συμφωνία διοίκησης και αναλυτών

Λόγω της αυξημένης συμμετοχής των χρηστών των πληροφοριακών συστημάτων στη συλλογή δεδομένων για τη διαχείριση επικινδυνότητας, είναι απαραίτητη η αδιάλειπτη υποστήριξη και συμπαράσταση της διοίκησης. Και στις δύο μεθόδους προτείνεται σε κάθε στάδιο η συνάντηση με τη διοίκηση του αξιολογούμενου οργανισμού ώστε να υπάρχει ενημέρωση για την πορεία της μελέτης, να επιβεβαιώνονται τα δεδομένα και να επιλύονται τυχόν απορίες των αναλυτών. Ωστόσο, υπάρχουν περιπτώσεις όπου οι στόχοι του οργανισμού δεν είναι εναρμονισμένοι με τους στόχους της ασφάλειας των πληροφοριακών συστημάτων. Για το λόγο αυτό, απαιτούνται αυξημένες επικοινωνιακές ικανότητες από την πλευρά των αναλυτών, καθώς και διερευνητική ματιά ώστε να εξασφαλίζεται η ακρίβεια και εγκυρότητα των στοιχείων (Yazar, 2002).

8.1.3 Ευελιξία

8.1.3.1 Προσαρμογή ως προς τον οργανισμό και το πληροφοριακό σύστημα

Η μέθοδος CRAMM δεν προσφέρει πολλές δυνατότητες προσαρμογής. Συγκεκριμένα, κάθε τροποποίηση προκύπτει μετά από πλήρη ανανέωση της βάσης, η οποία δεν είναι συχνή. Σημαντικό κρίνεται και το ότι το εργαλείο CRAMM δεν υποστηρίζει πληροφοριακά συστήματα με διασύνδεση στο υπολογιστικό νέφος, με αποτέλεσμα να απαιτείται περαιτέρω μελέτη από πλευράς του αναλυτή και χρήση κάποιου άλλου εργαλείου. Η δυνατότητα τροποποίησης που παρέχει το εργαλείο PILAR το καθιστά πιο ευέλικτο και παραμετροποιήσιμο ώστε να εναρμονιστεί με τις συνθήκες και τις ανάγκες του εκάστοτε οργανισμού (Crespo et al., 2006). Επίσης σημαντική είναι η ύπαρξη διαφορετικών εκδόσεων για κάθε εργαλείο με σκοπό να χρησιμοποιηθεί το κατάλληλο ανάλογα με τον οργανισμό και το αξιολογούμενο πληροφοριακό σύστημα. Και οι δύο μέθοδοι προσφέρουν ικανότητα κάλυψης όλων των φάσεων του κύκλου ζωής της ασφάλειας των πληροφοριακών συστημάτων (π.χ. σχεδιασμός, ανάπτυξη-υλοποίηση και αναβάθμιση). Η CRAMM θεωρείται καταλληλότερη για συστήματα που έχουν εγκατασταθεί και λειτουργούν σε στατικές θέσεις από ότι για φορητά συστήματα.

8.1.3.2 Κάλυψη μελλοντικών αλλαγών

Παρά την ευρεία εφαρμογή της μεθόδου CRAMM και την επιστημονική της αναγνώριση, παρατηρείται μια βραδυπορία στην ενσωμάτωση των νέων τεχνολογικών απαιτήσεων. Αυτό δικαιολογείται σε κάποιο βαθμό από το γεγονός ότι η μέθοδος CRAMM συμβαδίζει με μεγάλο βαθμό με πρότυπα και χρησιμοποιείται εκτεταμένα για χορήγηση πιστοποιήσεων. Είναι σύνηθες να υπάρχει καθυστέρηση στην προτυποποίηση νέων προϊόντων και υπηρεσιών, επομένως δεν προβλέπεται επίσημη διαδικασία ώστε να ενσωματωθεί στο εργαλείο CRAMM. Αντιθέτως, το εργαλείο PILAR ανανεώνεται διαρκώς, παρέχοντας νέες δυνατότητες στους αναλυτές.

Η τελευταία έκδοση του εργαλείου CRAMM είναι η 5.2 (2003) και της MAGERIT είναι η έκδοση 3 (2009) με την πρώτη επίσημη έκδοση (έκδοση 1.2). Σε αντίθεση με το CRAMM το εργαλείο Pilar διακρίνεται από πολύ συχνές ενημερώσεις. Μέχρι την ημερομηνία συγγραφής του παρόντος κειμένου, η τελευταία έκδοση είναι η 5.4

(Ιανουάριος 2014) (European Union Agency for Network and Information Security, 2014).

8.1.3.3 Επιλογή συνδυασμού αντιμέτρων

Τόσο το εργαλείο CRAMM όσο και το PILAR παρέχουν λειτουργικές και όχι τεχνικές προδιαγραφές. Σε περίπτωση αντικρουόμενων αντιμέτρων (δηλαδή αντιμέτρων που εξυπηρετούν διαφορετικές ανάγκες) δεν προβλέπεται εσωτερικός μηχανισμός που να τα αποκλείει. Είναι ευθύνη του αναλυτή να επιλέξει ποιο θα προταθεί τελικά, λαμβάνοντας υπόψη το χειρότερο σενάριο για τη μέθοδο CRAMM, αλλά και τις εξαρτήσεις των αγαθών για τη μέθοδο MAGERIT (Mellado et al., 2006).

8.1.4 Πολυπλοκότητα, Εγκυρότητα, Αξιοπιστία

Οι περισσότερες μέθοδοι ανάλυσης κινδύνου βασίζονται σε στατιστικά μοντέλα και κυρίως στη μέθοδο Bayes. Την ίδια προσέγγιση ακολουθούν και οι μέθοδοι CRAMM και MAGERIT. Η εγκυρότητα της εφαρμογής της στατιστικής θεωρίας για τον υπολογισμό της πιθανότητας εμφάνισης μιας απειλής έχει αμφισβητηθεί από πολλούς ερευνητές, αλλά εξακολουθεί να είναι η πιο διαδεδομένη. Για τη μέθοδο CRAMM δεν παρέχεται ο αλγόριθμος ανάλυσης της επικινδυνότητας, γεγονός που θεωρείται μειονέκτημα της μεθόδου. Αντίθετα, το εργαλείο PILAR παρέχει αλγορίθμική ανάλυση για την ποιοτική και την ποσοτική μέθοδο που εφαρμόζεται στα εκάστοτε στάδια διευκολύνοντας την κατανόηση του εργαλείου (Xenakis & Wolthusen, 2011). Η μέθοδος CRAMM θεωρείται από πολλές χώρες ως η μόνη επίσημη μέθοδος για την ανάλυση επικινδυνότητας, προσδίδοντάς της μεγαλύτερη εγκυρότητα και αξιοπιστία στον επιστημονική κοντότητα.

Η μέθοδος CRAMM είναι ποιοτική, ενώ η μέθοδος MAGERIT χρησιμοποιεί τόσο την ποιοτική όσο και την ποσοτική προσέγγιση. Οι ποιοτικές προσεγγίσεις δυσκολεύουν την οικονομική ανάλυση, κάνοντας δύσκολη τη δικαιολόγηση των επενδύσεων που αφορούν τα μέτρα ελέγχου (European Union Agency for Network and Information Security, 2014). Τόσο το εργαλείο PILAR ακολουθεί την προσέγγιση που ακολουθήθηκε με το εργαλείο CRAMM, δηλαδή βρίσκονται υπό την άμεση εποπτεία δημόσιων οργανισμών ώστε να παρέχουν επαρκή προστασία κατά το νόμο

και την επιστήμη και να διασφαλίζουν όσο το δυνατό την αμεροληψία τους απέναντι σε τεχνικά προϊόντα και λύσεις.

8.1.5 Πληρότητα

Η πληρότητα εξετάζεται ως προς τις τεχνολογικές παραμέτρους του πληροφοριακού συστήματος, τις απαιτήσεις ασφάλειας και τις παραμέτρους επικινδυνότητας. Όλες οι παραπάνω πτυχές αλλάζουν άρδην λόγω των ταχύτατων τεχνολογικών εξελίξεων. Επομένως απαιτούνται εργαλεία που θα προσαρμόζονται γρήγορα στις επιταγές της σύγχρονης εποχής. Όπως προαναφέρθηκε, ένα από τα μειονεκτήματα του εργαλείου CRAMM είναι οι μη συχνές ανανεώσεις της βάσης. Επομένως υπάρχουν δεδομένες χρονικές περίοδοι που το εργαλείο CRAMM χρειάζεται την υποστήριξη και άλλων εργαλείων προκειμένου να καλύψει τις ανάγκες των αναλυτών (π.χ. υπολογιστικό νέφος, έξυπνα κινητά τηλέφωνα κ.λπ.). Το εργαλείο PILAR δείχνει πως προσαρμόζεται ευκολότερα, ίσως και λόγω της έκδοσης που παρέχει αυξημένη παραμετροποίηση στους αναλυτές και μπορούν να συμπεριλάβουν περισσότερες πτυχές προς εξέταση, εξασφαλίζοντας πιο αυξημένη πληρότητα.

8.1.6 Συνέπεια

Τόσο το εργαλείο CRAMM όσο και το PILAR υλοποιούν επιστημονικά καταξιωμένες μεθόδους στο χώρο της διαχείρισης κινδύνου. Η ευρεία διάδοση των μεθόδων αποτελεί ισχυρή απόδειξη της συνέπειας που τις χαρακτηρίζει (Xenakis & Wolthusen, 2011). Επομένως, για παρόμοια συστήματα με παρόμοια χαρακτηριστικά κινδύνου έχουν προταθεί παρόμοιες λύσεις ασφαλείας και έκτακτης ανάγκης.

8.1.7 Ευκολία χρήσης

Σχετικά με τα εργαλεία που τις υλοποιούν, το εργαλείο CRAMM χαρακτηρίζεται από τους περισσότερους ερευνητές ως ιδιαίτερα δύσχρηστο με μη φιλική διεπαφή προς το χρήστη. Η ενσωμάτωση πλαισίων ελέγχου και επιλογής ήταν ορθή, αλλά δεν άλλαξε σε μεγάλο βαθμό την εμπειρία των χρηστών. Η εκμάθηση που συνιστάται από την εταιρεία που διαθέτει το εργαλείο, υποδεικνύει και τις δυσκολίες που έγκεινται στη χρήση και την πλήρη αξιοποίηση των δυνατοτήτων του. Το εργαλείο PILAR κρίνεται

πιο εύκολο στη χρήση του και υπάρχει η επιλογή επιπέδου χρήστη με την εμφάνιση επιλογών που αντιστοιχούν στην εμπειρία του (Crespo et al., 2006)

Και τα δύο εργαλεία παράγουν εκτενείς αναφορές και προσφέρουν τη δυνατότητα εποπτικής παρουσίασης με χρήση πινάκων και γραφημάτων. Το εργαλείο CRAMM παρέχει τη δυνατότητα εμφάνισης της έκθεσης επικινδυνότητας αλλά επί πληρωμή, ενώ το εργαλείο PILAR δε χρεώνει την απλή εμφάνιση. Το εργαλείο CRAMM μπορεί να κάνει εξαγωγή σε αρχείο τύπου ASCII ή RichText, ενώ το PILAR σε XML, RTF, HTML και CSV. Ειδικότερα η παρουσίαση σε XML είναι πολύ σημαντική, καθώς διευκολύνει την αναζήτηση των στοιχείων όχι μόνο μέσω του διαδικτύου αλλά και του σημασιολογικού ιστού και βοηθά στη διασύνδεση με άλλα εργαλεία που υποστηρίζουν την XML (European Union Agency for Network and Information Security, 2014).

8.1.8 Αρχή κόστους-ωφέλειας

Η παραγωγή ολοκληρωμένης τεκμηρίωσης για τα αντίμετρα που προτείνονται είναι καθοριστικής σημασίας για τον οργανισμό. Αποτελεί εργαλείο επικοινωνίας ανάμεσα στους ειδικούς των πληροφοριακών συστημάτων και τη διοίκηση των οργανισμών, καθώς επιτρέπει την έκφραση του προβλήματος της ασφάλειας σε γλώσσα κατανοητή από τη διοίκηση, αντιμετωπίζοντας την ασφάλεια ως «επένδυση» που αποτιμάται με όρους κόστους/οφέλους. Και στις δύο μεθόδους υπάρχει σαφής αιτιολόγηση για τις δαπάνες που θα χρειαστούν για την εφαρμογή των προτεινόμενων αντιμέτρων και χρήση εποπτικών μέσων για την καλύτερη κατανόηση από τη διοίκηση των οργανισμών. Ωστόσο, η άνλη φύση του κινδύνου περιορίζει την παραδοσιακή τεχνική ανάλυσης κόστους – ωφέλειας (Yazar, 2002).

8.1.9 Υποστήριξη από το κυττάλληλο λογισμικό

Τόσο η μέθοδος CRAMM όσο και η μέθοδος MAGERIT συνοδεύονται από τα εργαλεία CRAMM και PILAR αντίστοιχα, που τις υλοποιούν και τις επεκτείνουν. Για καθένα εργαλείο έχει προβλεφθεί αντίστοιχη εκπαίδευση των χρηστών με κόστος που προαναφέρθηκε.

8.2 Χαρακτηριστικά οργανισμού

8.2.1 Επίπεδο επικινδυνότητας

Το επίπεδο επικινδυνότητας ενός οργανισμού καθορίζει σε μεγάλο βαθμό ποια μέθοδος θα χρησιμοποιηθεί. Για οργανισμούς που χαρακτηρίζονται ως κρίσιμες υποδομές ή για οργανισμούς που θέλουν να κατέχουν πιστοποίηση ασφαλείας, τότε προτιμάται η μέθοδος που είναι αναγνωρισμένη στην εκάστοτε χώρα. Για την Ελλάδα η μόνη επιστημονική μέθοδος που αναγνωρίζεται είναι η CRAMM. Ωστόσο, στο εξωτερικό όλο και περισσότεροι οργανισμοί επιλέγουν τη μέθοδο MAGERIT και το εργαλείο PILAR λόγω της δυνατότητας να ανταποκριθεί στις συνθήκες και στις ανάγκες του εκάστοτε οργανισμού με μεγαλύτερη ευελιξία (Crespo et al., 2006).

8.2.2 Μέγεθος

Το μέγεθος ενός οργανισμού μπορεί να αποτελέσει ισχυρό κριτήριο επιλογής τόσο της μεθόδου όσο και της έκδοσής της. Λόγω των καταβολών της μεθόδου CRAMM (μελέτη επικινδυνότητας στον ιατρικό τομέα του Ηνωμένου Βασιλείου) (United Kingdom Central Computer and Telecommunication Agency, 2009) και της πολυπλοκότητας εφαρμογής της προτιμάται κυρίως σε μεγάλους οργανισμούς. Για το εργαλείο PILAR προτείνονται διαφορετικές εκδόσεις αναλόγως του μεγέθους του οργανισμού. Για οργανισμούς μικρού μεγέθους προτείνονται οι εκδόσεις microPILAR και PILAR basic, ενώ για μεγαλύτερους οργανισμούς καλύτερη επιλογή είναι οι εκδόσεις PILAR ή RMAT (Manas, 2009).

8.2.3 Κουλτούρα ασφάλειας

Τόσο η μέθοδος CRAMM όσο και η μέθοδος MAGERIT προωθούν τη συμμετοχή των εργαζομένων και την ευαισθητοποίηση σε θέματα ασφάλειας. Ωστόσο, η μέθοδος CRAMM επικεντρώνεται στη δημιουργία κλίματος δέσμευσης και επίγνωσης σε θέματα ασφάλειας. Επιπρόσθετα η μέθοδος MAGERIT κάνει ειδική μνεία στη δημιουργία κουλτούρας ασφάλειας μέσα στην εταιρεία (Crespo et al., 2006), αποδεικνύοντας ότι θεωρεί την υιοθέτηση των μέτρων ασφαλείας όχι μόνο τεχνική υπόθεση αλλά και οργανωσιακή. Σε περίπτωση που ο οργανισμός δεν έχει

αναπτυγμένη κουλτούρα ασφάλειας και αντιμετωπίζει τη μελέτη επικινδυνότητας επιφυλακτικά και με κρυψίνοια, είναι βέβαιο ότι ανεξαρτήτως μεθόδου θα χρειαστεί πολύς χρόνος και κόπος από την πλευρά των αναλυτών. Και στις δύο μεθόδους η καθοδήγηση για τη δημιουργία πολιτικών και διαδικασιών ασφαλείας είναι κρίσιμης σημασίας (European Union Agency for Network and Information Security, 2014).

8.2.4 Εξωτερικές απαιτήσεις

Η μέθοδος CRAMM είναι η κύρια μέθοδος πιστοποίησης για τα πρότυπα ISO 27000, ενώ επικεντρώνεται στα ISO 27001:2005 και ISO 27001:2009 (United Kingdom Central Computer and Telecommunication Agency, 2009). Η MAGERIT καλύπτει περισσότερα πρότυπα όπως ISO 13335:2004, ISO 15408:2005, ISO 17799:2005 και ISO 27001:2005 (Crespo et al., 2006).

Ωστόσο, με την ανανέωση του ISO 27001:2013 απαιτείται η συμμόρφωση των εργαλείων και των μεθόδων τόσο με την ορολογία όσο και με τις αλλαγές που επέφερε. Η μέθοδος CRAMM έχει δημιουργηθεί στο Ηνωμένο Βασίλειο και η MAGERIT στην Ισπανία, επομένως καθεμιά υπακούει στους αντίστοιχους θεσπισμένους νόμους του κράτους. Για την εφαρμογή τους σε κάποια άλλη χώρα απαιτείται εναρμόνιση με το αντίστοιχο νομικό πλαίσιο. Η μέθοδος CRAMM καλύπτει τις απαιτήσεις της ευρωπαϊκής και της ελληνικής νομοθεσίας, που απαιτούν από τα πληροφοριακά συστήματα που επεξεργάζονται προσωπικά δεδομένα, τη λήψη μέτρων προστασίας (Δημοσχάκης, 2010). Με τον τρόπο αυτό, «εξασφαλίζεται επίπεδο ασφάλειας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων (Νόμος 2472/1997).

8.3 Διαδικασίες μεθόδων

Τόσο η μέθοδος CRAMM όσο και η MAGERIT ακολουθούν παρόμοια στάδια ανάλυσης επικινδυνότητας τα οποία είναι (Davenport, 2013):

- Γενικές πληροφορίες περιβάλλοντος.
- Μοντελοποίηση του συστήματος.
- Αναγνώριση αγαθών.
- Αξιολόγηση αγαθών.

- Ανάλυση απειλών.
- Ανάλυση κινδύνου.
- Επιλογή αντίμετρων.

8.3.1 Οριθέτηση πλαισίου ανάλυσης

Στον ιδιωτικό τομέα υπάρχουν σαφή όρια του πληροφοριακού συστήματος. Ωστόσο, στο δημόσιο τομέα τα όρια είναι ασαφή και πρέπει να οριστούν ώστε να προκύψει ο εντοπισμός της ευθύνης. Ένα σημαντικό μειονέκτημα της CRAMM είναι ότι δεν περιλαμβάνει την διασύνδεση του πληροφοριακού συστήματος με άλλα εξωτερικά συστήματα. Επομένως, μία πολύ σημαντική πτυχή της ασφάλειας, δηλαδή η αλληλεξάρτηση του πληροφοριακού συστήματος με άλλα εκτός του οργανισμού, δεν εξετάζεται (European Union Agency for Network and Information Security, 2014). Αντιθέτως η MAGERIT λαμβάνει υπόψη της και αυτόν τον παράγοντα, καθιστώντας τη συμβατή με το ISO 31000:2009 (Manas, 2009).

8.3.2 Συνεντεύξεις και ερωτηματολόγια

Οι δύο μέθοδοι βασίζονται στην υψηλή εμπλοκή των εργαζομένων στον αξιολογούμενο οργανισμό αυξάνοντας και την πιθανότητα υιοθέτησης των προτεινόμενων αντιμέτρων. Απαιτούνται συναντήσεις τόσο με τη διοίκηση όσο και με κρίσιμους ανθρώπους από τις υπόλοιπες ομάδες ενδιαφέροντος, προκειμένου να διεξαχθούν συνεντεύξεις και να διαμοιραστούν ερωτηματολόγια που πρέπει να απαντηθούν. Σημαντικό κρίνεται να υπάρξει επικοινωνία τόσο με τους ιδιοκτήτες όσο και με τους χρήστες (Stoneburner et al., 2002). Μία από τις βασικές διαφορές των δύο μεθόδων είναι το περιεχόμενο των ερωτηματολογίων. Πιο συγκεκριμένα, το εργαλείο CRAMM ακολουθεί αυστηρή προτυποποίηση, ενώ το εργαλείο PILAR επιτρέπει στον αναλυτή να προσαρμόσει τα ερωτηματολόγια ανάλογα με τις ανάγκες του αξιολογούμενου οργανισμού (Crespo et al., 2006). Στο σημείο αυτό συλλέγονται και οι απαραίτητες πληροφορίες για το οργανόγραμμα, τις διαδικασίες και την τεχνοδιαμόρφωση του συστήματος προκειμένου να υπάρξει πλήρης κατανόηση της ροής και της διάχυσης της πληροφορίας. Επομένως αυτό το στάδιο διευκολύνει την καλύτερη κατανόηση της φύσης και της λειτουργίας του πληροφοριακού συστήματος.

8.3.3 Αναγνώριση αγαθών

Η CRAMM διαχωρίζει τα αγαθά στις εξής κατηγορίες (United Kingdom Central Computer and Telecommunication Agency, 2009) εξοπλισμός, υπηρεσίες, λογισμικό, δεδομένα και τοποθεσίες. Η μέθοδος MAGERIT κατηγοριοποιεί τα αγαθά στις εξής κατηγορίες (Crespo et al., 2006): υπηρεσίες, εφαρμογές, εξοπλισμός, μέσα αποθήκευσης, βιοηθητικός εξοπλισμός, δίκτυα επικοινωνιών, εγκαταστάσεις και πρόσωπα.

Κρίσιμος παράγοντας στη μέθοδο MAGERIT αλλά και στο εργαλείο PILAR είναι η αλληλεξάρτηση μεταξύ των αγαθών καθώς δημιουργεί μια διαστρωματοποιημένη ιεραρχία των αγαθών και των εξαρτήσεών τους που χρησιμοποιείται στη συνέχεια κατά την εκτίμηση της επικινδυνότητας. Πιο συγκεκριμένα, τα αγαθά μπορεί συχνά να είναι δομημένα σε επίπεδα, όπου τα ανώτερα στρώματα εξαρτώνται από τα χαμηλότερα (Crespo et al., 2006).

8.3.4 Αποτίμηση αγαθών

Κατά την αποτίμηση των αγαθών η CRAMM εξετάζει τις παρακάτω πτυχές United Kingdom Central Computer and Telecommunication Agency, 2009): διαθεσιμότητα, ακεραιότητα και εμπιστευτικότητα. Αντίστοιχα η MAGERIT λαμβάνει υπόψη αυτές τις διαστάσεις και προσθέτει την αυθεντικότητα των χρηστών των υπηρεσιών, την αυθεντικότητα της προέλευσης δεδομένων και την απονομή ευθυνών της χρήσης των υπηρεσιών και της πρόσβασης στα δεδομένα (Crespo et al., 2006). Για καθένα από αυτά τα κριτήρια διενεργούνται συνεντεύξεις και αποτιμάται η αξία κάθε αγαθού. Σημαντική διαφορά των δύο μεθόδων είναι ότι η MAGERIT χρησιμοποιεί την ανάλυση Delphi ώστε να εξετάσει τις διαφορετικές απόψεις και να καταλήξει στην κοινώς αποδεκτή για να χρησιμοποιηθεί στη συνέχεια στην εκτίμηση της επικινδυνότητας (Crespo et al., 2006). Μια τέτοια λειτουργία δεν προβλέπεται στην CRAMM. Η CRAMM βασίζεται κυρίως στις συνεντεύξεις για την αποτίμηση, ενώ η MAGERIT στα ερωτηματολόγια. Για την αποτίμηση αγαθών η CRAMM διαθέτει 10 επίπεδα, ενώ η MAGERIT διαθέτει 11 (European Union Agency for Network and Information Security, 2014). Στο τέλος αυτού του σταδίου, γίνεται επισκόπηση των στοιχείων με τη διοίκηση, προκειμένου να διασφαλιστούν η ακρίβεια των δεδομένων

και η συμφωνία μεταξύ του οργανισμού και των αναλυτών σχετικά με τα αγαθά που πρέπει να προστατεύονται και την αντίστοιχη αξία τους (Stoneburner et al., 2002).

8.3.5 Εκτίμηση απειλών

Το εργαλείο CRAMM καλύπτει τα παρακάτω είδη απειλών (United Kingdom Central Computer and Telecommunication Agency, 2009) λογικές απειλές, απειλές επικοινωνιών, τεχνικές βλάβες, ανθρώπινα σφάλματα και φυσικές απειλές. Στο εργαλείο PILAR οι απειλές ομαδοποιούνται επίσης σε πέντε κατηγορίες (Crespo et al., 2006): βιομηχανικές καταστροφές, φυσικές καταστροφές, λάθη/ακούσιες αποτυχίες και εκούσιες επιθέσεις. Παρά το μεγάλο αριθμό κατηγοριών, το PILAR περιλαμβάνει και απειλές που είναι πιο σύγχρονες όπως την κοινωνική μηχανική (Mellado et al., 2006). Όλες οι διαθέσιμες μέθοδοι ανάλυσης κινδύνου αντιμετωπίζουν διαφορετικού είδους απειλές ακολουθώντας τα ίδια βήματα και τις ίδιες λεπτομέρειες. Αυτό μπορεί να είναι παραπλανητικό για προμελετημένες απειλές, οι οποίες έχουν ανξημένο επίπεδο πολυπλοκότητας (π.χ. εξάρτηση μεταξύ των επιθέσεων, διαφορετικές πηγές απειλών κ.τ.λ.). Ο στόχος του επιτιθέμενου είναι επίσης σημαντικός, αφού αυτό που θέλει να προστατέψει η επιχείρηση μπορεί να μη συμπίπτει με αυτό που θέλει να βλάψει ο επιτιθέμενος (Welch & Lathrop, 2003).

Το PILAR διαφοροποιεί το μοντέλο εκτίμησης απειλών αναλόγως με το αν έχει χρησιμοποιηθεί ποσοτική ή ποιοτική προσέγγιση. Παράλληλα, μπορούν να προστεθούν νέες τρωτότητες και να αντιστοιχισθούν με τα αγαθά της προηγούμενης φάσης, οδηγώντας στην επέκταση της βάσης δεδομένων. Το CRAMM υπολογίζει ποιοτικά τις απειλές. Οι απειλές κατηγοριοποιούνται σε πέντε επίπεδα ενώ στο εργαλείο PILAR ακολουθείται διαφορετική ποιοτική προσέγγιση σε τρία επίπεδα (European Union Agency for Network and Information Security, 2014).

8.3.6 Εκτίμηση Κινδύνου

Οι τρωτότητες βασίζονται στην κατανόηση των λειτουργιών και των δυνατοτήτων που είναι διαθέσιμες μέσα από το περιβάλλον του συστήματος. Η MAGERIT υπολογίζει τον κίνδυνο για ένα αγαθό από το συσσωρευτικό κίνδυνο που προκύπτει από μια απειλή αλλά και τη συχνότητα εμφάνισης της απειλής αυτής. Πιο συγκριμένα, από τη στιγμή που έχει διαπιστωθεί ότι η απειλή μπορεί να βλάψει ένα

αγαθό, η τρωτότητα πρέπει να εκτιμηθεί λαμβάνοντας υπόψη δύο πτυχές την αποδόμηση του αγαθού και τη συχνότητα της απειλής. Η αποδόμηση μετρά τη ζημία που θα προκληθεί αν συμβεί ένα περιστατικό. Η αποδόμηση συχνά περιγράφεται ως μέρος της αξίας του αγαθού και για τη μέτρησή της χρησιμοποιούνται ποιοτικές εκφράσεις (Crespo et al., 2006). Όταν οι απειλές είναι ακούσιες, ο υπολογισμός της ανάλογης απώλειας είναι πιο ακριβής και απλός. Άλλα όταν η απειλή είναι εκούσια, δεν μπορούν να υπάρξουν αναλογίες αφού ο εισβολέας μπορεί να προκαλέσει μεγάλη ζημιά επιλεκτικά. Η συχνότητα προσθέτει μια επιπλέον διάσταση στην εξέταση της αποδόμησης των αγαθών, καθώς μια απειλή μπορεί να έχει τρομερές συνέπειες, αλλά είναι πολύ απίθανο να συμβεί. Παράλληλα, μια άλλη απειλή μπορεί να έχει πολύ μικρές συνέπειες, αλλά να είναι τόσο συχνές ώστε να συσσωρεύονται σημαντικές ζημίες. Υπολογίζεται ως ο μέσος αριθμός των εμφανίσεων της απειλής κατά τη διάρκεια μιας συγκεκριμένης περιόδου, συνήθως ετησίως.

Η μέθοδος CRAMM εξετάζει κάθε συνδυασμό του γινομένου επισφάλεια και επίπτωση και βρίσκει ποιο είναι το πιο επικίνδυνο. Αυτό το γινόμενο είναι που καθορίζει ποια μέτρα θα ληφθούν, λαμβάνοντας υπόψη μόνο το worst-case scenario. Παράλληλα παρέχεται “what-if” ανάλυση για τις επιπτώσεις των πιθανών αλλαγών κατά περίπτωση στο σύστημα ή στο δίκτυο και στο προφίλ ασφάλειάς του (United Kingdom Central Computer and Telecommunication Agency, 2009) Η κλίμακα που χρησιμοποιείται στη μέθοδο MAGERIT για την εκτίμηση κινδύνου παίρνει τιμές από το ένα μέχρι το εννέα ενώ στην CRAMM από το ένα μέχρι το επτά. Το εργαλείο MAGERIT είναι ικανό να υπολογίσει την επικινδυνότητα είτε με προκαθορισμένους πίνακες είτε με αλγορίθμική ανάλυση (ποιοτική και ποσοτική) που βασίζεται σε μαθηματικά μοντέλα, ενώ το εργαλείο CRAMM υπολογίζει την επικινδυνότητα για κάθε ομάδα αγαθών μόνο βάσει προκαθορισμένων πινάκων (United Kingdom Central Computer and Telecommunication Agency, 2009; Crespo et al., 2006).

8.3.7 Προσδιορισμός αντιμέτρων

Τα μέτρα ασφάλειας λαμβάνονται υπόψη στον υπολογισμό του κινδύνου με δύο τρόπους (Sabey & Taylor, 1980):

- Μειώνοντας τη συχνότητα των απειλών: Ονομάζονται προληπτικά μέτρα ασφάλειας. Στην ιδανική περίπτωση, θα εμποδίσουν εντελώς την εμφάνιση της απειλής.
- Περιορίζοντας τις ζημιές: Υπάρχουν μέτρα ασφάλειας που περιορίζουν άμεσα οποιαδήποτε αποδόμηση, ενώ άλλα επιτρέπουν την άμεση ανίχνευση της επίθεσης για να σταματήσει η πορεία της αποδόμησης. Υπάρχουν άλλα μέτρα ασφάλειας που επικεντρώνονται στη γρήγορη ανάκαμψη του συστήματος μετά από την πραγματοποίηση της απειλής. Σε όλες αυτές τις εκδοχές η απειλή εμφανίζεται, αλλά οι συνέπειες είναι περιορισμένες.

Κάθε αντίμετρο στην CRAMM αποτιμάται σε μια κλίμακα από το ένα μέχρι το επτά. Τα αντίμετρα διαχωρίζονται σε κατηγορίες και υποκατηγορίες, βάσει επτά διαστάσεων, οι οποίες δηλώνουν το είδος του μέτρου: λογισμικού, υλικού, επικοινωνίας, διαδικαστική, φυσική, προσωπικού και περιβάλλοντος. Αφού υπολογιστούν τα προτεινόμενα αντίμετρα, ο αναλυτής επιλέγει για κάθε αντίμετρο αν είναι εφαρμόσιμο ή όχι και υπολογίζεται η προτεραιότητα εφαρμογής κάθε μέτρου σε κλίμακα από το δύο έως το δέκα. Ο υπολογισμός βασίζεται στον αριθμό των απειλών, αν απαιτείται για την προστασία μιας κρίσιμης εφαρμογής ή αν υπάρχουν ήδη εγκατεστημένα εναλλακτικά αντίμετρα. Επίσης λαμβάνεται υπόψη το κόστος εφαρμογής, η αποτελεσματικότητα και το είδος της προστασίας που προσδίδει κάθε αντίμετρο. Για κάθε αντίμετρο ορίζεται και ο τύπος προστασίας στον οποίο αναφέρεται. Οι τύποι που ορίζει η CRAMM είναι: μείωση απειλής, μείωση τρωτότητας, μείωση επίπτωσης, ανίχνευση και ανάκαμψη. Πολύ σημαντική κρίνεται και η δυνατότητα επανιχνηλάτησης για την εξέταση συγκεκριμένου συνδυασμού αγαθού / απειλής / ευπάθειας που οδήγησε στην επιλογή των αντίστοιχων αντιμέτρων. Κάθε ομάδα αντιμέτρων στο εργαλείο CRAMM, έχει την ακόλουθη δομή:

1. Δήλωση πολιτικής, η οποία εξάγεται αυτολεξεί από το κατάλληλο έγγραφο ασφαλείας.
2. Ο στόχος και η ανάγκη που θα ικανοποιηθεί από την εφαρμογή των συγκεκριμένων αντιμέτρων.
3. Λεπτομερής περιγραφή της σχετιζόμενης επιχειρησιακής λειτουργίας με το αντίμετρο.

4. Τρόποι ή επιλογές που μπορούν να διασφαλίσουν την επιθυμητή λειτουργικότητα (United Kingdom Central Computer and Telecommunication Agency, 2009).

Στο εργαλείο PILAR τα αντίμετρα κατηγοριοποιούνται σύμφωνα με τέσσερις διαστάσεις (Crespo et al., 2006): διοίκηση, πολιτικές προσωπικού, τεχνικές λύσεις και φυσική ασφάλεια. Ωστόσο στο PILAR έχουμε περισσότερους τύπους αντιμέτρων (δέκα έναντι πέντε που έχει το εργαλείο CRAMM) και η προτεραιοποίηση γίνεται με κλίμακα από το μηδέν έως το δέκα. Και τα δύο εργαλεία διαθέτουν επιλογή αυτόματης υπόδειξης αντιμέτρων που θεωρούνται κατάλληλα και προσδιορίζουν τα αντίμετρα και τις σχετικές λύσεις συντελώντας στην εξασφάλιση της επιχειρησιακής συνέχειας.

9. Επίλογος

Οι οργανισμοί λειτουργούν σε ένα περιβάλλον υψηλής πολυπλοκότητας και διασύνδεσης. Αυτή η λειτουργικότητα εδράζεται σαφώς στα πληροφοριακά συστήματα που διαθέτουν. Η παραμικρή δυσλειτουργία, διακοπή ή παράνομη διείσδυση στα συστήματα αυτά μεταφράζεται σε κόστος. Σε συστήματα που περιέχουν ευαίσθητα δεδομένα οι επιπτώσεις δεν είναι μόνο οικονομικής αλλά και ζωτικής σημασίας, καθιστώντας την ασφάλεια των πληροφοριακών συστημάτων ακρογωνιαίο λίθο για τη σύγχρονη κοινωνία.

Οι οργανισμοί χρησιμοποιούν την εκτίμηση επικινδυνότητας για να καθορίσουν την έκταση των πιθανών απειλών και τους κινδύνους που σχετίζονται με ένα πληροφοριακό σύστημα. Η έννοια της επικινδυνότητας υποκαθιστά τον αόριστο στόχο της επίτευξης της ασφάλειας με τον εφικτό και μετρήσιμο στόχο του περιορισμού της επικινδυνότητας εντός αποδεκτών ορίων. Το αποτέλεσμα αυτής της διεργασίας συντελεί στην αναγνώριση των κατάλληλων ελέγχων για την πρόληψη και τον περιορισμό των κινδύνων και στην καλύτερη κατανόηση των εσωτερικών διαδικασιών του οργανισμού. Για την αξιολόγηση/αποτίμηση του επιπέδου ασφάλειας των πληροφοριακών συστημάτων εφαρμόζονται τεχνικές ανάλυσης επικινδυνότητας. Η ανάλυση επικινδυνότητας εμπεριέχει σημαντική υποκειμενικότητα στις εκτιμήσεις τόσο της αξίας των αγαθών, όσο και στην αποτίμηση των απειλών και τρωτοτήτων. Η υποκειμενικότητα αυτή συχνά συγκαλύπτεται πίσω από την αυστηρότητα των μαθηματικών-πιθανοτικών μοντέλων, τη συστηματικότητα των μεθόδων ανάλυσης επικινδυνότητας και την «αντικειμενικότητα» των εργαλείων που υποστηρίζουν τις σχετικές μεθόδους.

9.1 Συμπεράσματα

Στην παρούσα μελέτη παρουσιάστηκαν δημοφιλείς μέθοδοι μελέτης επικινδυνότητας που εφαρμόζονται από τους αναλυτές. Η επιλογή των συγκεκριμένων μεθόδων βασίστηκε στην αναγνωρισμότητά τους και δε σημαίνει ότι κρίνονται ως πιο σημαντικές από άλλες μεθόδους. Ωστόσο, η ευρεία αποδοχή τους από την επιστημονική κοινότητα αποτέλεσε και αποτελεί αναπόσπαστο χαρακτηριστικό της ταυτότητάς τους. Παρατηρείται ότι οι μέθοδοι έχουν κοινά χαρακτηριστικά (κυρίως σε διαδικαστικά θέματα) αλλά διαφέρουν σημαντικά σε τομείς όπως η υποστήριξη

από εξειδικευμένο λογισμικό και η προσαρμοστικότητα στις ανάγκες του οργανισμού και των χρηστών.

Στη συνέχεια προτάθηκαν κριτήρια σύμφωνα με τα οποία θα μπορούσαν να αξιολογηθούν και στη συνέχεια να επιλεγούν οι μέθοδοι. Παρατηρήθηκε ότι δεν υπάρχει κάποιο προτυποποιημένο πλαίσιο και αυτό που χρησιμοποιείται κατά κόρον και προτάθηκε από τον οργανισμό ENISA (2006) είναι πλέον ξεπερασμένο και εξετάζει τις μεθόδους υπό μια στενή έννοια. Παράλληλα επισημαίνεται ότι απαιτείται ο καθορισμός της στάθμισης για κάθε κριτήριο, καθώς κάθε οργανισμός πρέπει να επικεντρώνεται στα κριτήρια εκείνα που θεωρούνται πιο σημαντικά ανάλογα με τις ανάγκες του. Για την επίτευξη αυτής της στάθμισης προτείνεται η χρήση της μεθόδου AHP.

Επιπρόσθετα, επιχειρείται σύγκριση ανάμεσα στις μεθόδους CRAMM και MAGERIT και στα εργαλεία που τις υποστηρίζουν (CRAMM και PILAR αντίστοιχα). Η μέθοδος CRAMM είναι η πιο ευρέως αποδεκτή επιλογή, αλλά για το χρήστη που χρησιμοποιεί εργαλεία εκτίμησης κινδύνου δεν είναι ούτε η ευκολότερη, ούτε η πιο φιλική. Είναι, όμως, το εργαλείο του οποίου την εγκυρότητα κανένας ελεγκτής που πιστοποιεί για το ISO 27001 δεν μπορεί να αμφισβητήσει. Η μέθοδος MAGERIT ακόμα δεν έχει καθιερωθεί στην επιστημονική κοινότητα στο βαθμό αναγνώρισης της CRAMM. Οι συχνές ανανεώσεις της βάσης της και η προσαρμοστικότητα που τη χαρακτηρίζει, βρίσκουν ολοένα και μεγαλύτερη εφαρμογή στον τομέα της ανάλυσης και διαχείρισης επικινδυνότητας, αλλά δείχνουν ότι ακόμα απαιτείται χρόνος ώστε να φτάσει τη σταθερότητα που παρέχει η CRAMM. Επομένως είναι αδήριτη η ανάγκη για τη στήριξη της CRAMM από την επιστημονική κοινότητα, προκειμένου να μην ακολουθήσει τη μοίρα άλλων μεθόδων που αρχικά φάνηκε να κερδίζουν την εμπιστοσύνη των αναλυτών (Octave) αλλά στην πορεία επισκιάστηκαν και πάλι από την καθιερωμένη CRAMM.

Η νιοθέτηση της μεθόδου PILAR από το NATO μετά το 2016 είναι σαφής ένδειξη για το ότι σε μερικά χρόνια αναμένεται το εργαλείο να έχει εμπλουτιστεί και να έχει ωριμάσει σε τέτοιο βαθμό που να χρησιμοποιείται από διεθνείς οργανισμούς που διαχειρίζονται τεράστιο όγκο δεδομένων. Ωστόσο, η ελληνική πραγματικότητα έχει αποδείξει ότι δυσκολεύεται να ακολουθήσει τις επιταγές της εποχής και απαιτούνται πολλές συζητήσεις και διαβουλεύσεις προκειμένου να αλλάξει ένα καθιερωμένο πρότυπο. Ακόμα περισσότερο χρόνο χρειάζεται να καλλιεργηθεί το αίσθημα

εμπιστοσύνης που παρέχει μια ευρέως διαδεδομένη και καταξιωμένη μέθοδος όπως η CRAMM. Η αξιολόγηση που έγινε παραπάνω, φανερώνει ότι οι δύο μέθοδοι είναι ουσιαστικά ισάξιες. Τα σημεία στα οποία κερδίζει η CRAMM είναι η αναγνώριση από τη νομοθεσία και οι αυστηρές και προτυποποιημένες διαδικασίες. Ωστόσο η αυστηρή προτυποποίηση αποτελεί και την αχίλλειο πτέρνα της, καθώς δεν παρέχει στους αναλυτές την απαραίτητη ευελιξία σε ένα τεχνολογικό περιβάλλον που διαρκώς μεταβάλλεται. Η προσαρμοστικότητα της MAGERIT και η φιλική διεπαφή προς τους χρήστες είναι τα κύρια πλεονεκτήματά της και αποτελούν ισχυρά κίνητρα για τη χρήση της μεθόδου.

Τέλος, παρατίθεται πρότυπο για την τεκμηρίωση των αποτελεσμάτων της μεθόδου Magerit κατά τη μελέτη της επικινδυνότητας. Η τεκμηρίωση και τα έγγραφα που αναφέρονται στη μέθοδο Magerit είναι κυρίως στα ισπανικά. Επομένως οποιαδήποτε προσπάθεια για την εναρμόνιση της μεθόδου με τα ελληνικά δεδομένα κρίνεται ως απαραίτητη και σημαντική για τον τομέα της μελέτης επικινδυνότητας, καθώς μπορεί να είναι πολύ χρήσιμοι για τους ερευνητές και τους αναλυτές του πεδίου. Η ύπαρξη προτύπου τεκμηρίωσης θα διευκολύνει τις προσπάθειες υιοθέτησης της μεθόδου από τις αντίστοιχες ομάδες που ασχολούνται με τη μελέτη επικινδυνότητας, αυξάνοντας τη δημοτικότητά της.

Βιβλιογραφία

A Reference Security Management Plan for Energy Infrastructure. Prepared by the Harnser Group for the European Commission under Contract TREN/C1/185/200. 2010. Available at http://ec.europa.eu/energy/infrastructure/studies/doc/2010_rsmp.pdf.

Abie, H., & Borking, J. (2012). *Risk Analysis Methods and Practices*, Center for Democracy & Technology, USA.

Akintoye, A., Beck, M., Hardcastle, C., Chinyio, E., & Asenova, D. (2001). *Framework for risk assessment and management of private finance initiative projects* (p. 10). Glasgow, Scotland, UK: Glasgow Caledonian University.

Alberts, C. J., & Dorofee, A. (2002). *Managing information security risks: the OCTAVE approach*. Addison-Wesley Longman Publishing Co., Inc..

Ale, B. J. M. (2002). Risk assessment practices in The Netherlands. *Safety Science*, 40(1), 105-126.

Bailes, A. J., & Frommelt, I. (2004). *Business and security: public-private sector relationships in a new security environment*. Oxford University Press.

Baron, J., Hershey, J. C., & Kunreuther, H. (2000). Determinants of priority for risk reduction: the role of worry. *Risk Analysis*, 20(4), 413-428.

Baskerville, R. (1993). Information systems security design methods: implications for information systems development. *ACM Computing Surveys (CSUR)*, 25(4), 375-414.

Blakley, B., McDermott, E., & Geer, D. (2001). Information security is information risk management. In *Proceedings of the 2001 workshop on New security paradigms* (pp. 97-104). ACM.

Bloom, B. S. (1971). Handbook on formative and summative evaluation of student learning.

Bloom, M., & Milkovich, G. T. (1998). Relationships among risk, incentive pay, and organizational performance. *Academy of Management Journal*, 41(3), 283-297.

Bourguignon, F., Ferreira, F. and Leite, P. (2002). *Ex-ante evaluation of conditional cash transfer programs: the case of Bolsa Escola*. Policy Research Working Paper 2916. World Bank, Policy Research Department, Washington D.C

Browne, M. W., & Cudeck, R. (1989). Single sample cross-validation indices for covariance structures. *Multivariate Behavioral Research*, 24(4), 445-455.

Bryman, A. (2012). *Social research methods*. Oxford university press.

Burgess, P. (2006). Social values and the logic of threat: the European Programme for Critical Infrastructures Protection (EPCIP). In *Critical Infrastructure Protection Conference, Utrecht* (Vol. 8).

Bush, G. W. (2003). Homeland Security Presidential Directive (HSPD-7): Critical infrastructure identification, prioritization, and protection. *Washington, DC: White House*.

Campbell, P. L., & Stamp, J. E. (2004). *A classification scheme for risk assessment methods*. United States. Department of Energy.

Cardona, O. D. (2004). The need for rethinking the concepts of vulnerability and risk from a holistic perspective: a necessary review and criticism for effective risk management. *Mapping vulnerability: Disasters, development and people*, 37-51.

Carr, M. J., Konda, S. L., Monarch, I. A., Ulrich, F. C., & Walker, C. F. (1993). *T axonomy-Based Risk Identification*. SEI Technical Report SEI-93-TR-O06, Pittsburgh, PA: Software Engineering Institute.

Congressional Budget Office. (1983). *Public works infrastructures: Policy considerations for the 1980s.*, Government Printing Office.

COUNCIL DIRECTIVE 2008/114/CE (2008)

Craft, R. (1998). *An Open Framework for Risk Management*, Proceedings of the 21st National Information Systems Security Conference, Arlington, USA.

Crespo, F., Gomez, M., Candau, J., Manas, J.A. (2006). *MAGERIT– version 2, Methodology for Information Systems Risk Analysis and Management, Book I – The Method*, Ministerio de Administraciones Publicas.

Curcin, V., Woodcock, T., Poots, A. J., Majeed, A., & Bell, D. (2014). Model-driven approach to data collection and reporting for quality improvement. *Journal of biomedical informatics*.

Da Veiga, A., & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, 29(2), 196-207.

DANIDA (2006). Evaluation guidelines. Copenhagen, Denmark: Evaluation Department, Ministry of Foreign Affairs of Denmark.

Das, T. K., & Teng, B. S. (1998). Resource and risk management in the strategic alliance making process. *Journal of management*, 24(1), 21-42.

Davenport, T. H. (2013). *Process innovation: reengineering work through information technology*. Harvard Business Press.

DCSSI (2004) EBIOS – Expression of needs and identification of security objectives. <http://www.ssi.gouv.fr/archive/en/confidence/ebiospresentation.html>. Last Accessed 23 October 2014.

El Fray, I. (2012). A comparative study of risk assessment methods, MEHARI & CRAMM with a new formal model of risk assessment (FoMRA) in information systems. In *Computer Information Systems and Industrial Management* (pp. 428-442). Springer Berlin Heidelberg.

Ellis, J., Fisher, D., Longstaff, T., Pesante, L., & Pethia, R. (1997). *Report to the President's Commission on Critical Infrastructure Protection* (No. CMU/SEI-97-SR-00333). Carnegie-Mellon University, Pittsburgh.

ENISA. (2006). *Inventory of Risk Management/Risk Assessment methods and tools.* Last accessed 16 October 2014 http://www.enisa.europa.eu/rmra/rm_home.htm

Eskisabel Azpiazu, A. (2014). A Framework to select risk analysis methods in Healthcare.

European Commission. (2004). *Preparedness and Consequence Management in the Fight against Terrorism.*

Fischhoff, B., Slovic, P., & Lichtenstein, S. (1981). Lay foibles and expert fables in judgements about risk. *Progress in resource management and environmental planning*, 3, 161-202.

Fletcher, W. J. (2005). The application of qualitative risk assessment methodology to prioritize issues for fisheries management. *ICES Journal of Marine Science: Journal du Conseil*, 62(8), 1576-1587.

Forman, E. H. (1993). Facts and fictions about the analytic hierarchy process. *Mathematical and computer modelling*, 17(4), 19-26.

Forman, E. H., & Gass, S. I. (2001). The analytic hierarchy process-an exposition. *Operations research*, 49(4), 469-486.

Garrabrants, W. M., Ellis III, A. W., Hoffman, L. J., & Kamel, M. (1990). CERTS: a comparative evaluation method for risk management methodologies and tools. In *Computer Security Applications Conference, 1990., Proceedings of the Sixth Annual* (pp. 251-257). IEEE.

Gerber, M., & Von Solms, R. (2005). Management of risk in the information age. *Computers & Security*, 24(1), 16-30.

Gorman, S. P., Schintler, L., Kulkarni, R., & Stough, R. (2004). The revenge of distance: Vulnerability analysis of critical information infrastructure. *Journal of Contingencies and Crisis Management*, 12(2), 48-63.

Green, C. H., & McFadden, L. (2007). Defining 'vulnerability': conflicts, complexities and implications for coastal zone management. *Journal of Coastal Research*.

Gupta, P. K. (2011). Risk management in Indian companies: EWRM concerns and issues. *Journal of Risk Finance*, 12(2), 121-139.

Haines, Y. Y., Matalas, N. C., Lambert, J. H., Jackson, B. A., & Fellows, J. F. (1998). Reducing vulnerability of water supply systems to attack. *Journal of Infrastructure Systems*, 4(4), 164-177.

Hong, K. S., Chi, Y. P., Chao, L. R., & Tang, J. H. (2003). An integrated system theory of information security management. *Information Management & Computer*

Security, 11(5), 243-248.

Hopkinson, M. M. (2012). *The project risk maturity model: Measuring and improving risk management capability*. Gower Publishing, Ltd..

Humphreys, E. (2011). Information security management system standards. *Datenschutz und Datensicherheit-DuD*, 35(1), 7-11.

Information Security Forum (ISF) : The Standard of Good Practice (SOGP). http://www.isfsecuritystandard.com/index_ns.htm (2011)

ISO/IEC 13335: 1998. *Information Technology-Guidelines for the management of IT Security-Part 3: Techniques for the management of IT Security*. International Organization for Standardization.

ISO/IEC 27001:2005. *Information technology-security techniques-information security management systems-requirements*. International Organization for Standardization.

ISO/IEC 27002: 2005. *Information Technology-Security Techniques-Code of Practice for Information Security Management*. International Organization for Standardization.

Kaplan, S., & Garrick, B. J. (1981). On the quantitative definition of risk. *Risk analysis*, 1(1), 11-27.

Karolak, D. W., & Karolak, N. (1995). *Software engineering risk management: A just-in-time approach*. IEEE Computer Society Press.

Kasperson, R. E., Renn, O., Slovic, P., Brown, H. S., Emel, J., Goble, R., & Ratnick, S. (1988). The social amplification of risk: A conceptual framework. *Risk analysis*, 8(2), 177-187.

Katzke, S. W. (1988). A government perspective on risk management of automated information systems. In *Proceedings of 1988 Computer Security Risk Management Model Builders Workshop* (pp. 3-20).

Kiker, G. A., Bridges, T. S., Varghese, A., Seager, T. P., & Linkov, I. (2005). Application of multicriteria decision analysis in environmental decision making. *Integrated environmental assessment and management*, 1(2), 95-108.

Kitchenham, B., Linkman, S., & Law, D. (1997). DESMET: a methodology for evaluating software engineering methods and tools. *Computing & Control Engineering Journal*, 8(3), 120-126.

Kröger, W. (2008). Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools. *Reliability Engineering & System Safety*, 93(12), 1781-1787.

Kurowski, S., Zibuschka, J., Roßnagel, H., & Engelbach, W. (2012). A Survey of Interoperability Concepts for Security Systems in Public Transport. *Mobility in a Globalised World*, 6, 91.

- Landoll, D. J., & Landoll, D.** (2005). *The security risk assessment handbook: A complete guide for performing security risk assessments*. CRC Press.
- Lichtenstein, S.** (1996). Internet acceptable usage policy. *Computer Audit Update*, 1996(12), 10-21.
- Lund, M. S., Solhaug, B., & Stølen, K.** (2010). *Model-driven risk analysis: the CORAS approach*. Springer.
- Manas, J. A.** (2009). *PILAR–Risk Analysis and Management Tool*. (Last accessed 15 November 2014) http://www.pilar-tools.com/en/tools/pilar/v54/help_en/cia/index.html
- Markowsky, G.** (2011). Universal asset assessment system based on excelTM. In *Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), 2011 IEEE 6th International Conference on* (Vol. 2, pp. 747-752). IEEE.
- Mayerfeld, H. T.** (1989). Framework for Risk Management. A Synthesis of the Working Group Reports from the First Computer Security Risk Management Model Builders Workshop. In *Proceedings of the Second Computer Security Risk Management Model Builders Workshop* (pp. 1-19).
- Mays, N., & Pope, C.** (2000). Assessing quality in qualitative research. *Bmj*, 320(7226), 50-52.
- McManus, J.** (2012). *Risk management in software development projects*. Routledge.
- McNeil, A. J., Frey, R., & Embrechts, P.** (2010). *Quantitative risk management: concepts, techniques, and tools*. Princeton university press.
- Mellado, D., Fernández-Medina, E., & Piattini, M.** (2006). A comparative study of proposals for establishing security requirements for the development of secure information systems. In *Computational Science and Its Applications-ICCSA 2006* (pp. 1044-1053). Springer Berlin Heidelberg.
- Merkhofer, M. W.** (1985). An Approach for Assessing Health Risks Associated with Alternative Ambient Air Quality Standards. In *Environmental Impact Assessment, Technology Assessment, and Risk Analysis* (pp. 691-722). Springer Berlin Heidelberg.
- Merkhoffer, M. W.** (1983). *Comparative Evaluation of Quantitative Decision-making Approaches*. SRI International.
- Min, H. S. J., Beyeler, W., Brown, T., Son, Y. J., & Jones, A. T.** (2007). Toward modeling and simulation of critical national infrastructure interdependencies. *Iie Transactions*, 39(1), 57-71.
- Mirkin, B.G.**, 1979. *Group Choice*, Halsted Press, New York.
- Mooney, C. Z., & Duval, R. D.** (Eds.). (1993). *Bootstrapping: A nonparametric approach to statistical inference* (No. 94-95). Sage.
- Morgan, K. M., & Fischhoff, B.** (2001). The use of public risk ranking in regulatory

- development. *Improving regulation: Cases in environment, health, and safety*, 208.
- Morgan, M. G., Florig, H. K., DeKay, M. L., & Fischbeck, P.** (2000). Categorizing risks for risk ranking. *Risk analysis*, 20(1), 49-58.
- Munteanu, A.** (2006). Information security risk assessment: The qualitative versus quantitative dilemma. In *Managing Information in the Digital Economy: Issues & Solutions-Proceedings of the 6th International Business Information Management Association (IBIMA) Conference* (pp. 227-232).
- Niekerk, L. v., Labuschagne, L.** (2006). *The Peculum Model: Information Security Risk Management for the South African SMME*, ISSA 2006 Proceedings, 5th-7th July, Gauteng, Republic of South Africa.
- Nikroo, E. R., Tabriz, A. A., Farahani, R., & Tavakoli, M.** (2013). Prioritizing Strategies and Ranking Execution Methods by Integrated Approach of SWOT Analysis and Fuzzy Quality Function Deployment.
- Olle, T. W., Stuart, A. V., & Bhabuta, L.** (Eds.). (1988). *Computerized assistance during the information systems life cycle: proceedings of the IFIP WG 8.1 Working Conference on Computerized Assistance during the Information Systems Life Cycle, CRIS 88, Egham, England*.
- Paté-Cornell, M. E.** (1996). Uncertainties in risk analysis: Six levels of treatment. *Reliability Engineering & System Safety*, 54(2), 95-111.
- Paulk, M. C., Curtis, B., Chrassis, M. B., & Weber, C. V.** (1993). Capability maturity model, version 1.1. *Software, IEEE*, 10(4), 18-27.
- Peltier, T. R.** (2005). *Information security risk analysis*. CRC press.
- Pickard, A. J.** (2013). *Research methods in information*. Facet Publications.
- Potter, M., Gordon, S., & Hamer, P.** (2004). The nominal group technique: a useful consensus methodology in physiotherapy research. *New Zealand Journal of Physiotherapy*, 32, 126-130.
- Pruyt, E., Wijnmalen, D. J., & Bokkerink, M.** (2013). What can we learn from the evaluation of the Dutch
- Punch, K. F.** (2013). *Introduction to social research: Quantitative and qualitative approaches*. Sage.
- Radvanovsky, R. S., & McDougall, A.** (2009). *Critical infrastructure: homeland security and emergency preparedness*. CRC Press.
- Reddy, T. A., Snyder, S., Bem, J., & Bahnfleth, W.** (2011). Analysis Tools and Guidance Documents for Evaluating and Reducing Vulnerability of Buildings to Airborne Threats--Part 1: Literature Review. *ASHRAE Transactions*, 117(1).
- Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K.** (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *Control Systems, IEEE*, 21(6),

11-25.

- Robson, C.** (2011). *Real world research: a resource for users of social research methods in applied settings*. Chichester: Wiley.
- Saaty, T. L.** (1977). A scaling method for priorities in hierarchical structures. *Journal of mathematical psychology*, 15(3), 234-281.
- Saaty, T. L.** (1986). Axiomatic foundation of the analytic hierarchy process. *Management science*, 32(7), 841-855.
- Sabey, B. E., & Taylor, H.** (1980). *The known risks we run: the highway* (pp. 43-70). Springer US.
- Sajko, M., Hadjina, N., & Pesut, D.** (2010, May). Multi-criteria model for evaluation of information security risk assessment methods and tools. In *MIPRO, 2010 Proceedings of the 33rd International Convention* (pp. 1215-1220). IEEE.
- Sipahi, S., & Timor, M.** (2010). The analytic hierarchy process and analytic network process: an overview of applications. *Management Decision*, 48(5), 775-808.
- Smith, N. J., Merna, T., & Jobling, P.** (2013). *Managing risk in construction projects*. John Wiley & Sons.
- Smojver, S.** (2011). Selection of information security risk management method using analytic hierarchy process (ahp). In *Central European Conference on Information and Intelligent Systems, CECIIS–2011* (Vol. 37).
- Speier, C., Whipple, J. M., Closs, D. J., & Voss, M. D.** (2011). Global supply chain design considerations: mitigating product safety and security risks. *Journal of Operations Management*, 29(7), 721-736.
- Spence, D. .** (2007). *The European Union and Terrorism*. John Harper Publishing.
- Stoneburner, G., Goguen, A., & Feringa, A.** (2002). Risk management guide for information technology systems. *Nist special publication*, 800(30), 800-30.
- Straub, D. W., & Welke, R. J.** (1998). Coping with systems risk: security planning models for management decision making. *Mis Quarterly*, 441-469.
- Subramanian, N., & Ramanathan, R.** (2012). A review of applications of Analytic Hierarchy Process in operations management. *International Journal of Production Economics*, 138(2), 215-241.
- Suh, B., & Han, I.** (2003). The IS risk analysis based on a business model. *Information & Management*, 41(2), 149-158.
- Syalim, A., Hori, Y., & Sakurai, K.** (2009). Grouping provenance information to improve efficiency of access control. In *Advances in Information Security and Assurance* (pp. 51-59). Springer Berlin Heidelberg.
- Theoharidou, M., Kotzanikolaou, P., & Gritzalis, D.** (2009). Risk-based criticality

analysis. In *Critical infrastructure protection III* (pp. 35-49). Springer Berlin Heidelberg.

Thompson, K. M., & Graham, J. D. (1996). Going beyond the single number: using probabilistic risk assessment to improve risk management. *Human and Ecological Risk Assessment*, 2(4), 1008-1034.

Tipton, H. F., & Krause, M. (2012). *Information security management handbook*. CRC Press.

Tohidi, H. (2011). The Role of Risk Management in IT systems of organizations. *Procedia Computer Science*, 3, 881-887.

Turner, B. L., Kasperson, R. E., Matson, P. A., McCarthy, J. J., Corell, R. W., Christensen, L., & Schiller, A. (2003). A framework for vulnerability analysis in sustainability science. *Proceedings of the national academy of sciences*, 100(14), 8074-8079.

Uijt de Haag, P. A. M., & Ale, B. J. M. (1999). Guidelines for quantitative risk assessment (Purple Book). *Committee for the Prevention of Disasters, The Hague*.

United Kingdom Central Computer and Telecommunication Agency (1996), *CCTA Risk Analysis and Management Method: User Manual*, version 3.0 edition, HMSO, London.

Utne, I. B., Hokstad, P., & Vatn, J. (2011). A method for risk modeling of interdependencies in critical infrastructures. *Reliability Engineering & System Safety*, 96(6), 671-678.

Van Der Sluijs, J. P., Craye, M., Funtowicz, S., Kloprogge, P., Ravetz, J., & Risbey, J. (2005). Combining quantitative and qualitative measures of uncertainty in model-based environmental assessment: the NUSAP system. *Risk analysis*, 25(2), 481-492.

Voronca, S. L. (2012). Analysing some of the existing risk assessment and management standards applied worldwide, for energy companies. *Journal of Sustainable Energy*, 3(3).

Vorster, A., & Labuschagne, L. (2005). A framework for comparing different information security risk analysis methodologies. In *Proceedings of the 2005 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries* (pp. 95-103). South African Institute for Computer Scientists and Information Technologists.

Vose, D. (2008). *Risk analysis: a quantitative guide*. John Wiley & Sons.

Wahlgren, G., Bencherifa, K., & Kowalski, S. (2013). A Framework for selecting IT Security Risk Management Methods based on ISO27005. In *MIC-CPE 2013: 6th International Conference on Communications, Propagation and Electronics*. Kenitra, Morocco: 1-3 Februari 2013. Academy Publisher.

Wang, A. J. A. (2005). Information security models and metrics. In *Proceedings of the*

43rd annual Southeast regional conference-Volume 2 (pp. 178-184). ACM.

Webler, T., Rakel, H., Renn, O., & Johnson, B. (1995). Eliciting and classifying concerns: A methodological critique. *Risk Analysis*, 15(3), 421-436.

Weiss, J. (Ed.). (2010). *Protecting industrial control systems from electronic threats*. Momentum Press.

Welch, D., & Lathrop, S. (2003). Wireless security threat taxonomy. In *Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society* (pp. 76-83). IEEE.

Whitman, M., & Mattord, H. (2011). *Principles of information security*. Cengage Learning.

Wind, Y., & Saaty, T. L. (1980). Marketing applications of the analytic hierarchy process. *Management Science*, 26(7), 641-658.

Wood, M. D., Bostrom, A., Bridges, T., & Linkov, I. (2012). Cognitive mapping tools: Review and risk management needs. *Risk Analysis*, 32(8), 1333-1348.

Woodhouse, J. (2006). Putting the total jigsaw puzzle together: PAS 55 standard for the integrated, optimized management of assets. In *International Maintenance Conference*.

Xenakis, C., & Wolthusen, S. (Eds.). (2011). *Critical Information Infrastructure Security: 5th International Workshop, CRITIS 2010, Athens, Greece, September 2010, Revised Papers* (Vol. 6712). Springer.

Yazar, Z. (2002). A qualitative risk analysis and management tool-CRAMM. *SANS InfoSec Reading Room White Paper*.

Zsidisin, G. A., Ellram, L. M., Carter, J. R., & Cavinato, J. L. (2004). An analysis of supply risk assessment techniques. *International Journal of Physical Distribution & Logistics Management*, 34(5), 397-413.

Γκρίτζαλης Σ., Κάτσικας Σ., Γκρίτζαλης Δ.. (2003). *Ασφάλεια Υπολογιστών και Δικτύων*, Παπασωτηρίου.

International Standard ISO/IEC 27005, "Information technology-Security techniques-Information security risk management", First edition 2008

Κάτσικας Σ., Γκρίτζαλης Δ., Γκρίτζαλης Σ. (επ. επιμ.). (2004). *Ασφάλεια Πληροφοριακών Συστημάτων*, Εκδόσεις Νέων Τεχνολογιών.

ΠΔ 39/2011 «Προσαρμογή της ελληνικής νομοθεσίας προς τις διατάξεις της Οδηγίας 2008/114/EK του Συμβουλίου της 8ης Δεκεμβρίου 2008 ‘σχετικά με τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας, και σχετικά με την αξιολόγηση της ανάγκης βελτίωσης της προστασίας τους

ΠΑΡΑΡΤΗΜΑ

Επιτελική Σύνοψη Παραδοτέου

Το παρόν έργο αποβλέπει στην εκπόνηση του Σχεδίου Ασφάλειας των Πληροφοριακών Συστημάτων (στο εξής ΠΣ) του Οργανισμού X (στο εξής X).

Οι κυριότεροι επιμέρους στόχοι του έργου είναι:

1. Να καταγραφούν και να αποτιμηθούν τόσο οι κίνδυνοι που υφίστανται τα ΠΣ του X, όσο και οι πιθανές επιπτώσεις που είναι δυνατόν να υπάρξουν σε αυτά.
2. Να εντοπιστούν και να περιγραφούν όλα τα μέτρα και οι διαδικασίες προστασίας/ασφάλειας που πρέπει να λαμβάνονται από τον X για την επαρκή προστασία των Πληροφοριακών Συστημάτων.
3. Να προταθεί Πολιτική Ασφάλειας των ΠΣ αυτών (η Πολιτική Ασφάλειας και τα Μέτρα Ασφάλειας πο απαρτίζουν το Σχέδιο Ασφάλειας).

Για να επιτευχθούν οι ως άνω στόχοι, οι Μελετητές του X χρησιμοποίησαν τη διεθνώς πρότυπη μέθοδο Magerit.

Το παρόν παραδοτέο (ΠΑ-2: Σχέδιο Ασφάλειας ΠΣ του X) αποτελεί το δεύτερο και τελευταίο παραδοτέο του έργου, όπως προβλέπεται στη σχετική σύμβαση, και περιλαμβάνει: (α) τα αποτελέσματα της ανάλυσης επικινδυνότητας των ΠΣ του X, καθώς και (β) το Σχέδιο Ασφάλειας των ΠΣ του X (δηλαδή την Πολιτική Ασφάλειας τους, καθώς και τα αναγκαία Μέτρα Προστασίας τους).

Τα ευρήματα των μελετητών επιβεβαίωσαν τη σημασία και τη χρησιμότητα της αξιοποίησης των Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ) από το σύνολο, σχεδόν, των Διευθύνσεων του X.

Η μεθοδική αποτίμηση των αγαθών των πληροφοριακών συστημάτων του Οργανισμού εντόπισε και κατέγραψε, μεταξύ άλλων, τα εξής άξια (σχετικής) προσοχής ενδεχόμενα:

- (α) Σε ό,τι αφορά την απώλεια διαθεσιμότητας, η υψηλότερη επίπτωση (4/10, κατά Magerit) προκύπτει από την κακή εγκατάσταση της δικτύωσης.
- (β) Σε ό,τι αφορά την απώλεια ακεραιότητας, η υψηλότερη επίπτωση (4,8/10, κατά Magerit) προκύπτει λόγω ολικής καταστροφής ή σκόπιμης αλλοίωσης των δεδομένων στους σταθμούς εργασίας, αλλά και σε ενδεχόμενη σκόπιμη αλλοίωση δεδομένων καταγραφής της λειτουργίας ΠΣ (log files) ή ελέγχου πρόσβασης των εργαζομένων.

γ) Σε ό,τι αφορά την απώλεια εμπιστευτικότητας, η υψηλότερη επίπτωση (4,8/10, κατά Magerit) προκύπτει λόγω αποκάλυψης σε τρίτους των προσωπικών δεδομένων που φυλάσσονται στα αρχεία προσωπικού (Δεδομένα προσωπικού, μισθοδοσίας και ελέγχου πρόσβασης).

Η ανάλυση επικινδυνότητας των ΠΣ του ΟΣΕ εντόπισε και κατέγραψε, μεταξύ άλλων, τις εξής αδυναμίες, οι οποίες πρέπει να αντιμετωπιστούν κατά προτεραιότητα:

1. Ελλιπής προστασία για αντιμετώπιση διαρροής δεδομένων, σε συνδυασμό με υψηλή συγκέντρωση πληροφορίας σε μεμονωμένα συστήματα (πχ. πληροφοριακό σύστημα Biznet).
2. Αυξημένη πολυπλοκότητα και ανομοιογένεια στην τεχνοδιαμόρφωση του δικτύου του Χ (μεγάλος αριθμός ετερογενών συνδέσεων), που εισάγει δυσκολίες στη διαχείριση.
3. Ελλιπής ενημέρωση προς τη Διεύθυνση Πληροφορικής για την αποχώρηση εργαζομένων από την ενεργό υπηρεσία (πχ. συνταξιοδότηση, παραίτηση κλπ.).
4. Παλαιότητα μέρους του υλικού (εξυπηρετητές, κόμβοι, εκτυπωτές κλπ.) και λογισμικού (πχ. σύστημα ΧΟΔ), η οποία εισάγει δυσκολία και οικονομικό κόστος κατά τη συντήρηση και τη διαχείρισή τους.
5. Ελλιπής αξιοποίηση εξοπλισμού και μερική ανισοκατανομή στη χρήση κι αξιοποίηση των πόρων του Οργανισμού.
6. Στελέχωση των τομέων που σχετίζονται με τις ΤΠΕ με προσωρινό προσωπικό ή εξωτερικούς συνεργάτες.
7. Μη ικανοποίηση της αρχής της «αναγκαιότητας γνώσης» (need-to-know principle) κατά τον καθορισμό δικαιωμάτων πρόσβασης στα ΠΣ του Οργανισμού.
8. Αυξημένες αρμοδιότητες και φόρτος εργασίας σε συγκεκριμένο προσωπικό, σε συνδυασμό με την απουσία αντικαταστάτη σε περίπτωση απουσίας ή αποχώρησης.
9. Ελλιπής στελέχωση ή ολική απουσία του προσωπικού της Διεύθυνσης Πληροφορικής.
10. Απουσία οργανωτικού σχήματος που αφορά τη διαχείριση της Ασφάλειας ΠΣ.
11. Περιορισμένος βαθμός εναισθητοποίησης και κατάρτισης των χρηστών σε βασικά θέματα ασφάλειας ΠΣ, ιδιαίτερα λόγω της έλλειψης διαδικασιών για την ασφάλεια ΠΣ.
12. Ελλιπής (ή και ασαφής) διαχωρισμός υποχρεώσεων του προσωπικού (segregation of duties).
13. Ανεπαρκής αντιμετώπιση ανεπιθύμητης ηλεκτρονικής αλληλογραφίας.

- 14.Ελλιπής κατάρτιση σημαντικού ποσοστού του προσωπικού στη χρήση των κανόνων που διέπουν τον έλεγχο προσπέλασης.
- 15.Ελλιπής τεκμηρίωση της συμμόρφωσης προς κανονιστικές απαιτήσεις που αφορούν την προστασία δεδομένων προσωπικού χαρακτήρα και την ασφάλεια δεδομένων και πληροφοριακών συστημάτων
- 16.Προβλήματα φυσικής ασφάλειας σε εγκαταστάσεις που στεγάζουν τα ΠΣ.
- 17.Κτιριακές εγκαταστάσεις ευπαθείς και ευάλωτες σε επιθέσεις ειδικής βίας και βανδαλισμούς.

Για την ορθή αντιμετώπιση των αδυναμιών που εντοπίσθηκαν, προτείνεται η υιοθέτηση κατάλληλης πολιτικής ασφάλειας (περιγράφεται στην ενότητα B2), καθώς και η υιοθέτηση συστηματικών και μεθοδικών παρεμβάσεων, εκ μέρους του X, προκειμένου: (α) να αυξηθεί η αποτελεσματικότητα των μέτρων προστασίας που ήδη λαμβάνονται, και (β) να πλαισιωθούν τα υπάρχοντα μέτρα από σειρά επιπρόσθετων, με τελικό στόχο να επιτευχθεί η αναγκαία προστασία των ΠΣ του X, σε βάθος χρόνου.

Η υιοθέτηση της Πολιτικής Ασφάλειας από τη Διοίκηση του X, καθώς και η (σταδιακή, αλλά προγραμματισμένη) λήψη των Μέτρων Προστασίας που προτείνονται εγγυώνται, σύμφωνα με τους κανόνες της Επιστήμης, την κατά νόμο επαρκή προστασία των ΠΣ του X.

Πίνακας περιεχομένων

Περιεχόμενα.....	5
ΠΑΡΑΡΤΗΜΑ.....	184
Επιτελική Σύνοψη Παραδοτέου	184
A1. ΕΙΣΑΓΩΓΗ	189
A1.1 Ένθεση παραδοτέου	189
A1.2 Το ζήτημα της ασφάλειας Πληροφοριακών Συστημάτων	189
A1.3 Αντικείμενο, σκοπός και στόχοι Μελέτης Ασφάλειας	190
A1.4 Δομή παραδοτέου.....	191
A2. Πλαίσιο Μελέτης Ασφάλειας ΠΣ Χ.....	193
A2.1 Εννοιολογικό πλαίσιο.....	193
A2.2 Εξελίξεις, τάσεις και προβληματισμοί	195
A3. Μεθοδολογία Μελέτης Ασφάλειας	200
A3.1 Εισαγωγή.....	200
A4 Ανάλυση Οργανισμού	210
A4.1 Εισαγωγή.....	210
A4.2 Ορισμός Πεδίου Εφαρμογής.....	210
A4.3 Ιστορικό Οργανισμού	210
A4.4 Προσφερόμενες υπηρεσίες	211
A4.5 Διοικητικό και οργανωτικό πλαίσιο	211
A4.6 Διαδικασίες	212
A4.7 Ανάλυση παρούσας κατάστασης.....	217
A4.8 Συμπεράσματα.....	218
A5 Οριοθέτηση έργου	219
A5.1 Μελέτη Ευκαιρίας	219
A5.2 Καθορισμός Πεδίου Εφαρμογής.....	219
A5.3 Προγραμματισμός και Σχεδιασμός Έργου	220
A6 Πληροφορικά Συστήματα και Εγκαταστάσεις Οργανισμού	222
A6.1 Εισαγωγή	222
A6.2 Περιγραφή ΠΣ	222
A6.3 Αποτίμηση ΠΣ και Εγκαταστάσεων Οργανισμού.....	224
A7 Εκτίμηση επικινδυνότητας.....	228
A7.1 Εισαγωγή	228
A7.2 Απειλές και Ευπάθειες-Αδυναμίες	228
A8. Εκτίμηση Επιπτώσεων.....	237
A8.1 Δυνητική Επίπτωση	238
A8.2 Εναπομένουσα Αθροιστική Επίπτωση	240

A8.3 Εκτίμηση Δυνητικής Επικινδυνότητας	242
A8.4 Εκτίμηση Εναπομένουσας Επικινδυνότητας	244
A8.5 Συνολικά αποτελέσματα εκτίμησης επικινδυνότητας.....	246
A9. Διαχείριση επικινδυνότητας – Προτάσεις	248
A9.1 Εισαγωγή.....	248
A9.2 Περιοχές επικινδυνότητας	248
A9.3 Αξιολόγηση επικινδυνότητας.....	249
A9.4 Προτεινόμενο πλάνο ασφάλειας.....	253
A9.5 Πρότυπα Μέτρα Ασφάλειας	253
A10 Εκτίμηση αντιμέτρων	256
A10.1 Προσδιορισμός των αντιμέτρων.....	257
A10.2 Αξιολόγηση Αντιμέτρων.....	259

A1. ΕΙΣΑΓΩΓΗ

A1.1 Ένθεση παραδοτέου

Το παρόν παραδοτέο (ΠΑ-2, “Σχέδιο Ασφάλειας ΠΣ Χ”) εντάσσεται στη δεύτερη και τελευταία Φάση Εργασίας (ΦΕ-2, “Μελέτη Ανάλυσης και Διαχείρισης Επικινδυνότητας”) του έργου “Σχέδιο Ασφάλειας Πληροφοριακών Συστημάτων Χ”.

Η δεύτερη Φάση Εργασίας (ΦΕ-2) είχε ως αντικείμενο την ανάλυση και διαχείριση της επικινδυνότητας (risk analysis and management) των ΠΣ και των εγκαταστάσεων της Χ, όπως αυτά έχουν οριοθετηθεί και περιγραφεί στο παραδοτέο ΠΑ-1 της πρώτης φάσης εργασίας (ΦΕ-1) “Οριοθέτηση Έργου”.

Η ΦΕ-2 κατέληξε στο παρόν παραδοτέο, το οποίο περιλαμβάνει:

- α) τα αποτελέσματα της μελέτης ανάλυσης και διαχείρισης επικινδυνότητας των ΠΣ της Χ,
- β) τα προτεινόμενα **Μέτρα Ασφάλειας** των ΠΣ της Χ,
- γ) την προτεινόμενη **Πολιτική Ασφάλειας** των ΠΣ της Χ.

Η Πολιτική Ασφάλειας και τα Μέτρα Ασφάλειας συναποτελούν το Σχέδιο Ασφάλειας.

A1.2 Το ζήτημα της ασφάλειας Πληροφοριακών Συστημάτων

Η επίτευξη των στόχων ενός οργανισμού εξαρτάται σε μεγάλο βαθμό από τη δυνατότητά του να διασφαλίσει τις υποδομές που είναι απαραίτητες για την αποτελεσματική λειτουργία του. Στους σύγχρονους οργανισμούς, οι Τεχνολογίες Πληροφορικής και Επικοινωνιών αξιοποιούνται για τις περισσότερες από τις ενδοεπιχειρησιακές λειτουργίες και κυρίως για εκείνες που αφορούν την λήψη αποφάσεων και το συντονισμό των μονάδων τους. Με βάση αυτήν τη διαπίστωση προκύπτει ότι το Πληροφοριακό Σύστημα (εφεξής ΠΣ) ενός οργανισμού αποτελεί κρίσιμο στοιχείο της υποδομής του και η αποτελεσματική λειτουργία του συνδέεται άρρηκτα με την αποτελεσματική λειτουργία του ίδιου του οργανισμού.

Η προαναφερθείσα γενική παρατήρηση έχει άμεση εφαρμογή στην περίπτωση της Χ, καθώς υπάρχει σημαντική αναγκαιότητα διασφάλισης των ΠΣ που προκύπτει από:

- την **ποικιλία** και ένταση των κινδύνων που αντιμετωπίζουν τα σύγχρονα ΠΣ,
- τις κανονιστικές απαιτήσεις για προστασία δεδομένων προσωπικού χαρακτήρα,
- το σημαντικό κόστος που ενδέχεται να προκύψει από τυχόν σκόπιμες παραβιάσεις της ασφάλειας καθώς και από ακούσια, τυχαία και φυσικά γεγονότα που απειλούν ένα σύγχρονο ΠΣ.

Η ασφάλεια ενός ΠΣ χαρακτηρίζεται από το πλήθος και την ποικιλομορφία των παραγόντων που πρέπει να ληφθούν υπόψη. Οι παράγοντες αυτοί είναι τόσο τεχνικοί, όσο και διοικητικοί-οργανωτικοί. Για το λόγο αυτό, κάθε προσπάθεια προστασίας ενός ΠΣ πρέπει να λαμβάνει υπόψη τις εξής γενικές διαπιστώσεις:

- Η ασφάλεια των ΠΣ εξαρτάται από πολλούς παράγοντες και δεν είναι ούτε αποκλειστικά, ούτε κυρίως τεχνικό ζήτημα υπό στενή έννοια.
- Η επίτευξη απόλυτης ασφάλειας δεν είναι εφικτός στόχος, σε πραγματικές συνθήκες.
- Για κάθε επίπεδο ασφάλειας υπάρχει ένα αντίστοιχο κόστος που θα πρέπει να καταβληθεί για την επίτευξή του.
- Στο πλαίσιο της αρχής της αναλογικότητας, τα μέτρα προστασίας που θα ληφθούν πρέπει να αντιστοιχούν στο εκάστοτε επίπεδο και τη φύση των κινδύνων που αντιμετωπίζουν τα ΠΣ.

A1.3 Αντικείμενο, σκοπός και στόχοι Μελέτης Ασφάλειας

Σκοπός της παρούσης μελέτης είναι η διατύπωση προς την Χ τεκμηριωμένης πρότασης για την λήψη συγκεκριμένων και επαρκών μέτρων προστασίας των ΠΣ, προς την κατεύθυνση της διασφάλισης της απρόσκοπτης λειτουργίας της. Οι στόχοι της μελέτης παρουσιάζονται συνοπτικά στον Πίνακα A-1.

Στόχοι της Μελέτης Ασφάλειας των ΠΣ της Χ
1. Η καταγραφή και αποτίμηση τόσο των κινδύνων που αντιμετωπίζουν τα ΠΣ και οι εγκαταστάσεις της Χ (συμπεριλαμβανομένων υλικού, λογισμικού, δεδομένων, υλικού τεκμηρίωσης και δικτυακής υποδομής), όσο και των πιθανών επιπτώσεων που είναι δυνατόν να υποστούν τα αγαθά αυτά από ενδεχόμενες κακόβουλες ενέργειες ή από τυχαία γεγονότα.
2. Η μεθοδική επιλογή των κατάλληλων τεχνολογιών, καθώς και των αντίστοιχων τεχνολογικών μέτρων και των οργανωτικών και διαδικαστικών ενεργειών που είναι απαραίτητες για την ασφάλεια των ΠΣ και των εγκαταστάσεων της Χ.
3. Η πρόταση δόκιμης Πολιτικής Ασφάλειας για τα ΠΣ της Χ (κατά την έννοια του Νόμου 2472/97).

Πίνακας 17: Στόχοι της μελέτης ασφάλειας των ΠΣ της Χ

Το έργο καλύπτει συνολικά τα ζητήματα ασφάλειας των ΠΣ. Στο αντικείμενο του έργου περιλαμβάνονται τα μέσα επεξεργασίας πληροφοριών, ηλεκτρονικά και μη, καθώς και όλες οι εγκαταστάσεις που χρησιμοποιούνται για το σκοπό αυτό. Επίσης, το έργο αφορά στην υπάρχουσα τεχνοδιαμόρφωση (configuration) των υπολογιστικών συστημάτων, στις

κτιριακές υποδομές και εγκαταστάσεις της Χ, καθώς και στις εφαρμογές και λειτουργίες που πραγματοποιούνται στο πλαίσιο των ΠΣ.

Οι μελετητές έχουν λάβει υπόψη τους, στο μέτρο του δυνατού, τις προδιαγραφόμενες εξελίξεις, τόσο στον τομέα των Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ), όσο και στην λειτουργία των ΠΣ. Είναι σαφές ότι ενδεχόμενες μείζονες αλλαγές σε μία τουλάχιστον από τις προαναφερθείσες συνιστώσες οδηγούν στην ανάγκη άμεσης αναθεώρησης και επικαιροποίησης του Σχεδίου Ασφάλειας.

Όπως οίκοθεν νοείται, αλλά και όπως συνάγεται από τα ανωτέρω, στους στόχους του έργου δεν περιλαμβάνεται η υλοποίηση της πολιτικής ασφάλειας, ούτε και των μέτρων και διαδικασιών ασφάλειας που θα προταθούν.

Στο πλαίσιο της υλοποίησης των παραπάνω στόχων, για τη μελέτη ανάλυσης και διαχείρισης της επικινδυνότητας των ΠΣ εφαρμόστηκε η *πρότυπη μέθοδος Magerit*. Αναλυτική περιγραφή της Magerit έχει περιληφθεί στο παραδοτέο ΠΑ-1.

Για την επιλογή των προτεινόμενων μέτρων ασφάλειας έχουν ληφθεί υπόψη τα συμπεράσματα της μελέτης ανάλυσης και διαχείρισης επικινδυνότητας και συνεκτιμάται το κόστος υλοποίησής τους, η αποτελεσματικότητά τους, η αντιμετώπιση υπαρκτών κινδύνων, τα ισχύοντα μέτρα ασφάλειας κ.λπ. Με τον τρόπο αυτό διασφαλίζεται ότι δε θα προταθούν πολύπλοκα ή ιδιαίτερα δαπανηρά μέτρα ασφάλειας για την αντιμετώπιση κινδύνων με πολύ χαμηλή ή μηδαμινή πιθανότητα εμφάνισης.

A1.4 Δομή παραδοτέου

Το πρώτο κεφάλαιο εντάσσει το παραδοτέο στο πλαίσιο του έργου, περιγράφει τους **σκοπούς** και τους **στόχους** του, καθώς και τη **δομή** του.

Το δεύτερο κεφάλαιο παρουσιάζει **βασικές έννοιες** και τις **εξελίξεις**, η κατανόηση των οποίων είναι απαραίτητη για την εκπόνηση και την ανάλυση της μελέτης επικινδυνότητας.

Το τρίτο κεφάλαιο παρουσιάζει το **μεθοδολογικό, τεχνικό και οργανωσιακό πλαίσιο** στο οποίο εντάσσεται η μελέτη, καθώς και τη **μεθοδολογία** που ακολούθησε η ομάδα έργου για την εκπόνηση της μελέτης.

Στο τέταρτο κεφάλαιο παρουσιάζεται η ανάλυση του οργανισμού και πιο συγκεκριμένα το ιστορικό, οι προσφερόμενες υπηρεσίες, το διοικητικό και οργανωτικό πλαίσιο, οι διαδικασίες και η **υφιστάμενη κατάσταση**.

Το πέμπτο κεφάλαιο περιλαμβάνει την οριοθέτηση του έργου με τον ορισμό του **πεδίου εφαρμογής**, τον **προγραμματισμό** και το **σχεδιασμό** του έργου.

Στο έκτο κεφάλαιο παρουσιάζονται τα ΠΣ της X, οι εφαρμογές και ο εξοπλισμός που σχετίζονται με αυτό, σε αφαιρετικό αρχιτεκτονικό επίπεδο, καθώς και οι εγκαταστάσεις της.

Το έβδομο κεφάλαιο παρουσιάζει τις [απειλές](#) και τις [ευπάθειες](#) που σχετίζονται με την εταιρεία X, ώστε να χρησιμοποιηθούν κατά την εκτίμηση της επικινδυνότητας.

Το όγδοο κεφάλαιο περιλαμβάνει την εκτίμηση των επιπτώσεων και πιο συγκεκριμένα τη δυνητική και [εναπομένουσα αθροιστική επίπτωση](#), καθώς και την αντίστοιχη επικινδυνότητα.

Στο ένατο κεφάλαιο παρατίθενται οι [προτάσεις](#) της μελετητικής ομάδας για τη [διαχείριση](#) της επικινδυνότητας και τις ενέργειες που απαιτούνται για την αποτελεσματική [εφαρμογή](#) του Σχεδίου Ασφάλειας.

Τέλος, στο δέκατο κεφάλαιο παρουσιάζεται η εκτίμηση των αντιμέτρων με τον προσδιορισμό τους και την αξιολόγησή τους.

Στο πρώτο κεφάλαιο Στο δεύτερο κεφάλαιο παρουσιάζεται η [πολιτική ασφάλειας](#), καθώς και τα [προτεινόμενα μέτρα](#) και διαδικασίες προστασίας/ασφάλειας για τα ΠΣ του ΟΣΕ.

A2. Πλαίσιο Μελέτης Ασφάλειας ΠΣ Χ

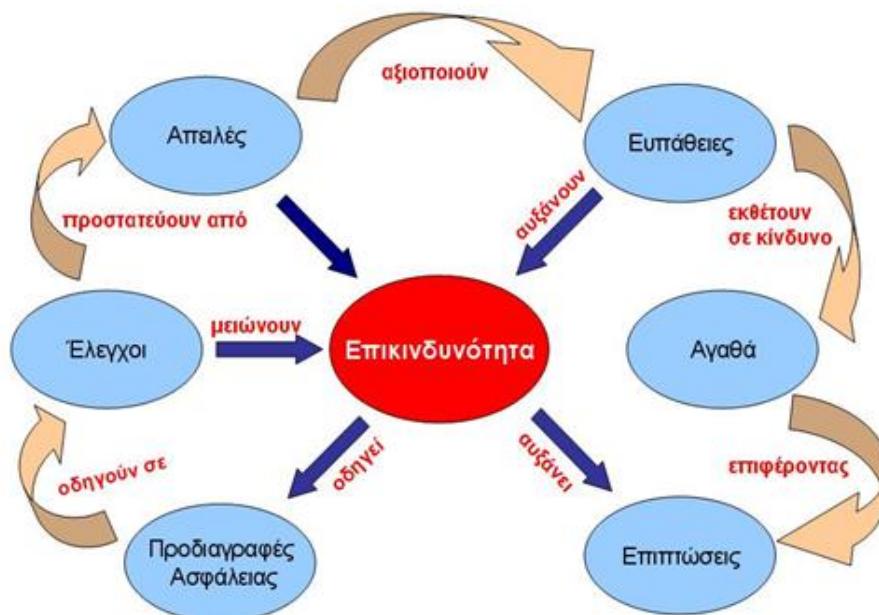
A2.1 Εννοιολογικό πλαίσιο

Η παρούσα μελέτη στηρίζεται σε ένα σαφές εννοιολογικό πλαίσιο, το οποίο αναφέρεται στην ασφάλεια των ΠΣ και των εγκαταστάσεων, κυρίως δε στην ανάλυση και διαχείριση της επικινδυνότητας. Για λόγους πληρότητας του παραδοτέου, οι κεντρικές έννοιες που σχετίζονται με την επικινδυνότητα αναπτύσσονται συνοπτικά στη συνέχεια.

Η ασφάλεια ενός ΠΣ έχει ως στόχο να προστατέψει τα αγαθά που έχουν αξία για τον Οργανισμό, είτε πρόκειται για πληροφορίες είτε για υπολογιστικούς πόρους. Τα τελευταία αναγνωρίζονται ως περιουσιακά στοιχεία ή **Αγαθά** (Assets) και η **αξία** τους είναι ανάλογη της **Επίπτωσης** (Impact) που θα έχει μία πιθανή **Ζημία** (Damage) ή απώλειά τους. Απαραίτητη προϋπόθεση, ώστε να έχουμε μία Απώλεια στα Αγαθά του ΠΣ, είναι να συμβεί **Παραβίαση** (Violation) της Ασφάλειας του. Οι Παραβιάσεις, με τη σειρά τους, προϋποθέτουν την ύπαρξη κάποιας **Αδυναμίας** στο σύστημα και την εμφάνιση σχετικής **Απειλής**.

Συνοψίζοντας, σημειώνουμε ότι μία Απειλή εκμεταλλεύεται μία Αδυναμία του συστήματος και προξενεί Ζημία σε ένα Αγαθό. Το γεγονός αυτό αναγνωρίζεται ως Παραβίαση της Ασφάλειας του Πληροφοριακού Συστήματος και προξενεί Επιπτώσεις στον Οργανισμό, ανάλογες της Αξίας του Αγαθού.

Η **Επικινδυνότητα** (Risk) ενός ΠΣ ορίζεται ως συνάρτηση τριών παραγόντων. Των Απειλών που αντιμετωπίζει το Πληροφοριακό Σύστημα, των Ευπαθειών (ή Αδυναμιών) του και των Επιπτώσεων που θα υπάρξουν από την πραγματοποίηση των Απειλών.



Εικόνα 39: Επικινδυνότητα και συνιστώσες της

Για παράδειγμα, η πυρκαγιά είναι μία Απειλή, η οποία για να εξαπλωθεί χρειάζεται να εκμεταλλευτεί μια αδυναμία, η οποία μπορεί να είναι η ύπαρξη εύφλεκτων υλικών και όταν πραγματοποιηθεί προξενεί βλάβη ή ολική καταστροφή σε ορισμένα Αγαθά του Οργανισμού. Το μέγεθος των συνεπειών που θα έχει η πυρκαγιά είναι ίσο με την Επίπτωση που θα έχει η απώλεια των αντίστοιχων Αγαθών. Η Ανάλυση Επικινδυνότητας αφορά τον προσδιορισμό της Επικινδυνότητας των ΠΣ και την εκτίμηση του μεγέθους της.

Ορισμένες από τις κύριες έννοιες που αφορούν στο παρόν σχέδιο ορίζονται στον πίνακα που ακολουθεί:

ΟΡΟΣ	Ορισμός	
Πληροφοριακό Σύστημα (Information System, IS)	Ένα οργανωμένο σύνολο αλληλεπιδρώντων στοιχείων (άνθρωποι, δεδομένα, λογισμικό, υλικός εξοπλισμός, διαδικασίες), το οποίο επεξεργάζεται δεδομένα και παράγει πληροφορίες για λογαριασμό μίας επιχείρησης ή ενός οργανισμού.	
Αγαθά ή Περιουσιακά Στοιχεία (Assets)	Πληροφορίες, δεδομένα ή υπολογιστικοί πόροι που έχουν αξία, άρα σπουδαιότητα εκφραζόμενη σε χρηματικούς ή άλλους όρους.	
Ασφάλεια Πληροφοριακού Συστήματος (IS Security)	Το οργανωμένο πλαίσιο από έννοιες, αρχές, διαδικασίες, τεχνικές και μέτρα που απαιτούνται, για να προστατεύθονται τόσο τα στοιχεία του ΠΣ όσο και ολόκληρο το ΠΣ από τυχαία ή σκόπιμη απειλή.	
Εγκυρότητα (Validity)	Απόλυτη ακρίβεια και πληρότητα μίας πληροφορίας.	
Ανθεντικότητα (Authenticity)	Αποφυγή ατελειών και ανακριβειών κατά την εξουσιοδοτημένη τροποποίηση μιας πληροφορίας.	
Ακεραιότητα (Integrity)	Αποφυγή μη εξουσιοδοτημένης τροποποίησης μίας πληροφορίας.	Χαρακτηριστικά ασφάλειας ΠΣ
Εμπιστευτικότητα (Confidentiality)	Αποφυγή αποκάλυψης πληροφοριών σε μη εξουσιοδοτημένες οντότητες.	
Διαθεσιμότητα (Availability)	Αποφυγή προσωρινής ή μόνιμης άρνησης διάθεσης της πληροφορίας ή των υπολογιστικών πόρων σε νόμιμα εξουσιοδοτημένους χρήστες.	
Σημείο Ευπάθειας-Αδυναμία (Vulnerability)	Σημείο ενός ΠΣ που μπορεί να επιτρέψει να συμβεί μία παραβίαση.	
Απειλή (Threat)	Μία πιθανή ενέργεια ή ένα γεγονός που μπορεί να προκαλέσει την απώλεια ενός ή περισσότερων χαρακτηριστικών ασφάλειας ενός πληροφοριακού συστήματος.	
Ζημία (Damage)	Η απώλεια, μερική ή ολική, της αξίας ενός αγαθού.	
Παραβίαση (Breach)	Ένα γεγονός το οποίο προσβάλλει μία ή περισσότερες από τις ακόλουθες ιδιότητες: Αυθεντικότητα, διαθεσιμότητα,	

	εμπιστευτικότητα, ακεραιότητα, εγκυρότητα.	
Περιστατικό (Incident)	Ένα γεγονός, το οποίο έχει ως συνέπεια μία παραβίαση ή που αποτελεί μία απόπειρα παραβίασης ή που θέτει σε κίνδυνο την ασφάλεια ενός ΠΣ.	
Επίπτωση (Impact)	Η απώλεια μίας αξίας, η αύξηση του κόστους ή άλλη απώλεια που προκύπτει ως αποτέλεσμα μίας παραβίασης.	
Επικινδυνότητα (Risk)	Συνάρτηση της αξίας ενός αγαθού, της έντασης των απειλών και της σοβαρότητας των αντίστοιχων αδυναμιών.	
Μέσο/μέτρο ασφάλειας /προστασίας (Security Counter-measure)	Ένα μέτρο σχεδιασμένο με σκοπό να εμποδίσει μία παραβίαση ή να μειώσει μία αδυναμία - σημείο ευπάθειας ή να μειώσει τις δυνητικές επιπτώσεις.	
Πολιτική Ασφάλειας (Security Policy)	Περιγραφή, σε γενικό επίπεδο, του συνόλου των κανόνων, των μέτρων και των διαδικασιών που ορίζουν τα φυσικά, διαδικαστικά και προσωπικά μέτρα ασφάλειας, που λαμβάνονται κατά τη διαχείριση, τη διανομή και την προστασία των αγαθών.	
Αυθεντικοποίηση (Authentication)	Η εξακρίβωση της γνησιότητας μίας πληροφορίας ή της γνησιότητας της ταυτότητας ενός χρήστη ή ενός υπολογιστικού συστήματος.	
Ανάδοχος, Συμβατικός συνεργάτης (Partner, Contracted Party)	Φορείς, εταιρείες, οργανισμοί ή φυσικά πρόσωπα με τους οποίους υπήρχαν, υπάρχουν, είτε πρόκειται να υπάρξουν εργασιακές συμβατικές σχέσεις.	

Πίνακας 18: Βασικές έννοιες και ορισμοί

A2.2 Εξελίξεις, τάσεις και προβληματισμοί

Όπως είναι γνωστό, οι σύγχρονες Τεχνολογίες Πληροφορικής και Επικοινωνιών (ΤΠΕ) προσφέρουν σημαντικές δυνατότητες συλλογής, διανομής, επεξεργασίας και παρουσίασης πληροφοριών. Ταυτόχρονα, όμως, η χρήση τους συνεπάγεται έκθεση σε κινδύνους ικανούς να απειλήσουν την αποτελεσματική λειτουργία των ΠΣ και κατά συνέπεια και την εύρυθμη λειτουργία ενός οργανισμού.

Σχετικές έρευνες παρουσιάζουν τους σύγχρονους οργανισμούς και επιχειρήσεις να υφίστανται σημαντικές οικονομικές απώλειες λόγω παραβίασης της ασφάλειας των συστημάτων τους. Για παράδειγμα, τα αποτελέσματα της ετήσιας έρευνας που πραγματοποιεί το CSI (Computer Security Institute) στις ΗΠΑ σχετικά με το κυβερνοεγκλημα (cybercrime) παρουσιάζουν σημαντική αυξητική τάση στις παραβιάσεις ΠΣ. Ενδεικτικά, οι κύριες τάσεις για το 2011 έχουν ως εξής (CSI, 2011):

- Η προσβολή από ιομορφικό λογισμικό παραμένει η πιο «δημοφιλής» απειλή (αναφορά από ποσοστό 67% των ερωτηθέντων).

- Ως σημαντικές απειλές εμφανίζονται η απώλεια ή κλοπή φορητών συσκευών (laptop/mobile devices), η κατάχρηση από εσωτερικούς χρήστες (insiders), πχ. πορνογραφία, πειρατικό λογισμικό κ.λπ., οι επιθέσεις phishing με φαινόμενο αποστολέα τον Οργανισμό, η επίθεση Denial of Service (DoS) και η παρουσία bots στο εταιρικό δίκτυο.
- Περίπου οι μισοί ερωτηθέντες Οργανισμοί ανέφεραν τουλάχιστον ένα περιστατικό ασφάλειας ανά έτος, ενώ τα μισά από αυτά ήταν προϊόν στοχευμένης επίθεσης.
- Η συνεισφορά των απαιτήσεων συμμόρφωσης (νομοθετικό, κανονιστικό και ρυθμιστικό πλαίσιο) στη βελτίωση των προγραμμάτων ασφάλειας αξιολογήθηκε ως θετική.
- Μόλις το 27,5 % αναφέρει τα περιστατικά σε αρμόδιες αρχές.
- Παραπάνω από τους μισούς ερωτηθέντες (ποσοστό 51%) δεν χρησιμοποιούν λύσεις cloud computing, όμως ένα αυξανόμενο ποσοστό αναφέρει ότι όχι μόνο χρησιμοποιεί αυτή τη λύση αλλά έχει και κατάλληλα μέτρα προστασίας.

Οι τάσεις αυτές επιβεβαιώνονται διεθνώς και από άλλες αξιόπιστες έρευνες, όπως η ετήσια έρευνα της Ernst & Young (18th Annual Ernst & Young Global Information Security Survey, 2014). Πιο συγκεκριμένα στη μελέτη αυτή τονίζονται οι ανάγκες για:

- Μελέτη και εκτίμηση της ασφάλειας των Οργανισμών.
- Στελέχωση και υποστήριξη για αλλαγή στην κουλτούρα της ασφάλειας των Οργανισμών.
- Ενημέρωση και αναθεώρηση πολιτικών ασφάλειας, διαδικασιών και υποστηριζόμενων προτύπων.
- Δημιουργία Κέντρου Επιχειρήσεων για την ασφάλεια.
- Δημιουργία και εφαρμογή αντιμέτρων για την κυβερνοασφάλεια.
- Έλεγχος πλάνων συνέχισης εργασιών του Οργανισμού και επανάκαμψης μετά από περιστατικά ασφάλειας.

Γενικά, οι απειλές που αντιμετωπίζει ένα ΠΣ μπορούν να χωριστούν σε δύο κατηγορίες. Η πρώτη αφορά τις κακόβουλες ενέργειες και η δεύτερη τις ακούσιες ζημίες και τα τυχαία γεγονότα. Οι απειλές που αντιμετωπίζει ένα ΠΣ περιλαμβάνουν, μεταξύ άλλων:

- Εισαγωγή κακόβουλου κάθικα - ιομορφικού λογισμικού
- Πλαστή χρήση ταυτότητας νόμιμου χρήστη

- Μη εξουσιοδοτημένη χρήση εφαρμογών
- Κατάχρηση πόρων
- Παρακολούθηση ή/και διήθηση επικοινωνιών
- Σφάλματα χειρισμού και συντήρησης
- Τεχνική αστοχία συστήματος
- Αστοχία λογισμικού
- Κλοπή υλικού
- Δολιοφθορά και εγκλήματα ειδικής βίας
- Απώλεια παροχής ηλεκτρικής ενέργειας
- Φυσικές καταστροφές
- Πυρκαγιά
- Καταστροφή από νερό/πλημμύρα

Η σημαντική ερευνητική δραστηριότητα στον τομέα της Ασφάλειας των ΠΣ τις τελευταίες δύο δεκαετίες έχει προσφέρει ένα σημαντικό αριθμό αποτελεσματικών τεχνικών και προϊόντων ασφάλειας. Οι υπάρχουσες τεχνικές και μηχανισμοί προστασίας μπορούν να προσφέρουν λύσεις στα περισσότερα από τα προβλήματα ασφάλειας που αντιμετωπίζει ένα ΠΣ. Παρά ταύτα, όπως αποδεικνύουν οι συχνές περιπτώσεις παραβίασης της ασφάλειας ακόμη και εξελιγμένων τεχνολογικά συστημάτων, τα τεχνικά μέσα προστασίας δεν αρκούν από μόνα τους, ώστε να εξασφαλίσουν την προστασία ενός ΠΣ. Η απουσία απόλυτα ασφαλών ΠΣ οφείλεται, κυρίως, στους παρακάτω λόγους:

- Στο σημαντικό ρόλο του ανθρώπινου παράγοντα.
- Στον πολυσύνθετο και το δυναμικό χαρακτήρα των απειλών.
- Στον περιορισμό των διαθέσιμων πόρων.

Όπως αναφέρεται στη σχετική βιβλιογραφία, η ανάπτυξη τεχνικών και μηχανισμών ασφάλειας δεν επαρκεί, καθώς το αδύνατο σημείο κάθε ΠΣ παραμένει η παρουσία ανθρώπινων πόρων (χρήστης, χειριστής, σχεδιαστής κ.λπ.). Συνεπώς, η ανάπτυξη ασφαλών ΠΣ θα πρέπει να δίνει βαρύτητα εξίσου στον τεχνικό, όσο και στον ανθρώπινο παράγοντα. Παράλληλα, οι απειλές που αντιμετωπίζει ένα ΠΣ χαρακτηρίζονται από ποικιλία, σύνθετη και συνεχή μεταβλητότητα. Για παράδειγμα, υπάρχουν φυσικές απειλές (π.χ. πυρκαγιά, σεισμός κ.λπ.), απειλές μη εξουσιοδοτημένης πρόσβασης (πχ. cracking), τεχνικές βλάβες,

λανθασμένοι χειρισμοί κ.λπ. Καθώς το τεχνολογικό περιβάλλον εξελίσσεται διαρκώς και με ταχύ ρυθμό και οι απειλές μεταβάλλονται και εξελίσσονται.

Επιπλέον, το κόστος των μέτρων ασφάλειας πρέπει να λαμβάνεται σοβαρά υπόψη. Το κόστος αυτό δεν αφορά μόνο στην προμήθεια και εγκατάσταση μηχανισμών και εργαλείων προστασίας. Συμπεριλαμβάνει το κόστος από τη χρήση πολύτιμων ανθρώπινων πόρων, για εκπαίδευση και ενημέρωση των χρηστών, για λήψη αποφάσεων που αφορούν την ασφάλεια, καθώς και για τη διεκπεραίωση εργασιών και διαδικασιών που αφορούν την ασφάλεια.

Συνοψίζοντας, κάθε προσπάθεια προστασίας ενός ΠΣ θα πρέπει να λαμβάνει υπόψη τις εξής διαπιστώσεις:

- Η ασφάλεια των ΠΣ εξαρτάται από πολλούς παράγοντες και δεν είναι δυνατό να αντιμετωπιστεί μόνο με εμπειρικές μεθόδους.
- Η επίτευξη απόλυτης ασφάλειας δεν είναι εφικτός στόχος, σε πραγματικές συνθήκες.
- Για κάθε επίπεδο ασφάλειας υπάρχει ένα αντίστοιχο κόστος που θα πρέπει να καταβληθεί για την επίτευξή του.
- Τα όποια μέτρα προστασίας ληφθούν θα πρέπει να αντιστοιχούν στην επικινδυνότητα που ενέχεται στη λειτουργία του ΠΣ (αρχή της αναλογικότητας).

Η τελευταία διαπίστωση αναφέρεται στην *αρχή της αναλογικότητας* (proportionality principle), σύμφωνα με την οποία τα μέτρα προστασίας πρέπει να είναι αντίστοιχα των κινδύνων που απειλούν ένα ΠΣ, της πιθανότητας υλοποίησης των απειλών και της σοβαρότητας των αντίστοιχων συνεπειών. Η αναγκαιότητα εφαρμογής της αρχής της αναλογικότητας προκύπτει ως συνέπεια των διαπιστώσεων που διατυπώθηκαν στις προηγούμενες παραγράφους και κατά συνέπεια αποτελεί τεχνική απαίτηση.

Επιπλέον, η λήψη μέτρων ανάλογων προς τους κινδύνους και τις συνέπειες αποτελεί και νομική απαίτηση για κάθε ΠΣ που επεξεργάζεται προσωπικά δεδομένα. Ειδικότερα, τα μέτρα προστασίας "πρέπει να εξασφαλίζουν επίπεδο ασφάλειας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων που είναι αντικείμενο της επεξεργασίας" ([Νόμος 2472/97](#), άρθ. 10, παρ. 3, καθώς και [Κοινοτική Οδηγία 95/46/ΕC](#), άρθ. 17, παρ. 2).

Για τη συμμόρφωση προς αυτή την υποχρέωση είναι απαραίτητη η εφαρμογή μίας μεθοδολογίας που εξασφαλίζει την αναλογικότητα των μέτρων προστασίας σε σχέση με τους πραγματικούς κινδύνους. Η πλέον διαδεδομένη και έγκυρη μεθοδολογία είναι η Ανάλυση και Διαχείριση Επικινδυνότητας. Σύμφωνα με τη μεθοδολογία αυτή, το ζήτημα της ασφάλειας αναλύεται με βάση τους παράγοντες που συνθέτουν την επικινδυνότητά του και ειδικότερα

την αξία των στοιχείων που συνθέτουν το σύστημα, τις απειλές που αυτό αντιμετωπίζει και τις αδυναμίες του.

A3. Μεθοδολογία Μελέτης Ασφάλειας

A3.1 Εισαγωγή

Η Ανάλυση και Διαχείριση Επικινδυνότητας στηρίζεται στην ανάλυση των Απειλών, των Αδυναμιών και των Επιπτώσεων. Είναι φανερό ότι το πλήθος και η ποικιλία των Απειλών που αντιμετωπίζουν τα ΠΣ δεν επιτρέπουν εμπειρική αντιμετώπιση του θέματος. Αν και η εμπειρία και οι ικανότητες του αναλυτή έχουν σημαντική συνεισφορά, ο κίνδυνος παράλειψης ή υποτίμησης μίας απειλής δεν μπορεί να αγνοηθεί. Το ίδιο ισχύει και για τις αδυναμίες του συστήματος.

Επιπλέον, οι συνδυασμοί απειλών και αδυναμιών που θα πρέπει να συνεκτιμηθούν είναι τόσοι, ώστε είναι αδύνατη η ανάλυσή τους χωρίς τη χρήση αυτοματοποιημένου εργαλείου βασισμένου σε λογισμικό. Επίσης, η ορθή επιλογή των αντιμέτρων διευκολύνεται σημαντικά από τη χρήση αυτοματοποιημένου εργαλείου που μπορεί να συνδέει τα προτεινόμενα αντίμετρα με το μέγεθος και τη φύση της Επικινδυνότητας.

Για την Ανάλυση και Διαχείριση Επικινδυνότητας των ΠΣ του Οργανισμού X χρησιμοποιήθηκε η πρότυπη (standard) [μέθοδος Magerit](#). Η μέθοδος Magerit (Crespo et al., 2006) αναπτύχθηκε το 1997 από το Ανώτατο Ισπανικό Συμβούλιο για την Ηλεκτρονική διακυβέρνηση (Consejo Superior de Administración Electrónica). Ο σκοπός της μεθόδου σχετίζεται άμεσα με τη γενικευμένη χρήση των ηλεκτρονικών μέσων. Τα μέσα αυτά δημιουργούν οφέλη, αλλά ταυτόχρονα υπόκεινται σε απειλές και κινδύνους που πρέπει να ελαχιστοποιηθούν με αντίμετρα. Με τον τρόπο αυτό, ενισχύεται η εμπιστοσύνη στη χρήση των μέσων. Αυτή τη στιγμή βρίσκεται στην τρίτη έκδοση με έτος θεώρησης το 2012.

Η μεθοδολογία Magerit αποσκοπεί στα εξής:

- Να αναδείξει την ύπαρξη απειλών, κινδύνων και την ανάγκη έγκαιρης αντιμετώπισής τους.
- Να προσφέρει μια συστηματική μέθοδο ανάλυσης των κινδύνων.
- Να υποβοηθήσει στην περιγραφή και το σχεδιασμό των κατάλληλων μέτρων ελέγχου της επικινδυνότητας.
- Να προετοιμάσει τον Οργανισμό για μία διαδικασία αξιολόγησης (valuation), ελέγχου (auditing) και πιστοποίησης (certification).
- Να επιτύχει ομοιομορφία στις αναφορές που εμπεριέχουν τα ευρήματα και τα συμπεράσματα της ανάλυσης, προτείνοντας μια ενιαία δομή.

Το λογισμικό που υποστηρίζει τη μέθοδο Magerit αποτελεί αναπόσπαστο τμήμα της και ονομάζεται EAR/Pilar. Μέσω του εργαλείου αυτού παρακολουθείται η ορθή βήμα προς βήμα εφαρμογή της μεθόδου, ενώ αποθηκεύονται και ενημερώνονται όλα τα στοιχεία που

συλλέγονται κατά την εφαρμογή της μεθόδου. Το εργαλείο διατέθηκε στην αγορά το 2004 και υποστηρίζεται από τον A.L.H.J. Mañas (Manas, 2009).

Τα στάδια και τα βήματα της μεθόδου παρουσιάζονται συνοπτικά στον Πίνακα A-3 και περιγράφονται λεπτομερώς στη συνέχεια.

Στάδιο	Βήματα σταδίου
1. Προετοιμασία και προγραμματισμός έργου (Preparation & Planning of implementation)	<i>Βήμα 1: Μελέτη σκοπιμότητας Βήμα 2: Καθορισμός πλαισίου αναφοράς Βήμα 3: Προγραμματισμός έργου Βήμα 4: Έναρξη έργου</i>
2. Ανάλυση επικινδυνότητας (Risk analysis)	<i>Βήμα 1: Αναγνώριση και Αποτίμηση Αγαθών Βήμα 2: Χαρακτηρισμός και Εκτίμηση Απειλών Βήμα 3: Χαρακτηρισμός Αντιμέτρων Βήμα 4: Εκτίμηση Επικινδυνότητας</i>
3. Διαχείριση επικινδυνότητας (Risk management)	<i>Βήμα 1: Λήψη αποφάσεων Βήμα 2: Προετοιμασία σχεδίου ασφάλειας Βήμα 3: Υλοποίηση σχεδίου ασφάλειας</i>

Πίνακας 19: Στάδια και βήματα της Magerit και του EAR/Pilar

A3.1.1 Περιγραφή Magerit

Τα βήματα της μεθοδολογίας περιγράφονται σε 3 βιβλία (MAGERIT - Methodology for Information Systems Risk Analysis and Management: Book I-The Method, Book II-The Elements, Book III-The Techniques). Στο πρώτο περιγράφεται αναλυτικά η μεθοδολογία, στο δεύτερο οι κοινοί τύποι αγαθών, τα κριτήρια αξιολόγησής τους, οι τυπικές απειλές και οι βέλτιστες πρακτικές. Τέλος, στο τρίτο βιβλίο παρέχονται βέλτιστες πρακτικές και συμπληρωματικές πληροφορίες για την ανάλυση και διαχείριση επικινδυνότητας.

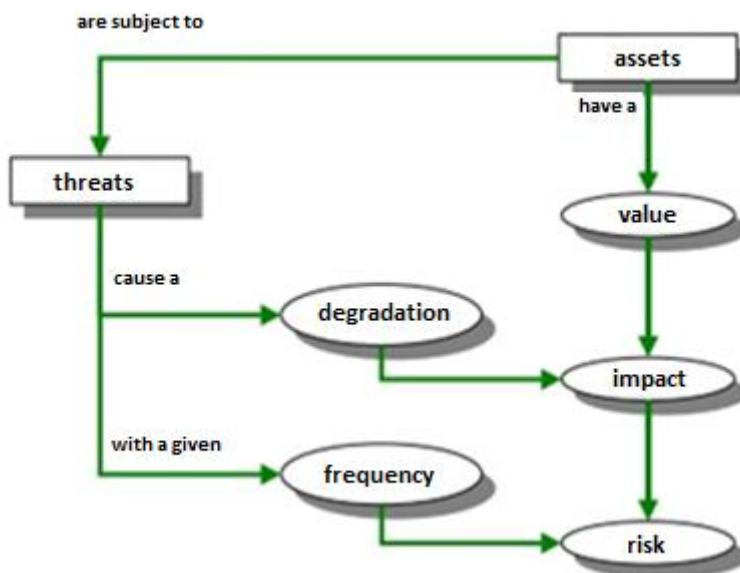
Κατά την έναρξη της μελέτης και κατά την πρώτη σύσκεψη της ομάδας μελέτης με τα καθ' ύλην αρμόδια στελέχη της εταιρίας θα πρέπει:

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

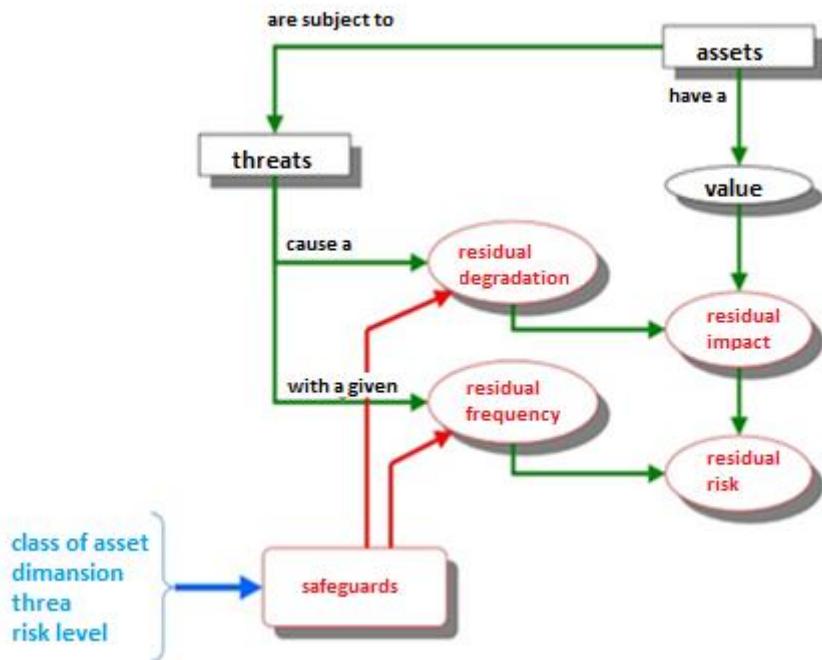
A3.1.2 Βήματα Magerit

Για τον προσδιορισμό του κινδύνου, η μεθοδολογία ακολουθεί τα εξής βήματα:

1. Καθορισμός των σχετικών αγαθών του Οργανισμού, των σχέσεων μεταξύ τους και της αξίας τους (π.χ. ποια ζημία/κόστος θα προκληθεί από την υποβάθμισή τους).
2. Καθορισμός των απειλών στις οποίες είναι εκτεθειμένα τα εν λόγω αγαθά.
3. Καθορισμός των μέσων προστασίας (safeguards) που υπάρχουν και πόσο αποτελεσματικά είναι έναντι του κινδύνου.
4. Εκτίμηση της επίπτωσης (impact), που ορίζεται ως η ζημιά που μπορεί να συμβεί στο αγαθό ως αποτέλεσμα μιας απειλής.
5. Εκτίμηση της επικινδυνότητας, που ορίζεται ως η σταθμισμένη επίπτωση στο ποσοστό εμφάνισης (ή την προσδοκία της εμφάνισης) της απειλής.



Εικόνα 40: Βήματα Magerit (χωρίς safeguards)



Εικόνα 41: Βήματα Magerit (με safeguards)

Για την καλύτερη οργάνωση των αποτελεσμάτων, τα βήματα 1, 2, 4 και 5 εκτελούνται πρώτα, παρακάμπτοντας το βήμα 3, έτσι ώστε αν δεν έχουν αναπτυχθεί μέτρα προστασίας οι οποιεσδήποτε τυχόν εκτιμήσεις των επιπτώσεων και των κινδύνων να είναι δυνητικές. Μόλις αναπτυχθεί αυτό το θεωρητικό σενάριο, τα μέτρα ασφάλειας λαμβάνονται υπόψη στο βήμα 3 παρέχοντας έτσι μία ρεαλιστική εκτίμηση της επίπτωσης των απειλών και του κίνδυνου. Στη συνέχεια, υπολογίζονται εκ νέου τα βήματα 4 και 5.

Τα 5 αυτά λειτουργικά βήματα μπορούν να ομαδοποιηθούν σε τρία βασικά στάδια:

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

A3.1.2.1 Στάδιο 1: Προετοιμασία και Προγραμματισμός Έργου

Η Magerit υλοποιεί ένα σύνολο εργασιών κατά την έναρξή της οι οποίες σχετίζονται με τη συλλογή της απαραίτητης πληροφορίας και το σχεδιασμό του έργου.

Βήμα 1: Αρχικά, πραγματοποιείται μελέτη σκοπιμότητας, κατά την οποία διερευνώνται τα προβλήματα που αντιμετωπίζει ο οργανισμός και τα πιθανά οφέλη που θα προκύψουν από την πραγματοποίηση ενός έργου ανάλυσης και διαχείρισης επικινδυνότητας. Αποτέλεσμα είναι η δημιουργία μίας προκαταρκτικής έκθεσης, η οποία προτείνει τις ενέργειες

προετοιμασίας για τη διεξαγωγή του έργου. Περιέχει μία λίστα θεμάτων όπως τα βασικά επιχειρήματα, λίστα που αφορά θέματα της ασφάλειας των συστημάτων πληροφοριών (π.χ. στρατηγικό σχέδιο δράσης), μία πρώτη προσέγγιση του πεδίου στο οποίο λειτουργεί ο Οργανισμός (π.χ. ανάγκες των μονάδων ή τμημάτων, κατευθύνσεις και τεχνικές διαχείρισης, οργανωτική δομή, τεχνικό περιβάλλον). Η έκθεση αυτή παρουσιάζεται στη διοίκηση του Οργανισμού η οποία λαμβάνει την απόφαση έγκρισης του έργου, αλλαγής στόχων ή καθυστέρησής του.

Βήμα 2: Μετά το πέρας της μελέτης σκοπιμότητας ακολουθεί ο καθορισμός των πλαισίου αναφοράς του έργου. Προσδιορίζονται οι βραχυπρόθεσμοι και μακροπρόθεσμοι στόχοι του έργου καθώς και οι διάφοροι περιορισμοί (π.χ. γεωγραφικοί, χρονικοί, λειτουργικοί κ.ά.) και οι δυσκολίες που θα προκύψουν. Επιπλέον γίνεται εκτίμηση των πόρων που απαιτούνται για την υλοποίηση του έργου (ανθρώπινοι, χρονικοί, οικονομικοί).

Βήμα 3: Έπειτα ακολουθεί ο προγραμματισμός του έργου. Σε αυτό το βήμα καθορίζεται το πλάνο των συνεντεύξεων που θα πραγματοποιηθούν για τη συλλογή πληροφοριών σχετικά με τον Οργανισμό και τον τρόπο λειτουργίας του. Στη συνέχεια, καθορίζεται ποια άτομα θα συμμετέχουν στη διαχείριση, υλοποίηση και συντήρηση του έργου και προσδιορίζονται τα καθήκοντά τους. Ορίζεται επίσης και η κατηγοριοποίηση της πληροφορίας που θα συλλεχθεί από τις συνεντεύξεις. Τέλος, παράγεται το χρονοδιάγραμμα του έργου.

Βήμα 4: Αφού ολοκληρωθούν οι παραπάνω δραστηριότητες, ακολουθεί η διαδικασία έναρξης του έργου. Σε αυτό το βήμα τροποποιούνται και συντάσσονται τα ερωτηματολόγια για τη συλλογή των απαραίτητων πληροφοριών, δημιουργείται ένας κατάλογος με τα αγαθά που πρέπει να προστατευθούν και προσδιορίζονται τα κριτήρια εκτίμησης των αγαθών και των απειλών. Επιπλέον, γίνεται ανάθεση των πόρων που απαιτούνται για τη διεκπεραίωση του έργου, ενώ παράλληλα γνωστοποιείται ο σκοπός και το πλάνο του έργου στους συμμετέχοντες και στους άμεσα εμπλεκόμενους.

Οι εργασίες που περιγράφονται πιο πάνω, ξεκινούν με ένα σύνολο συναντήσεων, συνεχίζουν με συνεντεύξεις και ολοκληρώνονται με τη συμπλήρωση ερωτηματολογίων. Η μεθοδολογία Magerit με το εργαλείο Pilar, παρέχει υψηλή ευελιξία και ένα ευέλικτο κορμό δημιουργίας ερωτηματολογίων. Η μέθοδος επίσης παρέχει οδηγίες για τις συνεντεύξεις και τις διαχωρίζει σε τρεις φάσεις. Η πρώτη φάση χαρακτηρίζεται από χαμηλής προτυποποίησης συνεντεύξεις, ενώ στη δεύτερη φάση και τρίτη φάση, οι συνεντεύξεις και τα ερωτηματολόγια παίρνουν μία πιο δομημένη και αυστηρή μορφή, ώστε να φτάσουμε στα τελικά αποτελέσματα. Το Pilar δίνει τη δυνατότητα ορισμού φάσεων για το έργο. Στο στάδιο της αποτίμησης της επικινδυνότητας, η κατάσταση του έργου αναπαριστάται σε κάθε μία από αυτές παράλληλα.

A3.1.2.2 Στάδιο 2: Ανάλυση Επικινδυνότητας

Το στάδιο αυτό χωρίζεται σε 4 επιμέρους βήματα:

- Αναγνώριση και Αποτίμηση Αγαθών,
- Χαρακτηρισμός και Εκτίμηση Απειλών,
- Χαρακτηρισμός Αντιμέτρων και
- Εκτίμηση Επικινδυνότητας.

Βήμα 1: Αναγνώριση και Αποτίμηση Αγαθών.

Στο στάδιο αυτό, τα αγαθά αναγνωρίζονται σύμφωνα με τις συνεντεύξεις που προηγήθηκαν.

Στη συνέχεια χωρίζονται σε 9 κατηγορίες, οι οποίες παρουσιάζονται στον παρακάτω πίνακα.

	Κατηγορίες αγαθών
Φυσικά Μέσα Αποθήκευσης (Media)	Υπηρεσίες (Services)
Βοηθητικός Εξοπλισμός (Auxiliary equipment)	Δεδομένα/Πληροφορία (Data/Information)
Εγκαταστάσεις Εξοπλισμού (Installations)	Εφαρμογές (Applications/Software)
Προσωπικό (Personel)	Εξοπλισμός (Computer Equipment/Hardware)
	Δίκτυα Επικοινωνιών (Communication networks)

Πίνακας 20: Κατηγοριοποίηση αγαθών στη μέθοδο Magerit

Στη Magerit και στο εργαλείο Pilar δε γίνεται διαχωρισμός υποκατηγοριών όπως γίνεται σε άλλες μεθοδολογίες όπως για παράδειγμα στην CRAMM, αλλά χρησιμοποιείται διαχωρισμός με στρώματα (layers), όπως τα αποκαλεί. Αυτό βοηθά στην αναγνώριση εξαρτήσεων και συσχετίσεων μεταξύ ομάδων αγαθών και διευκολύνει την πρόβλεψη για μία απειλή που αφορά κάποιο αγαθό χαμηλότερης προτεραιότητας. Πριν γίνει η αποτίμηση της αξίας των αγαθών, κατασκευάζεται ένα μοντέλο για το κάθε αγαθό. Στη Magerit αυτό μπορεί να πραγματοποιηθεί και με χρήση XML και ονομάζεται "Μοντέλο Εξάρτησης Αγαθών" (Asset Dependency Model).

Η δημιουργία εξαρτήσεων μεταξύ των αγαθών είναι σημαντική πτυχή της μεθόδου. Πιο συγκεκριμένα, ένα "υψηλότερο αγαθό" λέγεται ότι εξαρτάται από το "χαμηλότερο αγαθό", όταν η εμφάνιση μιας απειλής στο χαμηλότερο αγαθό έχει επίπτωση στο υψηλότερο. Διαισθητικά, θα μπορούσαν να ερμηνευθούν τα χαμηλότερα αγαθά ως οι πυλώνες (pillars) που

στηρίζουν την ασφάλεια των υψηλότερων αγαθών. Το χαρακτηριστικό αυτό της μεθόδου οδήγησε στην ονομασία του εργαλείου που υλοποιεί τη μέθοδο: το εργαλείο EAR/PILAR.

Αφού τα αγαθά αναγνωριστούν και κατηγοριοποιηθούν, η Magerit προχωρά στην αποτίμηση αυτών. Στο σημείο αυτό επιλέγεται προσωπικό το οποίο θεωρείται εξειδικευμένο ως προς τον τύπο του αγαθού. Για την αποφυγή μεγάλων αποκλίσεων στις εκτιμήσεις, γίνεται μία προσπάθεια σύγκλισης των διαφορετικών απόψεων μέσω της διαδικασίας Delphi. Η τεχνική Delphi βασίζεται στην έμμεση αλληλεπίδραση και στη δομημένη επικοινωνία μεταξύ εμπειρογνωμόνων. Ονομάζεται επίσης «επαναλαμβανόμενη συνέντευξη» με την έννοια ότι οι ίδιοι εμπειρογνώμονες απαντούν σε τουλάχιστον δύο ενότητες ερωτήσεων, που πρέπει να είναι σταδιακά περισσότερο δομημένες με βάση τα αποτελέσματα του προηγούμενου γύρου συνεντεύξεων. Αποτέλεσμα είναι η δημιουργία μίας αναφοράς, βάσει του κόστους που θα επιφέρει στην εταιρεία η πιθανή καταστροφή κάθε αγαθού. Στη συνέχεια τα σενάρια μεταφράζονται σε βαθμολογία, βάσει ενός συνόλου κανόνων. Κάθε κανόνας ακολουθεί μία κλίμακα, συνήθως από το μηδέν μέχρι το δέκα.

Βήμα 2: Χαρακτηρισμός και Εκτίμηση Απειλών.

Στο βήμα αυτό εντοπίζονται οι απειλές που αφορούν το κάθε αγαθό και δημιουργείται ένας κατάλογος απειλών. Επίσης υπολογίζεται η συχνότητα με την οποία κάθε απειλή μπορεί να συμβεί για κάθε αγαθό και εκτιμάται η υποτίμηση/υποβάθμιση (degradation) της αξίας ενός αγαθού μετά την πραγματοποίηση κάθε απειλής. Η συχνότητα προσθέτει μια επιπλέον διάσταση στην εξέταση της υποτίμησης/υποβάθμισης των αγαθών, καθώς μια απειλή μπορεί να έχει τρομερές συνέπειες, αλλά είναι πολύ απίθανο να συμβεί. Παράλληλα, μία άλλη απειλή μπορεί να έχει πολύ μικρές συνέπειες, αλλά να είναι τόσο συχνές ώστε να συσσωρεύονται σημαντικές ζημίες. Υπολογίζεται ως ο μέσος αριθμός των εμφανίσεων της απειλής κατά τη διάρκεια μιας συγκεκριμένης περιόδου, συνήθως ετησίως.

Οι απειλές ομαδοποιούνται σε τέσσερις κατηγορίες, όπως φαίνεται στον πίνακα 23.

Κατηγορίες απειλών
Φυσικές καταστροφές
Καταστροφές βιομηχανικής προέλευσης
Λάθη ή Ακούσιες αποτυχίες
Ηθελημένες επιθέσεις

Πίνακας 21: Κατηγοριοποίηση απειλών στη μέθοδο Magerit

Η μεθοδολογία μπορεί να εκτελεστεί είτε με ποιοτικά είτε με ποσοτικά κριτήρια. Σε κάθε μοντέλο, η επίπτωση υπολογίζεται βάσει της τιμής του αγαθού σε πέντε διαστάσεις ή και λιγότερες, οι οποίες αναφέρονται στη συνέχεια. Στο σημείο αυτό σημαντική βοήθεια παρέχει

το εργαλείο Pilar, αφού προσφέρει αυτοματοποιημένο υπολογισμό της πιθανότητας πραγμάτωσης μίας απειλής μέσα από διαφορετικές οπτικές γωνίες (πιθανότητα εμφάνισης, δυνητικότητα, ευκολία, επίπεδο, συχνότητα) και δίνει τη δυνατότητα εμπλουτισμού της υπάρχουσας βάσης του προσθέτοντας γνωστές τρωτότητες με τη μορφή αρχείων XML (CVE's). Οι ευπάθειες αυτές μπορούν να συνδεθούν με τα αντίστοιχα αγαθά που ορίστηκαν στην προηγούμενη φάση. Το Pilar, επίσης, συνυπολογίζει τις συσχετίσεις μεταξύ των αγαθών που αντιμετωπίζουν κοινή απειλή, τη συχνότητα εμφάνισης της απειλής και την υποτίμηση/υποβάθμιση (degradation) που μπορεί να προκύψει στα αγαθά, όπως αυτή ορίζεται από τη Magerit. Η υποτίμηση/υποβάθμιση μετρά τη ζημία που θα προκληθεί αν συμβεί ένα περιστατικό. Η υποτίμηση/υποβάθμιση συχνά περιγράφεται ως μέρος της αξίας του αγαθού και για τη μέτρησή της χρησιμοποιούνται ποιοτικές εκφράσεις. Η τρωτότητα προσδιορίζεται στη Κλίμακα: «Χαμηλή», Μεσαία ή Υψηλή».

Βήμα 3: Χαρακτηρισμός Αντιμέτρων.

Στο βήμα αυτό πραγματοποιείται εντοπισμός των ήδη υπαρχόντων αντιμέτρων κάθε είδους, τα οποία προκύπτουν καθ' όλη τη διάρκεια της μελέτης ενώ εκτιμάται η αποτελεσματικότητά τους. Για την αξιολόγηση των αντιμέτρων, η Magerit ορίζει τη διεξαγωγή συνεντεύξεων και συναντήσεων με τα κατάλληλα άτομα, όπως ακριβώς ορίστηκαν στο βήμα 1.

Τα αντίμετρα αποτιμώνται λαμβάνοντας υπόψη:

- Την καταλληλότητά τους για το σκοπό που υλοποιήθηκαν.
- Την ποιότητα της υλοποίησής τους.
- Την εκπαίδευση των υπεύθυνων για τη διαμόρφωση και την λειτουργία τους.
- Την εκπαίδευση των χρηστών, εφόσον αυτοί έχουν κάποιο ενεργό ρόλο.
- Την ύπαρξη μέτρων ελέγχου για τη μέτρηση της αποτελεσματικότητάς τους.
- Την ύπαρξη διαδικασιών για τακτικές αναθεωρήσεις των αντιμέτρων αυτών.

Από κάθε συνέντευξη, καταγράφεται μία 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 αποτελεσματικότητά τους.

Βήμα 4: Εκτίμηση Επικινδυνότητας.

Η εκτίμηση αυτή προκύπτει από τον προσδιορισμό της ενδεχόμενης και εναπομένουσας επίπτωσης στην οποία το σύστημα υποβάλλεται. Παράλληλα, ταξινομούνται οι προτεραιότητες που αφορούν τα αγαθά ή τις ομάδες αγαθών, με σειρά επίπτωσης ή επικινδυνότητας. Σκοπός αυτού του βήματος είναι ο υπολογισμός της επίπτωσης της επικινδυνότητας και η ερμηνεία των αποτελεσμάτων. Η μεθοδολογία Magerit, καθώς και το

Pilar, υπολογίζει την απομένουσα (residual) συνολική επικινδυνότητα λαμβάνοντας υπόψη τη συσσωρευμένη (accumulated) και την αποκλίνουσα (deflected) επικινδυνότητα. Η επικινδυνότητα που υπολογίζεται για κάθε αγαθό αθροίζεται (aggregated) όταν πληρούνται συγκεκριμένα κριτήρια. Η κλίμακα που χρησιμοποιείται για την αποτίμηση, τόσο της επικινδυνότητας όσο και της επίπτωσης, παίρνει τιμές από το ένα μέχρι το εννέα. Για τον υπολογισμό της επικινδυνότητας μπορούν να χρησιμοποιηθούν προκαθορισμένοι πίνακες ή αλγορίθμική ανάλυση. Το εργαλείο Pilar που υποστηρίζει τη μεθοδολογία, είναι ικανό να την υπολογίσει και ποιοτικά και ποσοτικά.

A3.1.2.3 Στάδιο 3: Διαχείριση Επικινδυνότητας

Η διαχείριση επικινδυνότητας μπορεί να χωριστεί σε 3 επιμέρους βήματα:

- Λήψη αποφάσεων,
- Προετοιμασία σχεδίου ασφάλειας και
- Υλοποίηση του σχεδίου ασφάλειας.

Βήμα 1: Λήψη Αποφάσεων.

Στόχος είναι η κατηγοριοποίηση της επικινδυνότητας σε μια κλίμακα (κρίσιμη, σοβαρή, αξιόλογη ή αποδεκτή). Σε αυτό το βήμα προσδιορίζεται η τιμή της επικινδυνότητας και ταξινομούνται οι επιπτώσεις σε μορφή αναφοράς, περιλαμβάνοντας οδηγίες για την αντιμετώπισή τους. Η διαδικασία αυτή είναι απαραίτητη για την λήψη αποφάσεων που θα πραγματοποιηθεί από τη διοίκηση προκειμένου να αντιμετωπιστούν οι απειλές στις οποίες είναι εκτεθειμένο το σύστημα και να περιοριστούν οι επιπτώσεις τους. Για την κατηγοριοποίηση και αποτίμηση της επικινδυνότητας λαμβάνονται υπόψη διάφοροι παράγοντες από τη διοίκηση του Οργανισμού, όπως για παράδειγμα η σοβαρότητα της επίπτωσης, οι νομικές υποχρεώσεις του Οργανισμού, η επίπτωση στη δημόσια εικόνα του Οργανισμού κ.ά.

Βήμα 2: Προετοιμασία σχεδίου ασφάλειας.

Σκοπός είναι η δημιουργία του πλάνου ασφάλειας του Οργανισμού. Για τη κατάρτιση ενός σχεδίου ασφάλειας θα πρέπει να ληφθούν υπόψη τα σενάρια εκείνα στα οποία οι επιπτώσεις και η επικινδυνότητα βρίσκονται σε κρίσιμο ή σοβαρό επίπεδο. Βάσει των σεναρίων αυτών, θα δημιουργηθεί ένα πλήθος προγραμμάτων ασφάλειας (π.χ. εκτίμηση κόστους, πλάνο αποδοχής, πλάνο λειτουργίας, πλάνο συντήρησης, πλάνο εκπαίδευσης, διαδικασίες ελέγχου απόδοσης και αποτελεσματικότητας) που θα παρέχουν τρόπους αντιμετώπισής τους. Ο τελικός στόχος είναι η υλοποίηση ή βελτίωση μιας σειράς αντιμέτρων τα οποία θα μειώσουν την επίπτωση και την επικινδυνότητα σε επίπεδα αποδεκτά από τη διοίκηση του Οργανισμού.

Αποτέλεσμα της διαδικασίας είναι η δημιουργία ενός τελικού σχεδίου το οποίο θα περιλαμβάνει και θα ενοποιεί όλες τις απαραίτητες ενέργειες, όπως αυτές ορίστηκαν στα επιμέρους σχέδια ασφάλειας που δημιουργήθηκαν.

Βήμα 3: Υλοποίηση του σχεδίου ασφάλειας.

Το βήμα αυτό περιλαμβάνει τις εργασίες που πρέπει να εκτελεστούν για κάθε πρόγραμμα ασφάλειας ξεχωριστά, με σκοπό την υλοποίηση και εφαρμογή του ενιαίου σχεδίου ασφάλειας που έχει καθοριστεί στο προηγούμενο βήμα. Αποτέλεσμα της εφαρμογής του είναι η υλοποίηση των καθορισμένων αντιμέτρων, η δημιουργία KPI'S (key performance indicators) για τη μέτρηση αποτελεσματικότητας, η υιοθέτηση προτύπων, καθώς και η δημιουργία ενημερωμένων μοντέλων επικινδυνότητας για τον Οργανισμό.

A4 Ανάλυση Οργανισμού

A4.1 Εισαγωγή

Η υλοποίηση καινούριων τεχνολογιών στο περιβάλλον εργασίας και η ανάδυση νέων μορφών εργασίας, έχει οδηγήσει στην ολοένα και μεγαλύτερη εξάρτηση των ανθρώπων στον επαγγελματικό τους τομέα από υπολογιστικά συστήματα. Τα συστήματα όμως πάσχουν από τρωτότητες, οι οποίες απειλούν την ασφάλεια τόσο των Οργανισμών, όσο και των ίδιων των εργαζομένων. Η παρούσα μελέτη αναφέρεται στα ΠΣ του Οργανισμού X, στις υπάρχουσες εφαρμογές και αρχεία, καθώς και στις εγκαταστάσεις όπου στεγάζεται σήμερα αυτός και καλύπτει το υλικό, το λογισμικό, τα δεδομένα, τις διαδικασίες και το προσωπικό που απασχολείται σε αυτόν.

A4.2 Ορισμός Πεδίου Εφαρμογής

Το παρόν έγγραφο, αποσκοπεί στην ανάδειξη των σημαντικών περιοχών και την παροχή χρήσιμης πληροφορίας για την αντιμετώπιση και πρόληψη προβλημάτων ασφάλειας. Η πληροφορία απευθύνεται τόσο στη διοίκηση του οργανισμού, όσο και στους ίδιους τους εργαζόμενους, με σκοπό την καλύτερη επιλογή μηχανισμών για τον περιορισμό ή την αντιμετώπιση της επικινδυνότητας.

A4.3 Ιστορικό Οργανισμού

Ο Οργανισμός X δραστηριοποιείται στο αρχιπέλαγος των νησιών Jambelí brava από το 1976. Την περίοδο 1978-1981 ασχολείτο κυρίως με την παραγωγή γαρίδας σε ειδικά διαμορφωμένα ιχθυοτροφία. Από το Μάρτιο του 1983, απόκτησε άδεια για την διεξαγωγή τόσο εσωτερικού, όσο και εξωτερικού εμπορίου. Την περίοδο από το 1982 μέχρι το 1991 ασχολήθηκε αποκλειστικά με την παραγωγή, εξαγωγή και επεξεργασία γαρίδων. Η επεξεργασία της γαρίδας πραγματοποιήθηκε στους ειδικά διαμορφωμένους ιδιόκτητους χώρους του Οργανισμού, που βρίσκονταν στο νοτιοδυτικό δακτύλιο του νησιού, στην περιοχή Pines. Από το 1992 μέχρι σήμερα, ο Οργανισμός έχει αφοσιωθεί αποκλειστικά στην παραγωγή, ενώ έχει σταματήσει την επεξεργασία γαρίδας.

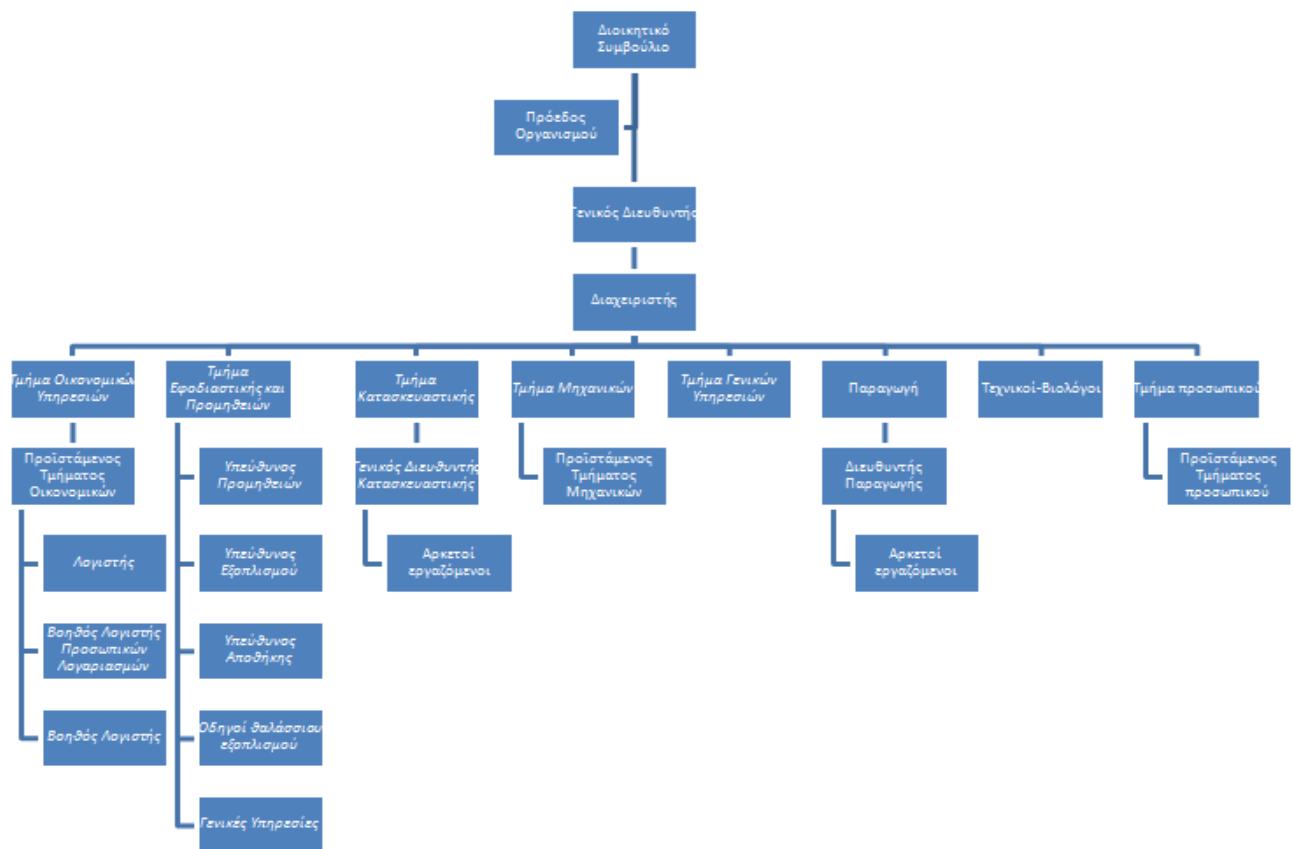
Στόχος του Οργανισμού είναι η συνέχιση της ανοδικής μέχρι τώρα πορείας του, και η αύξηση της απόδοσης των ιχθυοτροφείων του. Μέχρι στιγμής απασχολεί συνολικά 85 άτομα, εκ των οποίων 30 βρίσκονται σε σύμβαση για την παροχή απαραίτητων υπηρεσιών στον Οργανισμό. Ο Οργανισμός έχει πάρει την πιστοποίηση οργανικού και βιολογικού προϊόντος ISO 14024-Type 1 Ecolabel. Ο χώρος όπου στεγάζονται οι εγκαταστάσεις του, φιλοξενεί συνολικά 44 εργαζόμενους.

A4.4 Προσφερόμενες υπηρεσίες

Ο Οργανισμός δραστηριοποιείται στην εκμετάλλευση βιολογικών υδρόβιων ειδών. Ως μέρος των υπηρεσιών που προσφέρει προς τρίτους είναι η εγκατάσταση σταθμών εκκόλαψης και η επεξεργασία και μάρκετινγκ ειδών γαρίδας και άλλων υδρόβιων Οργανισμών. Η κύρια υπηρεσία που παρέχει είναι η παραγωγή γαρίδας και η εξαγωγή της σε χώρες του εξωτερικού και συγκεκριμένα σε χώρες της Αμερικής και της Ευρώπης.

A4.5 Διοικητικό και οργανωτικό πλαίσιο

Η Διοικητική Υπαγωγή των οργανωτικών μονάδων του Οργανισμού X είναι η εξής:



Εικόνα 42: Διοικητική Υπαγωγή των οργανωτικών μονάδων

Μονάδες Υπαγόμενες στη Διοίκηση

1. Τμήμα Οικονομικών Υπηρεσιών- Προϊστάμενος Τμήματος Οικονομικών
 - Λογιστής

- Βοηθός Λογιστής Προσωπικών Λογαριασμών
 - Βοηθός Λογιστής
2. Τμήμα Εφοδιαστικής και Προμηθειών
 - Υπεύθυνος Προμηθειών (COMPRAS)
 - Υπεύθυνος Εξοπλισμού
 - Υπεύθυνος Αποθήκης
 - Οδηγοί Θαλάσσιου Εξοπλισμού
 - Γενικές Υπηρεσίες
 3. Τμήμα Κατασκευαστικής - Γενικός Διευθυντής Κατασκευαστικής
 4. Τμήμα Μηχανικών- Προϊστάμενος Μηχανικών
 5. Τμήμα Γενικών Υπηρεσιών
 6. Τμήμα Παραγωγής -Προϊστάμενος Παραγωγής
 7. Τμήμα Προσωπικού - Προϊστάμενος Τμήματος Προσωπικού
 8. Τεχνικοί-Βιολόγοι

Το οργανόγραμμα του Οργανισμού κρίνεται αρκετά απλουστευμένο. Δεν υπάρχει ξεκάθαρος διαχωρισμός μεταξύ τμημάτων. Οι περισσότεροι προϊστάμενοι βρίσκονται κάτω από την επίβλεψη του γενικού διευθυντή, χωρίς να υπάρχει όμως ξεκάθαρη δομή για το κομμάτι το οποίο διοικεί ο κάθε ένας. Κρίνεται σκόπιμη η πρόταση αναδιοργάνωσης του οργανογράμματος, τόσο οριζόντια όσο και κάθετα.

A4.6 Διαδικασίες

Οι κύριες περιοχές οι οποίες συμβάλλουν στην επίτευξη των στόχων του Οργανισμού είναι οι εξής:

- Λογιστική διαχείριση
- Οικονομική διαχείριση
- Διαχείριση προσωπικού
- Διαχείριση εφοδιαστικής αλυσίδας και προμηθειών

Η Λογιστική Διαχείριση είναι υπεύθυνη για την εκτέλεση των εξής δραστηριοτήτων:

- Διεξαγωγή των ετήσιων φορολογικών δηλώσεων.
- Παροχή συμβουλών και επιτήρηση των εγγράφων εσωτερικού ελέγχου του Οργανισμού.
- Καταγραφή και τήρηση των λογιστικών βιβλίων του Οργανισμού.

Επιπλέον διεξάγει περιοδικές δραστηριότητες όπως:

- Ζητάει από τον υπεύθυνο (manager) του Οργανισμού εβδομαδιαίες αναφορές.

- Ενημέρωση του αρχείου εγγράφων και των αρχείων της εταιρείας (ανά δεκαπενθήμερο).

Η Οικονομική διαχείριση διεξάγει τις ακόλουθες δραστηριότητες:

- Διαχείριση Ταμειακών Ροών.
- Διαχείριση Τραπεζικών Λογαριασμών.
- Εξουσιοδότηση εντολών Πληρωμής.

Η Διαχείριση προσωπικού εκτελεί τις ακόλουθες δραστηριότητες:

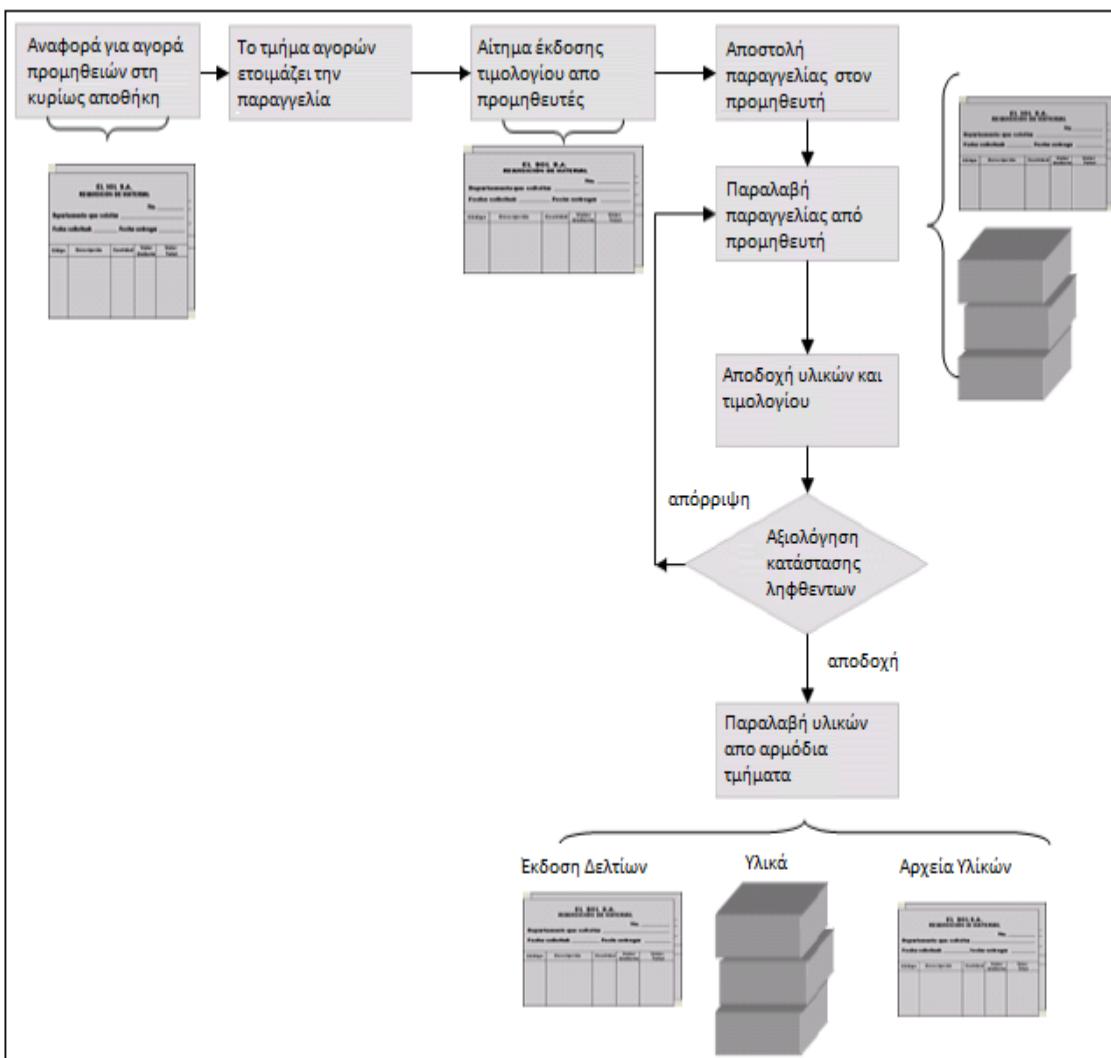
- Χειρισμός μισθοδοσίας για κάθε εργαζόμενο.
- Διαχείριση συμβολαίων εργασίας.
- Συνεργασία με κοινωνικές ασφαλίσεις για κάθε εργαζόμενο.

Η Διαχείριση εφοδιαστικής αλυσίδας και προμηθειών εκτελεί τις ακόλουθες δραστηριότητες:

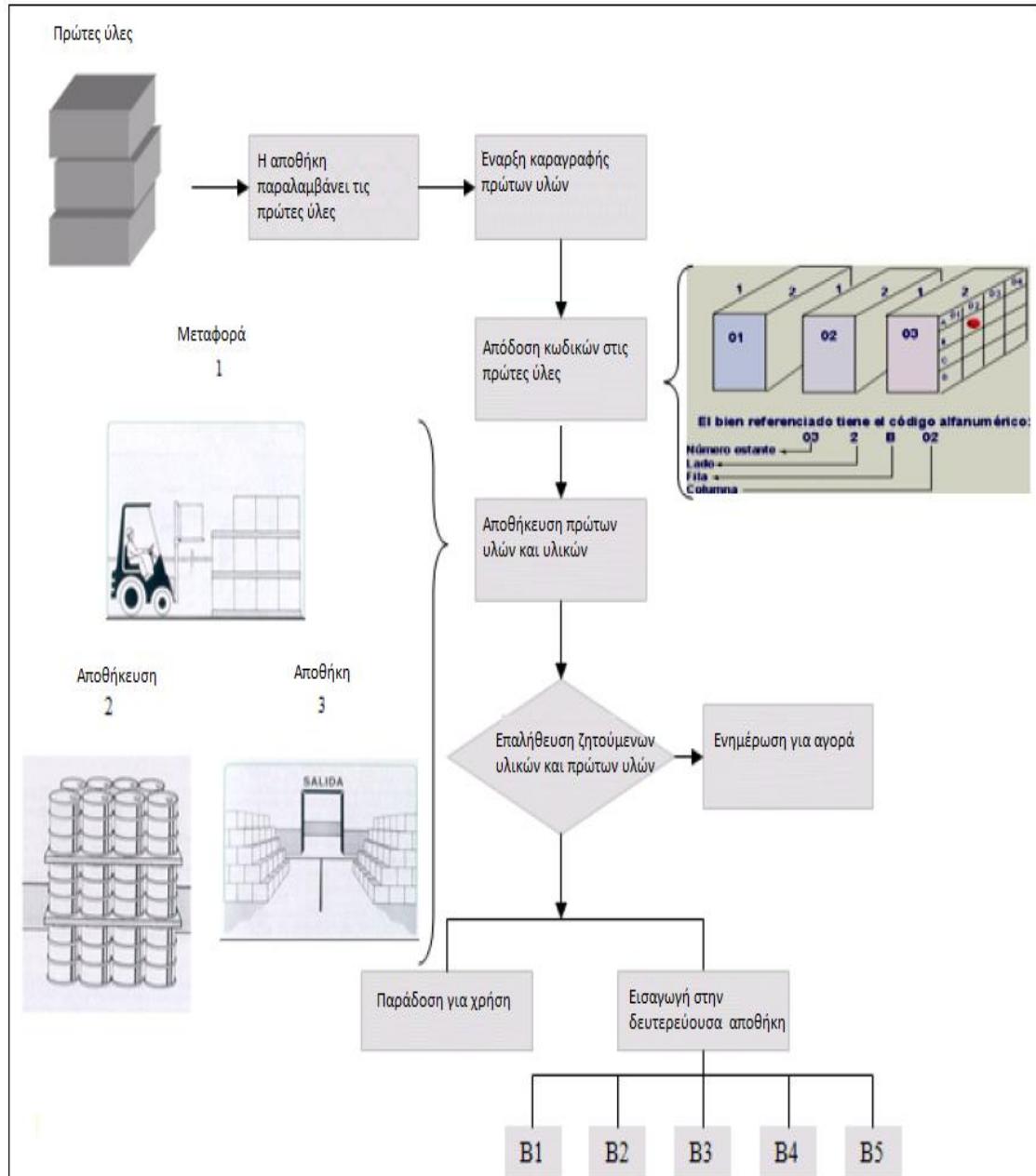
- Είναι υπεύθυνη για συντονισμό των δραστηριοτήτων αλιείας.
- Επικοινωνεί με όλους τους προμηθευτές του Οργανισμού για την αγορά των απαραίτητων υλικών και προμηθειών.

Κάθε εργαζόμενος μια φορά κάθε εργάσιμης ημέρας αποθηκεύει τις πληροφορίες που αφορούν την εργασία του σε ένα CD.

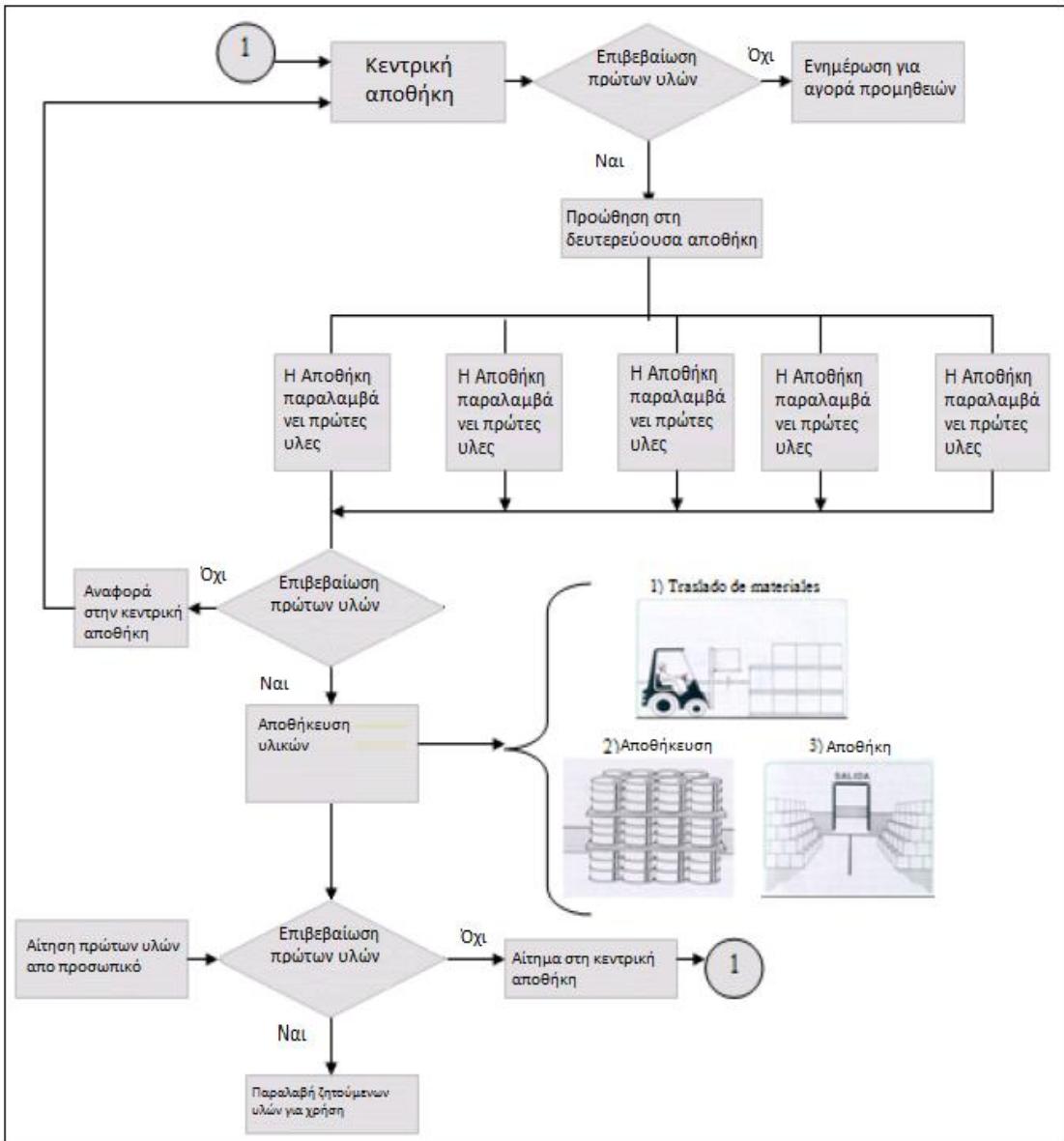
A4.6.1 Λειτουργικές Διαδικασίες



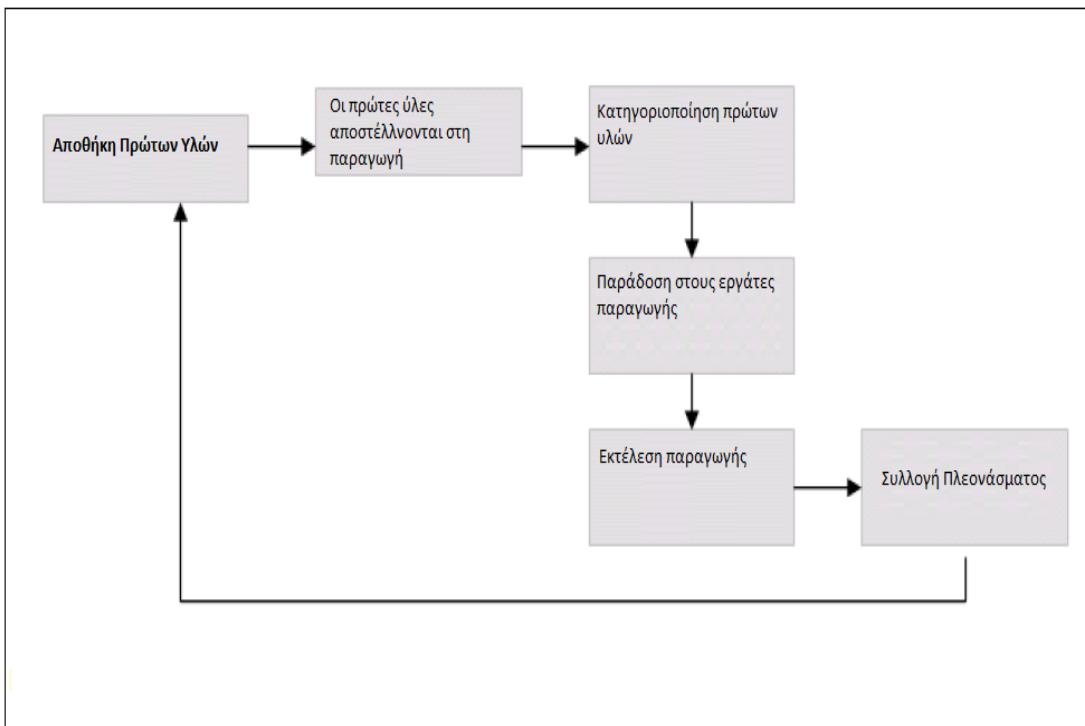
Εικόνα 43: Διαδικασία αγοράς προμηθειών



Εικόνα 44: Διαδικασία αποθήκευσης υλικών στην κυρίως αποθήκη



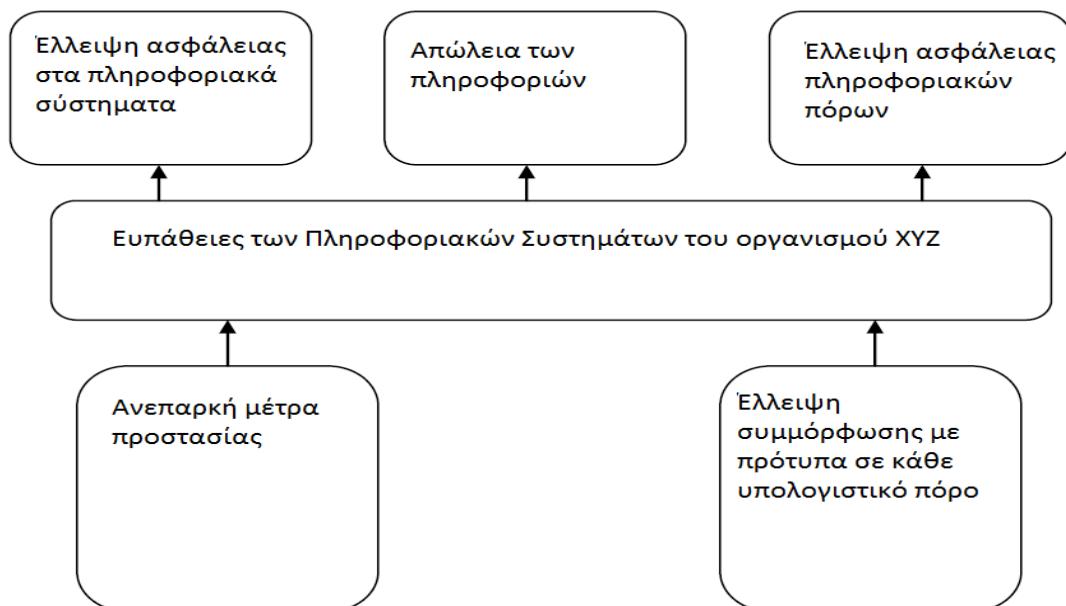
Εικόνα 45: Διαδικασία διαχωρισμού υλικών στην αποθήκη



Εικόνα 46: Διαδικασία χρήσης υλικών στην παράγωγη

A4.7 Ανάλυση παρούσας κατάστασης

Η τρέχουσα κατάσταση του Οργανισμού, κρίνεται ανησυχητική. Δεν εφαρμόζονται στις διαδικασίες του Οργανισμού τα κατάλληλα μέτρα ασφάλειας, γεγονός το οποίο ενδέχεται να επιφέρει σημαντικές συνέπειες σε περίπτωση εκδήλωσης κάποιου περιστατικού.



Εικόνα 47: Υφιστάμενη εικόνα οργανισμού

Στις εγκαταστάσεις του Οργανισμού X, παρουσιάζεται η ύπαρξη αρκετών απειλών, εκδήλωση των οποίων ενδέχεται να επιφέρει σημαντικές επιπτώσεις στην ασφάλειά του. Κύρια αιτία κρίνεται η έλλειψη επαρκών μέτρων ασφάλειας, όπως για παράδειγμα η μη ύπαρξη λογισμικού καταπολέμησης ιομορφικού λογισμικού σε όλους τους υπολογιστές. Επίσης παρατηρείται κατάχρηση των διαδικτυακών υπηρεσιών καθώς δεν υπάρχει περιορισμός πρόσβασης στις σελίδες, με αποτέλεσμα οι υπάλληλοι να μπαίνουν ελεύθερα σε σελίδες κοινωνικής δικτύωσης, ή άλλες σελίδες όπου μπορεί να υπάρξει διαρροή πληροφορίας.

Επιπλέον, η πρόσβαση στο δωμάτιο του κεντρικού υπολογιστή ο οποίος δρα ως ο κύριος εξυπηρετητής για τις εφαρμογές του Οργανισμού, είναι ελεύθερη προς όλο το προσωπικό. Αυτό το κάνει επιρρεπές σε επιθέσεις όπως άρνηση διαθεσιμότητας, απώλεια πληροφορίας, ενώ παράλληλα παρατηρήθηκε και μία γενική έλλειψη μέτρων ασφάλειας και συμμόρφωσης με τα διεθνή πρότυπα ασφάλειας σε όλους του υπολογιστικούς πόρους του Οργανισμού.

Η εγκατάσταση του τοπικού δικτύου (LAN) έχει γίνει εσφαλμένα, και βρίσκεται εκτεθειμένο σε σκόνη, κάτι που μπορεί να προκαλέσει παρεμβολές και θόρυβο στην επικοινωνία μεταξύ των υπολογιστικών πόρων του Οργανισμού.

A4.8 Συμπεράσματα

- Αρκετά ανησυχητικό είναι το γεγονός ότι δεν φαίνεται να έχει διεξαχθεί στο παρελθόν μελέτη επικινδυνότητας βασισμένη σε διεθνή πρότυπα ασφαλείας ΠΣ. Υπάρχει μεγάλη πιθανότητα οι έλεγχοι απειλών και τα μέτρα που έχουν υλοποιηθεί, να μην απευθύνονται σε τρέχουσες απειλές που στοχεύουν ΠΣ.
- Η έρευνα και επιλογή των αντιμέτρων πρέπει να πραγματοποιηθεί μέσα στα πλαίσια ανάλυσης επικινδυνότητας ΠΣ, λαμβάνοντας υπόψη την κρισιμότητα και την προτεραιότητα των πιο σημαντικών αγαθών του Οργανισμού
- Η εφαρμογή της μεθοδολογίας Magerit, θα αποτελέσει βασικό εργαλείο για τον μετριασμό της επικινδυνότητας στον Οργανισμό X, καθώς επίσης και θα βοηθήσει στη συμμόρφωση αυτού με το θεσμικό πλαίσιο περί προστασίας και ασφάλειας ΠΣ.

A5 Οριοθέτηση έργου

Πριν την έναρξη του έργου, πραγματοποιήθηκαν οι εξής ενέργειες:

- Μελέτη ευκαιρίας (opportunity study).
- Καθορισμός πεδίου εφαρμογής (project scope).
- Σχεδιασμός και προγραμματισμός έργου (project planning).

Το έργο θα αναπτυχθεί με τη μεθοδολογία MAGERIT μέσω του εργαλείου Pilar. Για την αποτελεσματική διεξαγωγή του έργου, απαραίτητη είναι η συμμετοχή, συνεργασία και υποστήριξη από όλο το προσωπικό που ασχολείται με τα ΠΣ του Οργανισμού.

A5.1 Μελέτη Ευκαιρίας

Η δραστηριότητα αυτή έχει ως στόχο να προωθήσει την ανάπτυξη του έργου Ανάλυσης και Διαχείρισης Επικινδυνότητας για τον Οργανισμό X.

Ο Οργανισμός, έχει επωφεληθεί από τις δυνατότητες που προσφέρει η τεχνολογία, ειδικά στον τομέα της πληροφορίας και της τηλεπικοινωνίας. Παρόλα αυτά δεν υπάρχει επίγνωση των ζητημάτων ασφάλειας που επιφέρει η εφαρμογή αυτής της τεχνολογίας. Μέσα από τις συνεντεύξεις των εργαζόμενων στο τμήμα προσωπικού, στο τμήμα λογιστικής, στο τμήμα οικονομικών και στο τμήμα εφοδιαστικής αλυσίδας, έγινε ξεκάθαρο ότι υπάρχουν σημαντικές απειλές για την ασφάλεια το Οργανισμού.

Έχει παρατηρηθεί ότι τα συστήματα τα οποία διαχειρίζονται κρίσιμη για τον Οργανισμό πληροφορία μένουν χωρίς συντήρηση, ενώ παράλληλα η πληροφορία αυτή είναι προσπελάσιμη από όλους τους υπαλλήλους. Επίσης τα συστήματα διαχείρισης βάσεων δεδομένων βρίσκονται σε ανασφαλές περιβάλλον, αφού δεν υπάρχει ξεχωριστό δωμάτιο ειδικά σχεδιασμένο για την τοποθέτησή τους.

Επίσης οι κωδικοί πρόσβασης σε κάθε σταθμό εργασίας δεν είναι εμπιστευτικοί, κάτι το οποίο μπορεί να προκαλέσει υποκλοπή πληροφορίας, ενώ το πρόγραμμα προστασίας από ιομορφικό λογισμικό σε όλα τα μηχανήματα δεν είναι ενημερωμένο.

Τέλος το αντίγραφο ασφαλείας το οποίο τηρείται, πρόκειται για μια ξεπερασμένη μορφή, σε CD, τα οποία δεν αποθηκεύονται όπως πρέπει.

A5.2 Καθορισμός Πεδίου Εφαρμογής

Στο σημείο αυτό ορίζονται οι στόχοι του έργου, οι οποίοι αναλύονται σε 3 Φάσεις:

- Στο καθορισμό ενός προγράμματος, προσανατολισμένο στην ασφάλεια.

- Στην ανάλυση της τρέχουσας κατάστασης και στην εύρεση των περιοχών επικινδυνότητας.
- Στον έλεγχο των υπαρχόντων μηχανισμών ασφάλειας.

Το έργο επικεντρώνεται στα Τμήματα Λογιστικής, Οικονομικών, Προσωπικού και Εφοδιαστικής.

Οι εργαζόμενοι των διαφορετικών τμημάτων που θα συμμετέχουν στο έργο:

- Marcia Brito - Προϊστάμενος του Τμήματος Οικονομικών.
- Guisella Cobos - Τμήμα Εφοδιαστικής.
- Yolanda Ortega (Λογιστής) - Προϊστάμενος Λογιστηρίου.
- Mercy Pastor (Λογιστής)- Βοηθός Λογιστή.
- Lic. Alessandra Gomez Προϊστάμενος του Τμήματος Προσωπικού.
- Joseph Anchaluisa (Μηχανικός Συστημάτων) - Πρόσωπο υπεύθυνο για τη διατήρηση του συστήματος BIZNET.
- Κάρλος Γκαρσία (Μηχανικός Συστημάτων) - Υπεύθυνος της συντήρησης του εξοπλισμού πληροφορικής.
- Diana Arcaya – Γραμματέας.

A5.3 Προγραμματισμός και Σχεδιασμός Έργου

Για την άντληση περαιτέρω πληροφορίας σχετικά με συστήματα του Οργανισμού, πραγματοποιήθηκαν συνεντεύξεις με κάθε εμπλεκόμενο, με συνολική διάρκεια 7 εργάσιμες ημέρες. Οι συνεντεύξεις βοηθούν στον καθορισμό των περιοχών που πρέπει να εστιάσει το έργο.

Η Ομάδα εκτέλεσης του έργου αποτελείται από τους:

- Karina Gaona

Οι ομάδα χρηστών για την μελέτη των ΠΣ του Οργανισμού, αποτελείται από τους ίδιους τους χρήστες των πληροφοριακών συστημάτων.

Για τη συλλογή της πληροφορίας έγινε προσαρμογή των ενδεικτικών ερωτηματολογίων της μεθοδολογίας Magerit, όπως αυτά βρίσκονται στο βιβλίο 2, “Κατάλογος Στοιχείων”. Τα ερωτηματολόγια βοηθούν στην άντληση πληροφοριών για την εύρεση απειλών, ευπαθειών, πιθανών επιπτώσεων και αντιμέτρων. Από τα ερωτηματολόγια βρέθηκε πως δεν έχει συμβεί κάποιο περιστατικό ασφάλειας μέχρι στιγμής, κάτι που ίσως αποτελεί και την αιτία της ανεπαρκούς ύπαρξης μέτρων προστασίας και μηχανισμών αντιμετώπισης περιστατικών στον Οργανισμό.

Η περιγραφή της μεθοδολογίας Magerit και των σταδίων τα οποία θα ακολουθηθούν για την πραγματοποίηση του έργου έχει γίνει αναλυτικά στο παρόν Κεφάλαιο.

Α6 Πληροφορικά Συστήματα και Εγκαταστάσεις Οργανισμού

A6.1 Εισαγωγή

Στο Κεφάλαιο που ακολουθεί περιγράφονται τα αποτελέσματα της αποτίμησης των δεδομένων που διαχειρίζονται τα ΠΣ του Οργανισμού X, καθώς και των βασικών κτιριακών εγκαταστάσεών του.

A6.2 Περιγραφή ΠΣ

Η μελέτη ασφάλειας αφορά τα ΠΣ που υπάρχουν στον X. Σημειώνεται ότι στον X υπάρχει ένα σύνολο από συστήματα και εφαρμογές. Η μελέτη αφορά το υλικό, το λογισμικό, τα δεδομένα, τις διαδικασίες και το προσωπικό που απασχολείται στο πλαίσιο των ΠΣ. Συγκεκριμένα, το πεδίο που καλύπτει η μελέτη περιλαμβάνει τις εξής κατηγορίες αγαθών, όπως αυτές προκύπτουν σύμφωνα με την επιλεγμένη μεθοδολογία:

[S] Υπηρεσίες (Services)

- [IS] Εσωτερικές Υπηρεσίες (Internal Services):
- [TELF_PIB] Τηλεφωνία
- [INTERNET_PIB] Διαδίκτυο

[SW] Λογισμικό (Software)

- [SW] Εφαρμογές
- [SIS_PIB] BIZNET
- [OFF_PIB] Εφαρμογές γραφείου
- [AV_PIB] Πρόγραμμα Προστασίας από Ιομορφικό Λογισμικό
- [OS_PIB] Λειτουργικό Σύστημα Υπολογιστών
- [OTR_PIB] Λοιπά έτοιμα πακέτα

[HW] Εξοπλισμός (Hardware)

- [SDB_PIB] Εξυπηρετητής της βάσης δεδομένων
- [PRINT_PIB] Μέσα εκτύπωσης
- [PC_PIB] Προσωπικοί υπολογιστές
- [ROUTER_PIB] ROUTER

[Com] Επικοινωνία (Communications)

- [IPPHONE_PIB] Τηλεφωνία IP
- [WIFI_PIB] RED WIFI
- [LAN_PIB] RED LAN

- [IEX_PIB] Διαδίκτυο

[SI] Αποθηκευτικά Μέσα (Media)

- [CD_PIB] CD

[AUX] Βοηθητικός Εξοπλισμός (Auxiliary Equipment)

- [GEN_PIB] Ηλεκτρική γεννήτρια
- [CABLING_PIB] Καλωδίωση εγκαταστάσεων
- [MOB_PIB] Έπιπλα
- [SISVG_PIB] Σύστημα παρακολούθησης
- [ANT_PIB] Κεραίες
- [RAD_PIB] Ραδιόφωνο
- [SAI_PIB] UPS
- [AUXOTR_PIB] Λοιπά βοηθητικά εξαρτήματα

[P] Προσωπικό (personnel)

- [JF_PIB] Προϊστάμενος Τμήματος Οικονομικών
- [DBA_PIB] Συντήρηση BD
- [SP_PIB] Συντήρηση EQ
- [JC_PIB] Προϊστάμενος Τμήματος Λογιστικής
- [JLC_PIB] Προϊστάμενος Τμήματος Εφοδιαστικής και Προμηθειών
- [JP_PIB] Προϊστάμενος Τμήματος Προσωπικού
- [AC_PIB] Βοηθός Λογιστή
- [D_PIB] Γραμματέας

[L] Εγκαταστάσεις (Locations and Installations)

Το κτίριο στο οποίο στεγάζονται τα ΠΣ του X, βρίσκεται στο νοτιοδυτικό δακτύλιο του νησιού, στην περιοχή Pines. Πρόκειται για ένα ισόγειο κτίριο, το οποίο στεγάζει όλα τα συστήματα και τα γραφεία του Οργανισμού. Το κτίριο αυτό διαθέτει ενιαίο κλιματισμό και σύστημα πυρανίχνευσης και πυρόσβεσης, αλλά όχι σε όλους τους χώρους (π.χ. διαδρόμους), ενώ η πυρόσβεση δεν είναι αυτόματη. Δεν υπάρχει ξεχωριστό Computer Room, αλλά τα συστήματα είναι προσβάσιμα από όλο το προσωπικό.

- [BUILDING_PIB] Κυρίως κτίριο

[D] Δεδομένα:

- [vr] Αρχεία ζωτικής σημασίας (1)
- [Com] Δεδομένα εμπορικού ενδιαφέροντος (2)

- [adm] Δεδομένα διοικητικού ενδιαφέροντος
- [Source] Πηγαίος κώδικας
- [Exe] Αντικείμενο κώδικα
- [Conf] Διαμόρφωση δεδομένων
- [Log] Αρχεία ιστορικού (logs)
- [Test] Δεδομένα δοκιμών
- [per] Προσωπικά δεδομένα (3)
- [A] Υψηλό επίπεδο
- [M] Μέσο επιπέδο
- [B] Βασικό επίπεδο
- [label] Διαβαθμισμένα δεδομένα (4)
- [S] Άκρως Απόρρητο ΕΕ
- [R] Μυστικό ΕΕ
- [C] Εμπιστευτικό ΕΕ
- [DL] Περιορισμένης χρήσης (Restricted) ΕΕ
- [SC] Αταξινόμητα δεδομένα

A6.3 Αποτίμηση ΠΣ και Εγκαταστάσεων Οργανισμού

A6.3.1 Εισαγωγή

Στο Κεφάλαιο αυτό περιγράφονται τα αποτελέσματα της αποτίμησης των δεδομένων που διαχειρίζονται τα ΠΣ της Χ, καθώς και των βασικών κτιριακών εγκαταστάσεών της. Η ακολουθούμενη μεθοδολογία αποδίδει ιδιαίτερη βαρύτητα στα δεδομένα και λιγότερο στο υλικό και λογισμικό, καθώς τα τελευταία μπορούν να αποτιμηθούν με βάση το κόστος αντικατάστασής τους, ενώ τα δεδομένα θα πρέπει να αποτιμηθούν με βάση τις επιπτώσεις της απώλειας των βασικών χαρακτηριστικών ασφάλειας, και πιο συγκεκριμένα την απώλεια της διαθεσιμότητας, της ακεραιότητας και της εμπιστευτικότητας τους.

A6.3.2 Μέθοδος αποτίμησης

Τα δεδομένα αξιολογούνται με βάση τις απόψεις των τελικών χρηστών των πληροφοριών που παρέχουν τα ΠΣ του Οργανισμού. Στο πλαίσιο της ακολουθούμενης μεθοδολογίας, όπως έχει ήδη αναφερθεί, η αποτίμηση δε λαμβάνει υπόψη την πιθανότητα εκδήλωσης μίας απειλής, αλλά μόνο την επίπτωση από την ενδεχόμενη επιτυχή πραγματοποίηση της απειλής αυτής. Η ακρίβεια της αποτίμησης συναρτάται με την ακρίβεια και πληρότητα των

δεδομένων και των σχετικών εκτιμήσεων που κοινοποιήθηκαν στους μελετητές.

Η αξιολόγηση γίνεται αριθμητικά σε κλίμακα [0-10] και οι τιμές που έχουν αποδοθεί προκύπτουν από τους Πίνακες Αποτίμησης που συνοδεύουν τη μέθοδο και το εργαλείο λογισμικού PILAR. Αν οι επιπτώσεις υπάγονται σε περισσότερες από μία από τις κατηγορίες, τότε λαμβάνεται υπόψη η κατηγορία που δίδει το μεγαλύτερο βαθμό.

Σε αυτό το πλαίσιο ζητήθηκε από τα στελέχη της X να περιγράψουν το πιο απαισιόδοξο, κατά την άποψή τους, σενάριο (worst case scenario) για την επίπτωση που θα είχε κάθε ένα από τα παρακάτω ενδεχόμενα (αγνοώντας τα υφιστάμενα μέτρα ασφάλειας):

(α) Απώλεια της διαθεσιμότητας των δεδομένων.

(β) Απώλεια της ακεραιότητας των δεδομένων: μερική, ολική, σκόπιμη αλλοίωση, λάθη μετάδοσης (λανθασμένη δρομολόγηση, άρνηση αποστολής ή λήψης μηνύματος, παρακολούθηση κίνησης, παρεμβολή λανθασμένων μηνυμάτων, μη παράδοση μηνυμάτων, απώλεια ακολουθίας μηνυμάτων).

(γ) Αποκάλυψη των δεδομένων.

A.6.3.3 Αποτελέσματα Αποτίμησης

Κάθε αποτίμηση πρέπει να λαμβάνει υπόψη τα ακόλουθα στοιχεία:

- Διαστάσεις στις οποίες τα υπάρχοντα στοιχεία είναι σχετικά.
- Εκτίμηση της αξίας σε κάθε διάσταση

Επίπεδο	Κριτήριο
10	Επίπεδο 10
9	Επίπεδο 9
8	Επίπεδο 8 (+)
7	Υψηλό
6	Υψηλό (-)
5	Μέτριο (+)
4	Μέτριο
3	Μέτριο (-)
2	Χαμηλό (+)
1	Χαμηλό
0	Αποσβέσιμο

Πίνακας 22: Κριτήρια Αποτίμησης Αγαθών

Διάσταση Ασφαλείας	Χαρακτηριστικό
Διαθεσιμότητα των δεδομένων.	[Δ]
Ακεραιότητα των δεδομένων.	[Ακ]

Εμπιστευτικότητα των δεδομένων.	[Ε]
Αυθεντικοίση των χρηστών και των πληροφοριών.	[Αυθ]
Μη αποτοίση ευθύνης των υπηρεσιών και των δεδομένων.	[ΜηΑ]

Πίνακας 7: Κριτήρια Αποτίμησης Αγαθών

Αγαθά	Διαστάσεις				
	[Δ]	[Ακ]	[Ε]	[Αυθ]	[ΜηΑ]
Εσωτερικές Υπηρεσίες					
Τηλεφωνία	[6]			[7]	[7]
Διαδίκτυο	[8] ¹			[8]	[8]
Εφαρμογές					
Κύρια Εφαρμογή Εταιρείας Χ		[9]	[9]	[9]	[9]
Εφαρμογές Γραφείου					[7]
Πρόγραμμα Προστασίας από Ιούς					[7]
Λειτουργικό Σύστημα					[7]
Άλλο Λογισμικό					[5]
Εξοπλισμός					
Υπηρεσίες Βάσεων Δεδομένων		[9]	[9]	[9]	[9]
Περιφερειακές Συσκευές					[6]
Υπολογιστές Γραφείου					[8]
Δρομολογητές					[8]
Τηλεπικοινωνίες					
Τηλεφωνία		[7]			
Δίκτυο WI FI					[7]
Δίκτυο LAN					[7]
Διαδίκτυο		[7]	[7]		
Επιπρόσθετος Εξοπλισμός					
Καλωδιώσεις	[7] ²				
Έπιπλα	[7]				
Συστήματα Παρακολούθησης	[7]				
Κεραίες	[7]				
Ραδιόφωνο	[7]				
Σύστημα Αδιάλειπτης Παροχής Ηλεκτρικού	[7]				
Άλλος επιπρόσθετος εξοπλισμός	[5]				
Υποστήριξη των Πληροφοριών					
CD		[7]	[7]		
Εγκαταστάσεις					
Κτίριο			[8]		
Προσωπικό					
Επικεφαλής Τμήματος Οικονομικών			[8]		
Συντηρητής Βάσεων Δεδομένων			[7]		
Συντηρητής Εξοπλισμού			[7]		
Επικεφαλής Λογιστηρίου			[8]		
Επικεφαλής Προμηθειών			[8]		
Επικεφαλής Προσωπικού			[8]		
Βοηθός Λογιστή			[7]		

Υπάλληλοι			[6]		
-----------	--	--	-----	--	--

Πίνακας 8: Αποτίμηση Αγαθών

⁽¹⁾ Διαταραχή των εσωτερικών δραστηριοτήτων της εταιρείας X

⁽²⁾ Απώλεια της εμπιστοσύνης (Φήμη)

A7 Εκτίμηση επικινδυνότητας

A7.1 Εισαγωγή

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, και

Πιθανότητα x Επίπτωση = Επικινδυνότητα.

Στο Κεφάλαιο αυτό παρουσιάζονται και αποτιμώνται οι απειλές που αντιμετωπίζουν τα ΠΣ και οι εγκαταστάσεις του X.

Το εργαλείο Pilar έχει δημιουργηθεί σύμφωνα με τη μέθοδο Magerit. Σύμφωνα με τη μέθοδο αυτή, οι απειλές κατατάσσονται σε τέσσερις ομάδες:

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

Ο στόχος αυτού του σταδίου της ανάλυσης είναι ο χαρακτηρισμός του περιβάλλοντος στο οποίο μια απειλή μπορεί να συμβεί, όπου οι συνέπειες είναι πιθανό να περάσουν και στα πρόσωπα. Μπορούμε να συνοψίσουμε το στόχο αυτού του σταδίου στη φράση «γνωρίζω τον εχθρό μου» ("Magerit versión 3 .0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro 1-Método, p. 40)

A7.2 Απειλές και Ευπάθειες-Αδυναμίες

Ο χαρακτηρισμός των απειλών αποτελείται από δύο επιμέρους εργασίες:

- Αναγνώριση των απειλών
- Αποτίμηση των απειλών

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

Αγαθό	Απειλή
Τηλεφωνία	[Ε.1] Λάθη χρηστών

Διαδίκτυο	[A.7] Ακούσια λάθη
BIZNET	[B.5] Φυσική βλάβη ή λογικό λάθος [E.20] Τρωτότητα προγράμματος (λογισμικό) [E.21] Λάθη συντήρησης/ενημέρωσης προγράμματος (λογισμικό) [A.5] Μη εξουσιοδοτημένη πρόσβαση (πλαστοπροσωπία)
Γραφείο	[E.1] Λάθη χρηστών [E.20] Τρωτότητα προγράμματος (λογισμικό) [E.21] Λάθη συντήρησης/ενημέρωσης προγράμματος (λογισμικό) [A.8] Ιομορφικό Λογισμικό
Πρόγραμμα προστασίας από ιούς	[E.8] Ιομορφικό Λογισμικό [E.20] Τρωτότητα προγράμματος (λογισμικό) [E.21] Λάθη συντήρησης/ενημέρωσης προγράμματος (λογισμικό)
Λειτουργικό Σύστημα	[B.5] Φυσική βλάβη ή λογικό λάθος [E.1] Λάθη χρηστών [E.8] Ιομορφικό Λογισμικό [E.20] Τρωτότητα προγράμματος (λογισμικό) [E.21] Λάθη συντήρησης/ενημέρωσης προγράμματος (λογισμικό) [A.7] Ακούσια λάθη
Άλλο Λογισμικό	[E.8] Ιομορφικό Λογισμικό [E.20] Τρωτότητα προγράμματος (λογισμικό) [E.21] Λάθη συντήρησης/ενημέρωσης προγράμματος (λογισμικό)
Σύστημα Βάσεων Δεδομένων	[Φ.1] Φωτιά [Φ.2] Καταστροφές από νερό [Φ.*] Φυσικές Καταστροφές [B.3] Ρύπανση Περιβάλλοντος [B.5] Φυσική βλάβη ή λογικό λάθος [B.7] Συνθήκες θερμοκρασίας ή υγρασίας [E.2] Λάθη διαχειριστή Συστήματος / Ασφάλειας [E.23] Λάθη συντήρησης / αναβάθμισης εξοπλισμού (Υλισμικό) [A.11] Μη εξουσιοδοτημένη πρόσβαση [A.23] Διακίνηση υλικού
Περιφερειακές Συσκευές	[B.5] Φυσική βλάβη ή λογικό λάθος [B.7] Συνθήκες θερμοκρασίας ή υγρασίας [E.23] Λάθη συντήρησης / αναβάθμισης εξοπλισμού (Υλισμικό) [A.11] Μη εξουσιοδοτημένη πρόσβαση
Υπολογιστές Γραφείου	[Φ.2] Καταστροφές από νερό [Φ.*] Φυσικές Καταστροφές [B.*] Βιομηχανικές Καταστροφές [B.5] Φυσική βλάβη ή λογικό λάθος [B.7] Συνθήκες θερμοκρασίας ή υγρασίας [E.23] Λάθη συντήρησης / αναβάθμισης εξοπλισμού (Υλισμικό) [E.24] Εξάντληση πόρων συστήματος

	[A.6] Κατάχρηση προνομίων πρόσβασης [A.7] Ακούσια λάθη
Δρομολογητής	[Φ.1] Φωτιά [Φ.2] Καταστροφές από νερό [Φ.*] Φυσικές Καταστροφές [B.3] Ρύπανση Περιβάλλοντος [B.5] Φυσική βλάβη ή λογικό λάθος [B.7] Συνθήκες θερμοκρασίας ή υγρασίας [A.11] Μη εξουσιοδοτημένη πρόσβαση
Τηλεπικοινωνίες	[B.8] Αποτυχία των υπηρεσιών επικοινωνίας [E.9] Σφάλματα δρομολόγησης [E.15] Τροποποίηση των πληροφοριών [E.19] Διαρροή πληροφοριών [A.7] Ακούσια λάθη [A.9] Δρομολόγηση μηνυμάτων [A.10] Τροποποίηση της ακολουθίας μηνυμάτων [A.12] Ανάλυση της κυκλοφορίας [A.14] Υποκλοπή πληροφοριών
Δίκτυο WI FI	[B.8] Αποτυχία των υπηρεσιών επικοινωνίας [E.9] Σφάλματα δρομολόγησης
Δίκτυο LAN	[B.8] Αποτυχία των υπηρεσιών επικοινωνίας [E.9] Σφάλματα δρομολόγησης [E.10] Λάθη στην ακολουθία των μηνυμάτων [A.5] Μη εξουσιοδοτημένη πρόσβαση (πλαστοπροσωπία) [A.9] Δρομολόγηση μηνυμάτων [A.10] Τροποποίηση της ακολουθίας μηνυμάτων [A.11] Μη εξουσιοδοτημένη πρόσβαση
Διαδίκτυο	[B.8] Αποτυχία των υπηρεσιών επικοινωνίας [E.15] Τροποποίηση των πληροφοριών
Καλωδιώσεις	[B.3] Ρύπανση Περιβάλλοντος [B.7] Συνθήκες θερμοκρασίας ή υγρασίας
Έπιπλα	[B.3] Ρύπανση Περιβάλλοντος
Συστήματα Παρακολούθησης	[B.3] Ρύπανση Περιβάλλοντος [B.7] Συνθήκες θερμοκρασίας ή υγρασίας
Κεραίες	[B.3] Ρύπανση Περιβάλλοντος
Ραδιόφωνο	[B.3] Ρύπανση Περιβάλλοντος
Σύστημα Αδιάλειπτης Παροχής Ηλεκτρικού	[B.3] Ρύπανση Περιβάλλοντος
Άλλος επιπρόσθετος εξοπλισμός	[B.3] Ρύπανση Περιβάλλοντος
CD	[E.15] Τροποποίηση των πληροφοριών [E.19] Εμπρησμός [A.15] Τροποποίηση πληροφοριών [A.19] Αποκάλυψη πληροφοριών
Κτίριο	[Φ.1] Φωτιά [Φ.2] Καταστροφές από νερό [Φ.*.1] Τυφώνας [Φ.*.4] Σεισμός [Φ.*.9] Παλιρροϊκό Κύμα [Φ.*.11] Καύσωνας [B.*] Βιομηχανικές καταστροφές

	[A.27] Εχθρική κατάληψη
Επικεφαλής Τμήματος Οικονομικών	[E.28.1] Ασθένεια [E.28.2] Απεργία [A.29] Εκβιασμός [A.30] Κοινωνική Μηχανική
Συντηρητής Βάσεων Δεδομένων	[E.4] Λάθη στη διαμόρφωση [E.19.3] Επίθεση από αγνώστους
Συντηρητής Εξοπλισμού	[E.4] Λάθη στη διαμόρφωση [E.19.3] Επίθεση από αγνώστους [A.29.2] EK των έσω απειλή
Επικεφαλής Λογιστηρίου	[E.28.1] Ασθένεια [E.28.2] Απεργία [A.29] Εκβιασμός [A.30] Κοινωνική Μηχανική
Επικεφαλής Προμηθειών	[E.28.2] Απεργία [A.29] Εκβιασμός [A.30] Κοινωνική Μηχανική
Επικεφαλής Προσωπικού	[E.28.1] Ασθένεια [E.28.2] Απεργία [A.29] Εκβιασμός
Βοηθός Λογιστή	[E.28.1] Ασθένεια [E.28.2] Απεργία [A.29] Εκβιασμός [A.30] Κοινωνική Μηχανική
Υπάλληλοι	[E.28.1] Ασθένεια [A.29] Εκβιασμός [A.30] Κοινωνική Μηχανική

Πίνακας 9: Απειλές οργανισμού X

Οι στόχοι της αποτίμησης των απειλών είναι:

- Εκτίμηση της πιθανότητας νε 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.

ΠΥ	Πολύ υψηλή
Υ	Υψηλή
Μ	Μέτρια
Χ	Χαμηλή
ΠΧ	Πολύ χαμηλή
Ο	

Πίνακας 10: Υποβάθμιση αξίας αγαθού

Πιθανότητα πραγματοποίησης απειλής [Π]	
ΣΣ	Σχεδόν σίγουρο
ΠΠ	Πολύ πιθανό
Π	Πιθανό

A	Απίθανο
Σ	Σπάνιο
ΠΣ	Πολύ σπάνιο
Ο	

Πίνακας 231: Πιθανότητα πραγματοποίησης απειλής

Αγαθό	Απειλή	[Π]	[Δ]	[Ακ]	[Ε]	[Αυθ]	[ΜηΑ]
Τηλεφωνία	[E.1] Λάθη χρηστών	A	M	-	-	-	-
Διαδίκτυο	[A.7] Ακούσια λάθη	ΠΠ	M	M	M	-	-
BIZNET	[B.5] Φυσική βλάβη ή λογικό λάθος	P	Y	-	-	-	-
	[E.20] Τρωτότητα προγράμματος (λογισμικό)	P	X	M	M	-	-
	[E.21] Λάθη συντήρησης/ενημέρωσης προγράμματος (λογισμικό)	P	X	X	M	-	-
	[A.5] Μη εξουσιοδοτημένη πρόσβαση (πλαστοπροσωπία)	P	Y	A	Y	-	-
Γραφείο	[E.1] Λάθη χρηστών	P	M	M	M	-	-
	[E.20] Τρωτότητα προγράμματος (λογισμικό)	P	M	M	M	-	-
	[E.21] Λάθη συντήρησης/ενημέρωσης προγράμματος (λογισμικό)	P	M	X	-	-	-
	[A.8] Ιομορφικό Λογισμικό	A	X	X	X	-	-
Πρόγραμμα προστασίας από ιούς	[E.8] Ιομορφικό Λογισμικό	A	X	X	X	-	-
	[E.20] Τρωτότητα προγράμματος (λογισμικό)	P	M	M	M	-	-
	[E.21] Λάθη συντήρησης/ενημέρωσης προγράμματος (λογισμικό)	P	M	M	-	-	-

Λειτουργικό Σύστημα	[B.5] Φυσική βλάβη ή λογικό λάθος	Π	M	-	-	-	-
	[E.1] Λάθη χρηστών	A	M	M	M	-	-
	[E.8] Ιομορφικό Λογισμικό	A	X	X	X	-	-
	[E.20] Τρωτότητα προγράμματος (λογισμικό)	Π	X	M	M	-	-
	[E.21] Λάθη συντήρησης/ενημέρωσης προγράμματος (λογισμικό)	Π	M	X	-	-	-
	[A.7] Ακούσια λάθη	Π	X	X	X	-	-
Άλλο Λογισμικό	[E.8] Ιομορφικό Λογισμικό	A	X	X	X	-	-
	[E.20] Τρωτότητα προγράμματος (λογισμικό)	A	X	X	X	-	-
	[E.21] Λάθη συντήρησης/ενημέρωσης προγράμματος (λογισμικό)	A	M	M	-	-	-
Σύστημα Βάσεων Δεδομένων	[Φ.1] Φωτιά	Π	Y	-	-	-	-
	[Φ.2] Καταστροφές από νερό	Π	Y	-	-	-	-
	[Φ.*] Φυσικές Καταστροφές	Π	Y	-	-	-	-
	[B.3] Ρύπανση Περιβάλλοντος	Π	Y	-	-	-	-
	[B.5] Φυσική βλάβη ή λογικό λάθος	Π	Y	-	-	-	-
	[B.7] Συνθήκες Θερμοκρασίας ή υγρασίας	ΠΠ	PY			-	-
	[E.2] Λάθη διαχειριστή Συστήματος / Ασφάλειας	Π	M	M	M	-	-
	[E.23] Λάθη συντήρησης / αναβάθμισης εξοπλισμού (Υλισμικό)	Π	M	-	-	-	-
	[A.11] Μη εξουσιοδοτημένη πρόσβαση	ΠΠ	-	Y	Y	-	-
	[A.23] Διακίνηση υλικού	ΠΠ	Y	-	Y	-	-

Περιφερειακές Συσκευές	[B.5] Φυσική βλάβη ή λογικό λάθος [B.7] Συνθήκες θερμοκρασίας ή υγρασίας [E.23] Λάθη συντήρησης / αναβάθμισης εξοπλισμού (Υλισμικό) [A.11] Μη εξουσιοδοτημένη πρόσβαση	Π Π Π Α	Μ Μ Μ -	- - - Μ	- - - Μ	- - - -	- - - -
Υπολογιστές Γραφείου	[Φ.2] Καταστροφές από νερό [Φ.*] Φυσικές Καταστροφές [Β.*] Βιομηχανικές Καταστροφές [B.5] Φυσική βλάβη ή λογικό λάθος [B.7] Συνθήκες θερμοκρασίας ή υγρασίας	A A Π Π Α	M M X M M	- - - - -	- - - - -	- - - - -	- - - - -
	[E.23] Λάθη συντήρησης / αναβάθμισης εξοπλισμού (Υλισμικό)	Π	M	-	-	-	-
	[Ε.24] Εξάντληση πόρων συστήματος	Π	M	-	-	-	-
	[Α.6] Κατάχρηση προνομίων πρόσβασης	A	M	M	M	-	-
	[Α.7] Ακούσια λάθη	Π	M	X	M	-	-
	[Φ.1] Φωτιά	A	M	-	-	-	-
	[Φ.2] Καταστροφές από νερό	A	M	-	-	-	-
	[Φ.*] Φυσικές Καταστροφές	A	M	-	-	-	-
	[Β.3] Ρύπανση Περιβάλλοντος	A	M	-	-	-	-
	[B.5] Φυσική βλάβη ή λογικό λάθος	Π	M	-	-	-	-
	[B.7] Συνθήκες θερμοκρασίας ή υγρασίας	Π	M	-	-	-	-
	[A.11] Μη εξουσιοδοτημένη πρόσβαση	A	-	X	X	-	-
Δρομολογητής	[Φ.1] Φωτιά [Φ.2] Καταστροφές από νερό [Φ.*] Φυσικές Καταστροφές [Β.3] Ρύπανση Περιβάλλοντος [B.5] Φυσική βλάβη ή λογικό λάθος [B.7] Συνθήκες θερμοκρασίας ή υγρασίας [A.11] Μη εξουσιοδοτημένη πρόσβαση	A A A A Π Π Α	M M M M M M -	- - - - - - X	- - - - - - X	- - - - - - -	- - - - - - -

Τηλεπικοινωνίες	[B.8] Αποτυχία των υπηρεσιών επικοινωνίας [E.9] Σφάλματα δρομολόγησης [E.15] Τροποποίηση των πληροφοριών [E.19] Διαρροή πληροφοριών [A.7] Ακούσια λάθη [A.9] Δρομολόγηση μηνυμάτων [A.10] Τροποποίηση της ακολουθίας μηνυμάτων [A.12] Ανάλυση της κυκλοφορίας [A.14] Υποκλοπή πληροφοριών	A Π Π Π Π Π Π Π	M - - M - Y - - M M - M - M - Y -	- - M - - - M M - M - - Y -	- - - - - - - - - - - - - -	
Δίκτυο WI FI	[B.8] Αποτυχία των υπηρεσιών επικοινωνίας [E.9] Σφάλματα δρομολόγησης	Π Π	M -	- -	Y -	- -
Δίκτυο LAN	[B.8] Αποτυχία των υπηρεσιών επικοινωνίας [E.9] Σφάλματα δρομολόγησης [E.10] Λάθη στην ακολουθία των μηνυμάτων [A.5] Μη εξουσιοδοτημένη πρόσβαση (πλαστοπροσωπία) [A.9] Δρομολόγηση μηνυμάτων [A.10] Τροποποίηση της ακολουθίας μηνυμάτων [A.11] Μη εξουσιοδοτημένη πρόσβαση	A Π Π Π Π Π A	X - - - M - M - M M - M - M -	- - - - X - - M - M M - M - M - -	- - - - - - - - - - - - -	
Διαδίκτυο	[B.8] Αποτυχία των υπηρεσιών επικοινωνίας	Π	Y M	- -	- -	- -

	[E.15] Τροποποίηση των πληροφοριών	Π	-	-	-	-	-
Καλωδιώσεις	[B.3] Ρύπανση Περιβάλλοντος [B.7] Συνθήκες Θερμοκρασίας ή υγρασίας	A ΠΣ	Y X	X -	-	-	-
Έπιπλα	[B.3] Ρύπανση Περιβάλλοντος	A	M	-	-	-	-
Συστήματα Παρακολούθησης	[B.3] Ρύπανση Περιβάλλοντος [B.7] Συνθήκες Θερμοκρασίας ή υγρασίας	A ΠΠ	M Y	-	-	-	-
Κεραίες	[B.3] Ρύπανση Περιβάλλοντος	A	Y	-	-	-	-
Ραδιόφωνο	[B.3] Ρύπανση Περιβάλλοντος	A	Y	-	-	-	-
Σύστημα Αδιάλειπτης Παροχής Ηλεκτρικού	[B.3] Ρύπανση Περιβάλλοντος	A	M	-	-	-	-
Άλλος επιπρόσθετος εξοπλισμός	[B.3] Ρύπανση Περιβάλλοντος	Π	M	-	-	-	-
CD	[E.15] Τροποποίηση των πληροφοριών [E.19] Εμπρησμός [A.15] Τροποποίηση πληροφοριών [A.19] Αποκάλυψη πληροφοριών	A A A A	- - - -	- X - X	- X - X	- - - -	- - - -
Κτίριο	[Φ.1] Φωτιά [Φ.2] Καταστροφές από νερό [Φ.*.1] Τυφώνας [Φ.*.4] Σεισμός [Φ.*.9] Παλιρροϊκό Κύμα [Φ.*.11] Καύσωνας [Β.*] Βιομηχανικές καταστροφές [Α.27] Εχθρική κατάληψη	Π Π Π Π Π ΠΠ Π Π	Y Y Y M M X X ΠΥ	- - - - - - - - Y	- - - - - - - - -	- - - - - - - - -	- - - - - - - - -
Επικεφαλής	[E.28.1] Ασθένεια	Π	M	-	M	-	-

Τμήματος Οικονομικών	[E.28.2] Απεργία [A.29] Εκβιασμός [A.30] Κοινωνική Μηχανική	A A ΠΠ	X M Y	M - M	- M X	- - -	- - -
Συντηρητής Βάσεων Δεδομένων	[E.4] Λάθη στη διαμόρφωση [E.19.3] Επίθεση από αγνώστους	Π Π	- -	Y Y	- Y	- -	- -
Συντηρητής Εξοπλισμού	[E.4] Λάθη στη διαμόρφωση [E.19.3] Επίθεση από αγνώστους [A.29.2] Εκ των έσω απειλή	Π Π Π	- - M	- Y Y	- - M	- - -	- - -
Επικεφαλής Λογιστηρίου	[E.28.1] Ασθένεια [E.28.2] Απεργία [A.29] Εκβιασμός [A.30] Κοινωνική Μηχανική	Π Α Α ΠΠ	M X M Y	M M - M	M - M X	- - - -	- - - -
Επικεφαλής Προμηθειών	[E.28.2] Απεργία [A.29] Εκβιασμός [A.30] Κοινωνική Μηχανική	Α Α Π	X M ΠΥ	Y - X	- M -	- - -	- - -
Επικεφαλής Προσωπικού	[E.28.1] Ασθένεια [E.28.2] Απεργία [A.29] Εκβιασμός	Π Α Α	M M X	- - M	- M -	- - -	- - -
Βοηθός Λογιστή	[E.28.1] Ασθένεια [E.28.2] Απεργία [A.29] Εκβιασμός [A.30] Κοινωνική Μηχανική	ΠΠ ΠΣ Α Π	M X M M	- - - X	- - M M	- - - -	- - - -
Υπάλληλοι	[E.28.1] Ασθένεια [A.29] Εκβιασμός [A.30] Κοινωνική Μηχανική	Α Α ΠΠ	M M M	M - M	- M M	- - -	- - -

Πίνακας 12: Αξιολόγηση απειλών

Ο βαθμός επικινδυνότητας υπολογίζεται για κάθε συνδυασμό απειλής, αδυναμίας και αγαθού και αποτιμάται σε κλίμακα 0-9. Στον υπολογισμό δε λαμβάνονται υπόψη τα υπάρχοντα αντίμετρα. Η τιμή του βαθμού επικινδυνότητας χρησιμοποιείται για την επιλογή συγκεκριμένων μέτρων προστασίας στα πλαίσια του Σχεδίου Ασφάλειας.

A8. Εκτίμηση Επιπτώσεων

Η εκτίμηση των επιπτώσεων έχει ως στόχο:

- Τον υπολογισμό της δυνητικής επίπτωσης στην οποία υποβάλλεται το σύστημα.
- Τον ορισμό της εναπομένουσας επίπτωσης.

Για τον υπολογισμό της δυνητικής επίπτωσης (potential impact) λαμβάνεται υπόψη η αξία των κρίσιμων για τον Οργανισμό αγαθών και τα αποτελέσματα της αποτίμησης απειλών, χωρίς την εφαρμογή οποιωνδήποτε αντιμέτρων. Η εναπομένουσα επίπτωση (residual impact) υπολογίζεται λαμβάνοντας υπόψη και την αποτελεσματικότητα υπαρχόντων αντιμέτρων.

A8.1 Δυνητική Επίπτωση

Πρόκειται για την έκταση της ζημιάς που προκαλείται από την πραγματοποίηση μιας απειλής. Γνωρίζοντας την αξία των αγαθών και την αποδόμηση που προκαλείται σε αυτά από τις απειλές που τα αφορούν, η δυνητική επίπτωση ορίζεται και ως η άμεση επίπτωση της πραγμάτωσης των απειλών αυτών στο ΠΣ και εντοπίζεται στη:

[Δ] Διαθεσιμότητα

[Ακ] Ακεραιότητα

[Ε] Εμπιστευτικότητα

[Ανθ] Αυθεντικότητα πληροφορίας (authenticity of users and information)

[ΜηΑ] Μη αποποίηση της ευθύνης (accountability of service and data)

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

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

ΑΓΑΘΟ	ΔΙΑΣΤΑΣΕΙΣ				
	Δ	Ακ	Ε	Ανθ	ΜηΑ
Εσωτερικές Υπηρεσίες					
[TELF_PIB] Τηλεφωνία ΙΡ	3				
[INTERNET_PIB] Διαδίκτυο	4	6	6		
Εφαρμογές					
[SIS_PIB] BIZNET		8	8		
[OFF_PIB] Εφαρμογές γραφείου		6	6		

[AV_PIB] Πρόγραμμα προστασίας από ιομορφικό λογισμικό - ANIVIRUS	6	6		
[OS_PIB] Λειτουργικό Σύστημα	7	7		
[OTR_PIB] Λοιπά πακέτα λογισμικού	6	6		
Εξοπλισμός				
[SDB_PIB] Σύστημα Βάσεων Δεδομένων	8	8		
[PRINT_PIB] Περιφερειακές συσκευές	6	6		
[PC_PIB] Προσωπικοί υπολογιστές	6	6		
[ROUTER_PIB] Δρομολογητής	3	3		
Επικοινωνία				
[IPPHONE_PIB] Τηλεφωνία IP	4			
[WIFI_PIB] Δίκτυο WI-FI		6		
[LAN_PIB] Δίκτυο LAN	6	8	6	
[IEX_PIB] Διαδίκτυο	6			
Αποθηκευτικά Μέσα				
[CD_PIB] CD	3	3		
Βοηθητικός Εξοπλισμός				
[CABLING_PIB] Καλωδιώσεις	6			
[MOB_PIB] Έπιπλα	4			
[SISVG_PIB] Συστήματα παρακολούθησης	4			
[ANT_PIB] Κεραίες	4			
[RAD_PIB] Ραδιόφωνο	4			
[SAI_PIB] UPS	1			

[AUXOTR_PIB] Λοιπά βοηθητικά εξαρτήματα	2				
Εγκαταστάσεις					
Κεντρικό Κτίριο		8			
Προσωπικό (personnel)					
[JF_PIB] Προϊστάμενος Τμήματος Οικονομικών	5				
[DBA_PIB] Συντηρητής Βάσεων Δεδομένων	4				
[SP_PIB] Συντηρητής Εξοπλισμού	4				
[JC_PIB] Προϊστάμενος Τμήματος Λογιστικής	7				
[JLC_PIB] Προϊστάμενος Τμήματος Εφοδιαστικής και προμηθειών	5				
[JP_PIB] Προϊστάμενος Τμήματος Προσωπικού	5				
[AC_PIB] Βοηθός Λογιστή	6				
[D_PIB] Γραμματέας	5				

Πίνακας 13: Εκτίμηση επιπτώσεων

A8.2 Εναπομένουσα Αθροιστική Επίπτωση

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

ΑΓΑΘΟ	ΔΙΑΣΤΑΣΕΙΣ				
	Δ	Ακ	Ε	Αυθ	ΜηΑ
Εσωτερικές Υπηρεσίες					
[TELF_PIB] Τηλεφωνία IP	2				
[INTERNET_PIB] Διαδίκτυο	4	5	5		
Εφαρμογές					
[SIS_PIB] BIZNET		5	5		

[OFF_PIB] Εφαρμογές γραφείου	0	0		
[AV_PIB] Πρόγραμμα προστασίας από ιομορφικό λογισμικό - ANTIVIRUS	3	3		
[OS_PIB] Λειτουργικό Σύστημα Υπολογιστών	4	4		
[OTR_PIB] Λοιπά έτοιμα πακέτα	3	3		
Εξοπλισμός				
[SDB_PIB] Εξυπηρετητής της βάσης δεδομένων	3	4		
[PRINT_PIB] Μέσα εκτύπωσης	3	3		
[PC_PIB] Προσωπικοί υπολογιστές	3	5		
[ROUTER_PIB] ROUTER	0	0		
Επικοινωνία				
[IPPHONE_PIB] Τηλεφωνία IP	1			
[WIFI_PIB] RED WI-FI		2		
[LAN_PIB] RED LAN	3	4	3	
[IEX_PIB] Διαδίκτυο	2			
Αποθηκευτικά Μέσα				
[CD_PIB] CD	3	3		
Βοηθητικός Εξοπλισμός				
[CABLING_PIB] Καλωδίωση εγκαταστάσεων	4			
[MOB_PIB] Έπιπλα	0			
[SISVG_PIB] Σύστημα παρακολούθησης	1			
[ANT_PIB] Κεραίες	1			
[RAD_PIB] Ραδιόφωνο	1			

[SAI_PIB] UPS	0				
[AUXOTR_PIB] Λοιπά βοηθητικά εξαρτήματα	1				
Εγκαταστάσεις					
Κεντρικό Κτίριο			5		
Προσωπικό (personnel)					
[JF_PIB] Προϊστάμενος Τμήματος Οικονομικών		2			
[DBA_PIB] Συντήρηση BD		0			
[SP_PIB] Συντήρηση EQ		1			
[JC_PIB] Προϊστάμενος Τμήματος Λογιστικής		2			
[JLC_PIB] Προϊστάμενος Τμήματος Εφοδιαστικής και προμηθειών		0			
[JP_PIB] Προϊστάμενος Τμήματος Προσωπικού		0			
[AC_PIB] Βοηθός Λογιστή		1			
[D_PIB] Γραμματέας		0			

Πίνακας 1424: Εναπομένουσα Αθροιστική Επίπτωση

A8.3 Εκτίμηση Δυνητικής Επικινδυνότητας

Η δυνητική επικινδυνότητα υπολογίζεται λαμβάνοντας υπόψη την αξία των αγαθών και την αποτίμηση των απειλών. Στον υπολογισμό δεν λαμβάνονται υπόψη τα υπάρχοντα αντίμετρα. Η επικινδυνότητα αποτιμάται με τιμές από το 0 μέχρι το 9.

[9]: Επιπέδου 9, [8]: Επιπέδου 8, [7]: Εξαιρετικά κρίσιμη, [6]: Πολύ κρίσιμη, [5]: Κρίσιμη, [4]: Πολύ Υψηλή, [3]: Υψηλή, [2]: Μεσαία, [1]: Χαμηλή, [0]: Αμελητέα

ΑΓΑΘΟ	ΔΙΑΣΤΑΣΕΙΣ				
	Δ	Ακ	Ε	Ανθ	ΜηΑ
Εσωτερικές Υπηρεσίες					
[TELF_PIB] Τηλεφωνία IP	1,8				

[INTERNET_PIB] Διαδίκτυο	4,2	5,4	5,4	5,4	
Εφαρμογές					
[SIS_PIB] BIZNET		6,6	6,6		
[OFF_PIB] Εφαρμογές γραφείου		5,4	5,4		
[AV_PIB] Πρόγραμμα προστασίας από ιομορφικό λογισμικό - ANTIVIRUS		5,4	5,4		
[OS_PIB] Λειτουργικό Σύστημα Υπολογιστών		5,4	5,4		
[OTR_PIB] Λοιπά έτοιμα πακέτα		4,5	4,5		
Εξοπλισμός					
[SDB_PIB] Εξυπηρετητής της βάσης δεδομένων		6,6	6,6		
[PRINT_PIB] Μέσα εκτύπωσης		3,6	3,6		
[ROUTER_PIB] ROUTER		1,8	1,8		
Επικοινωνία					
[IPPHONE_PIB] Τηλεφωνία IP		3,3			
[WIFI_PIB] RED WI-FI			4,5		
[LAN_PIB] RED LAN		4,5	6,6	4,5	
[IEX_PIB] Διαδίκτυο		4,5			
Αποθηκευτικά Μέσα					
[CD_PIB] CD		1,8	1,8		
Βοηθητικός Εξοπλισμός					
[GEN_PIB] Ηλεκτρική γεννήτρια	2,1				
[CABLING_PIB] Καλωδίωση εγκαταστάσεων	4,5				
[MOB_PIB] Έπιπλα	2,4				

[SISVG_PIB] Σύστημα παρακολούθησης	3,3			
[ANT_PIB] Κεραίες	3,3			
[RAD_PIB] Ραδιόφωνο	3,3			
[SAI_PIB] UPS	1,5			
[AUXOTR_PIB] Λοιπά βιοηθητικά εξαρτήματα	2,1			
Εγκαταστάσεις				
Κεντρικό Κτίριο		6,6		
Προσωπικό (personnel)				
[JF_PIB] Προϊστάμενος Τμήματος Οικονομικών		4,8		
[DBA_PIB] Συντήρηση BD		3,3		
[SP_PIB] Συντήρηση EQ		3,3		
[JC_PIB] Προϊστάμενος Τμήματος Λογιστικής		6,0		
[JLC_PIB] Προϊστάμενος Τμήματος Εφοδιαστικής και προμηθειών		3,0		
[JP_PIB] Προϊστάμενος Τμήματος Προσωπικού		3,0		
[AC_PIB] Βοηθός Λογιστή		5,4		
[D_PIB] Γραμματέας		4,8		

Πίνακας 255: Εκτίμηση Δυνητικής Επικινδυνότητας

A8.4 Εκτίμηση Εναπομένουσας Επικινδυνότητας

Συσσωρευμένη Εναπομένουσα Επικινδυνότητα

Η συσσωρευμένη εναπομένουσα επικινδυνότητα δείχνει τη διάχυση της επικινδυνότητας ανάμεσα σε εξαρτώμενα αγαθά.

Όσα αγαθά παρουσιάζουν τιμή μεγαλύτερη του 3, αποτελούν σημείο εστίασης προσοχής με υψηλή επικινδυνότητα.

ΑΓΑΘΟ	ΔΙΑΣΤΑΣΕΙΣ
-------	------------

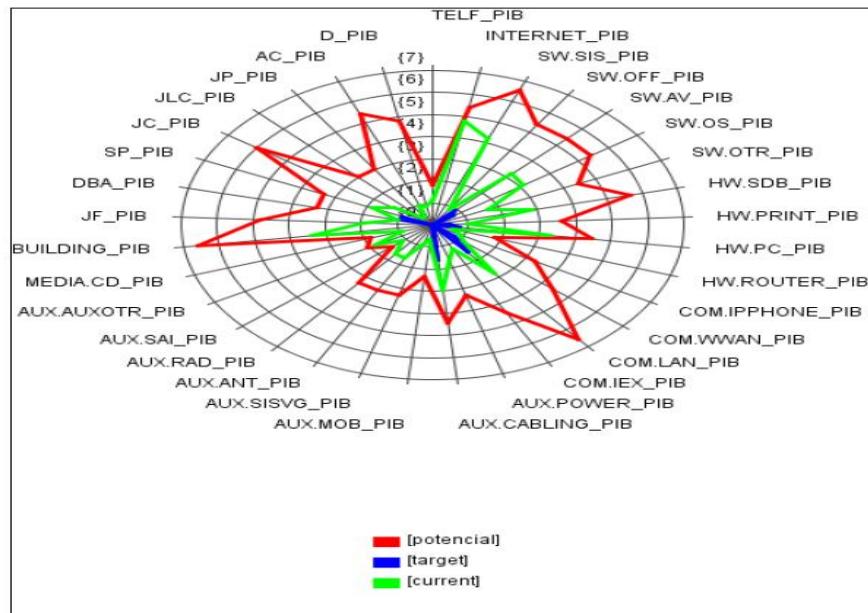
	Δ	Ακ	Ε	Αυθ	ΜηA
Εσωτερικές Υπηρεσίες					
[TELF_PIB] Τηλεφωνία IP	1,1				
[INTERNET_PIB] Διαδίκτυο	4,0	4,8	4,8		
Εφαρμογές					
[SIS_PIB] BIZNET		4,2	4,2		
[OFF_PIB] Εφαρμογές γραφείου		0,83	0,83		
[AV_PIB] Πρόγραμμα προστασίας από ιομορφικό λογισμικό - ANTIVIRUS		3,2	3,2		
[OS_PIB] Λειτουργικό Σύστημα Υπολογιστών		3,1	3,1		
[OTR_PIB] Λοιπά έτοιμα πακέτα		1,7	1,7		
Εξοπλισμός					
[SDB_PIB] Εξυπηρετητής της βάσης δεδομένων		2,1	3.8		
[PRINT_PIB] Μέσα εκτύπωσης		0.95	0.96		
[PC_PIB] Προσωπικοί υπολογιστές		1.7	3.3		
[ROUTER_PIB] ROUTER					
Επικοινωνία					
[IPPHONE_PIB] Τηλεφωνία IP		0,91			
[WIFI_PIB] RED WI-FI			1,1		
[LAN_PIB] RED LAN		2,2	3,5	2,8	
[IEX_PIB] Διαδίκτυο		1,2			
Αποθηκευτικά Μέσα					
[CD_PIB] CD		0,86	0,90		

Βοηθητικός Εξοπλισμός				
[CABLING_PIB] Καλωδίωση εγκαταστάσεων	3,0			
[MOB_PIB] Έπιπλα	0,63			
[SISVG_PIB] Σύστημα παρακολούθησης	0,93			
[ANT_PIB] Κεραίες	1,7			
[RAD_PIB] Ραδιόφωνο	1.7			
[SAI_PIB] UPS	1.1			
[AUXOTR_PIB] Λοιπά βοηθητικά εξαρτήματα	1,8			
Εγκαταστάσεις				
Κεντρικό Κτίριο			3,5	
Προσωπικό (personnel)				
[JF_PIB] Προϊστάμενος Τμήματος Οικονομικών			1,9	
[DBA_PIB] Συντήρηση BD			0,97	
[SP_PIB] Συντήρηση EQ			1,8	
[JC_PIB] Προϊστάμενος Τμήματος Λογιστικής			1,3	
[JLC_PIB] Προϊστάμενος Τμήματος Εφοδιαστικής και προμηθειών			0,42	
[JP_PIB] Προϊστάμενος Τμήματος Προσωπικού			0,42	
[AC_PIB] Βοηθός Λογιστή			0,92	
[D_PIB] Γραμματέας			0,83	

Πίνακας 16 Συσσωρευμένη Εναπονένουσα Επικινδυνότητα

A8.5 Συνολικά αποτελέσματα εκτίμησης επικινδυνότητας

Το ακόλουθο διάγραμμα αναπαριστά την διάχυση της επικινδυνότητας στο σύνολο του Οργανισμού.



Εικόνα 48: Διάχυση Επικινδυνότητας

A9. Διαχείριση επικινδυνότητας – Προτάσεις

A9.1 Εισαγωγή

Η Ανάλυση Επικινδυνότητας παρέχει τη δυνατότητα να εντοπιστούν οι τομείς που απαιτούν την λήψη μέτρων ασφάλειας (αντιμέτρων) και να προσδιοριστεί το επίπεδο προστασίας που απαιτείται. Το σύνολο των Μέτρων Ασφάλειας, σε συνδυασμό με την Πολιτική Ασφάλειας αποτελούν το *Σχέδιο Ασφάλειας*.

Η αποτελεσματικότητα του σχεδίου ασφάλειας προϋποθέτει την πιστή και συνολική εφαρμογή του. Τα αντίμετρα που προτείνονται βρίσκονται σε αλληλεξάρτηση και η αποτελεσματικότητα ενός αντιμέτρου εξαρτάται συχνά και από την υλοποίηση ενός άλλου. Για παράδειγμα, κανένα τεχνικό αντίμετρο δεν πρόκειται να αποδώσει τα αναμενόμενα αποτελέσματα, χωρίς την παράλληλη εφαρμογή ενός κατάλληλου οργανωτικού σχήματος και ενός προγράμματος ευαισθητοποίησης, ενημέρωσης και εκπαίδευσης.

Η επιλογή μόνο των θεωρουμένων “κρίσιμων” ή “άμεσης προτεραιότητας” αντιμέτρων ενέχει σοβαρούς κινδύνους. Για παράδειγμα, θα μπορούσαν να επιλεγούν για υλοποίηση αντίμετρα που αντιστοιχούν στις απειλές που εμφανίζονται πιο συχνά σε αντίστοιχα συστήματα, με βάση απλά στατιστικά δεδομένα. Όμως στην περίπτωση που κάποιος επιθυμεί να προσβάλει το σύστημα και γνωρίζει αυτές τις πιθανότητες, τότε θα επιλέξει τρόπους επίθεσης που αντιστοιχούν σε στατιστικά λιγότερο πιθανές απειλές. Έτσι, η κατάταξη των απειλών σε περισσότερο και λιγότερο πιθανές ανατρέπεται.

A9.2 Περιοχές επικινδυνότητας

Μετά την αποτίμηση των αγαθών και την εύρεση της διάστασης επικινδυνότητας που αυτά εκτίθενται, οι περιοχές που παρουσιάζονται στον παρακάτω πίνακα παρουσιάζουν το μεγαλύτερο βαθμό επικινδυνότητας.

ΑΓΑΘΟ	ΔΙΑΣΤΑΣΕΙΣ				
	Δ	Ακ	Ε	Ανθ	ΜηΑ
Εσωτερικές Υπηρεσίες					
[INTERNET_PIB] Διαδίκτυο	4,0	4,8	4,8		
Εφαρμογές					

[SIS_PIB] BIZNET		4,2	4,2		
[AV_PIB] Πρόγραμμα προστασίας από ιομορφικό λογισμικό - ANTIVIRUS		3,2	3,2		
[OS_PIB] Λειτουργικό Σύστημα Υπολογιστών		3,1	3,1		
Εξοπλισμός					
[SDB_PIB] Εξυπηρετητής της βάσης δεδομένων		2,1	3.8		
[PC_PIB] Προσωπικοί υπολογιστές		1.7	3.3		
Επικοινωνία					
[LAN_PIB] RED LAN		2,2	3,5	2,8	
Βοηθητικός Εξοπλισμός					
[CABLING_PIB] Καλωδίωση εγκαταστάσεων	3,0				
Εγκαταστάσεις					
Κεντρικό Κτίριο			3,5		

Πίνακας 1726: Περιοχές με μεγάλο βαθμό επικινδυνότητας

A9.3 Αξιολόγηση επικινδυνότητας

Ακολουθεί μία αξιολόγηση των περιοχών με το μεγαλύτερο βαθμό επικινδυνότητας

Διαδίκτυο: Το αγαθό αυτό ανήκει στην κατηγορία των Επιχειρησιακών Υπηρεσιών (Corporate Services), σύμφωνα με την ακολουθούμενη μεθοδολογία. Μετά την μελέτη των υπαρχόντων αντιμέτρων η απειλή με το μεγαλύτερο βαθμό, επηρεάζει τη διαθεσιμότητα της υπηρεσίας αυτής με βαθμό 4.0, και την εμπιστευτικότητα και ακεραιότητα με βαθμό 4.8. Πραγμάτωση της απειλής ενδέχεται να προκαλέσει συνέπειες όπως τη διακοπή της κανονικής ροής εργασιών του Οργανισμού και των καθημερινών δραστηριοτήτων, όπως η αποστολή emails στις αρμόδιες αρχές.

Μέτρα για την μείωση του ενδεχόμενου πραγμάτωσης :

- Περιορισμός συγκεκριμένων σελίδων, συμπεριλαμβανομένων σελίδων κοινωνικής δικτύωσης, καθώς και περιορισμός στο λογισμικό το οποίο ο κάθε υπάλληλος μπορεί

να κατεβάσει και να εγκαταστήσει στον υπολογιστή του. Περιορισμός σε λογισμικό για τη χρήση του Internet, ώστε αυτό να χρησιμοποιείται μόνο για δραστηριότητες του Οργανισμού και όχι για την προσωπική χρήση των εργαζομένων.

- Επίσης, δεν υπάρχει τίποτα που να εγγυάται την προστασία των υπηρεσιών, όπως η διασφάλιση της διαθεσιμότητας. Πρέπει να εγκατασταθούν τα ελάχιστα μέτρα και συσκευές (firewalls, proxy servers) για την υποστήριξη όσο το δυνατόν περισσότερο φορτίο στο δίκτυο.

Λογισμικό BizNet: Ανήκει στη κατηγορία εφαρμογών και πρόκειται για το κυρίως λογισμικό το οποίο χρησιμοποιεί ο Οργανισμός για τη διεξαγωγή των δραστηριοτήτων του. Εντοπίστηκαν απειλές με βαθμό επικινδυνότητας 4,2 στην ακεραιότητα και στην εμπιστευτικότητα. Η απειλή προέρχεται κυρίως από την έλλειψη κωδικού πρόσβασης στο σύστημα που βρίσκεται εγκατεστημένη η εφαρμογή. Αυτό επιτρέπει σε οποιοδήποτε άτομο με φυσική παρουσία να αλληλεπιδράσει στο σύστημα και πιθανόν να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε πληροφορία.

Μέτρα για την αντιμετώπιση:

- Θα πρέπει να υπάρχουν εμπιστευτικοί κωδικοί πρόσβασης για το σύστημα
- Ενίσχυση των δικαιωμάτων πρόσβασης, ανάλογα με τη θέση εργασίας, την περιγραφή αυτής και το είδος των δεδομένων που επεξεργάζονται..

Antivirus: Ανήκει στην κατηγορία των εφαρμογών. Η έλλειψη ενημερωμένου antivirus ενδέχεται να προκαλέσει τη διάδοση ιομορφικού λογισμικού στα συστήματα του Οργανισμού και ως εκ τούτου να προκαλέσει σοβαρές συνέπειες στην ακεραιότητα των δεδομένων καθώς και στην εμπιστευτικότητα αυτών. Για αυτό το λόγο ο βαθμός επικινδυνότητας στην ακεραιότητα και στην εμπιστευτικότητα είναι 3,2 αντίστοιχα. Ο κυριότερος λόγος από τον οποίο απειλείται το σύστημα από την έλλειψη antivirus είναι η συχνή χρήση εξωτερικής μνήμης (USB Stick) για τη μεταφορά αρχείων στα συστήματα του Οργανισμού.

Μέτρα για την αντιμετώπιση:

- Αγορά ή εγκατάσταση μίας πλήρως ενημερωμένης εφαρμογής Antivirus.
- Ενημέρωση της βάσης της εφαρμογής τουλάχιστον 4 φορές το μήνα.
- Συνιστάται η κατάργηση των θυρών εξωτερικών συνδέσεων USB από όλους τους υπολογιστές.

Λειτουργικό Σύστημα Υπολογιστών: Ανήκει στην κατηγορία των εφαρμογών. Οι απειλές που αφορούν το λειτουργικό σύστημα, αφορούν τη διάδοση ιομορφικού λογισμικού, το οποίο ενδέχεται να επηρεάσει την ακεραιότητα και την εμπιστευτικότητα με βαθμό 3,1. Αυτό

οφείλεται στην έλλειψη antivirus. Επίσης η ύπαρξη μη ενημερωμένων εφαρμογών ενδέχεται να προκαλέσει συνέπειες στην ακεραιότητα και στην εμπιστευτικότητα με βαθμό 3,0.

Μέτρα για την αντιμετώπιση:

- Απόκτηση λογισμικού με άδεια.
- Εγκατάσταση ειδικών ενημερώσεων που αφορούν τόσο το λογισμικό όσο και το λειτουργικό σύστημα
- Έλεγχος πρόσβασης στο λειτουργικό σύστημα χρησιμοποιώντας ξεχωριστό κωδικό ανά υπάλληλο.

Εξυπηρετητής της βάσης δεδομένων: Ανήκει στην κατηγορία του εξοπλισμού. Η απειλή η οποία οδηγεί σε υψηλό βαθμό επικινδυνότητας είναι ο χειρισμός εξοπλισμού ο οποίος ενδέχεται να επηρεάσει την εμπιστευτικότητα, με βαθμό 3,8. Η απειλή υπάρχει εξαιτίας της τοποθέτησης του εξοπλισμού σε εντελώς ανασφαλές περιβάλλον. Ο εξοπλισμός στον οποίο βρίσκεται εγκατεστημένο το σύστημα βάσεων δεδομένων βρίσκεται σε ένα κοινό δωμάτιο χωρίς έλεγχο πρόσβασης σε αυτό. Αυτό ενδεχομένως μπορεί να οδηγήσει στην εσκεμμένη απώλεια ή υποκλοπή πληροφορίας.

Μέτρα για την αντιμετώπιση:

- Μετακίνηση του διακομιστή σε δωμάτιο με όλα τα προβλεπόμενα μέτρα ασφάλειας, όπως έλεγχος πρόσβασης.
- Το δωμάτιο που θα μετακινηθεί ο διακομιστής, θα πρέπει να προφυλάσσεται και από τις φυσικές καταστροφές.

Προσωπικοί υπολογιστές: Ανήκει στην κατηγορία του εξοπλισμού. Η απειλή με το μεγαλύτερο βαθμό επικινδυνότητας είναι η χρήση του εξοπλισμού αυτού για σκοπούς πέρα των προκαθορισμένων. Η απειλή αυτή επηρεάζει την εμπιστευτικότητα με βαθμό 3,3 και την ακεραιότητα με βαθμό 1,7. Πρόκειται για μία πολύ κοινή απειλή, καθώς μερικοί εργαζόμενοι μπορεί να εγκαταστήσουν προγράμματα που δεν έχουν σχέση με την εργασία τους και αφορούν το προσωπικό τους ενδιαφέρον, όπως παιχνίδια, ταινίες, προσωπικά προγράμματα και άλλα.

Μέτρα για την αντιμετώπιση:

- Δημιουργία λογαριασμών χρηστών και διαχειριστή για την εγκατάσταση μόνο του απαραίτητου λογισμικού.

RED LAN: Ανήκει στην κατηγορία της επικοινωνίας. Απειλές εντοπίστηκαν στην δρομολόγηση πακέτων και μηνυμάτων, οι οποίες επηρεάζουν την εμπιστευτικότητα με βαθμό

3,5. Το δίκτυο δεν προστατεύεται από κανόνες δρομολόγησης, ούτε από μηχανισμούς αποτροπής μη εξουσιοδοτημένης πρόσβασης σε αυτό.

Μέτρα για την αντιμετώπιση:

- Ανάπτυξη κρυπτογραφικής προστασίας για την εμπιστευτικότητα των δεδομένων που ανταλλάσσονται.
- Παράλληλα με την υλοποίηση κρυπτογραφικών αλγορίθμων, συστήνεται η χρήση ψηφιακών πιστοποιητικών στις υπηρεσίες όπου ανταλλάσσονται δεδομένα, καθώς και η συχνή συντήρηση του τοπικού δικτύου.

Καλωδίωση εγκαταστάσεων: Ανήκει στην κατηγορία του βιοηθητικού εξοπλισμού. Η απειλή από τη ρύπανση του περιβάλλοντος έχει ένα υψηλό βαθμό επικινδυνότητας για τη διαθεσιμότητα (3,0). Η απειλή αυτή δίνεται από την κακή ποιότητα της εγκατάστασης των καλωδιώσεων και της σύνδεσης του εξοπλισμού που βρίσκονται εκτεθειμένα στη σκόνη και τη βρωμιά.

Μέτρα για την αντιμετώπιση:

- Δημιουργία ενημερωμένου πλάνου καλωδίωσης.
- Ονοματολογία, περιγραφή και χαρακτηρισμός όλων των συστατικών της καλωδίωσης.
- Αποφυγή διαδρομών της καλωδίωσης μέσα από κοινόχρηστους χώρους.
- Παρακολούθηση της πρόσβασης στην καλωδίωση.
- Διαχωρισμός ηλεκτρικής καλωδίωσης από δικτυακής, για αποφυγή παρεμβολών.
- Προστασία από τη φθορά ή μη εξουσιοδοτημένης παρακολούθησης (χρήση θωρακισμένου αγωγού, κουτιά ή πέρασμα καλωδίωσης μέσα από κλειστούς χώρους).

Κεντρικό Κτίριο: Ανήκει στην κατηγορία των εγκαταστάσεων. Οι εγκαταστάσεις του οργανισμού βρίσκονται σε μία ανασφαλή περιοχή, τόσο πληθυσμιακά, όσο και περιβαλλοντικά. Αυτό οδηγεί στη βαθμολόγηση του κεντρικού κτιρίου με 3,5 στην εμπιστευτικότητα. Το μοναδικό μέτρο προστασίας είναι η ύπαρξη ενός φρουρού στην κεντρική είσοδο.

Μέτρα για την αντιμετώπιση:

- Θα πρέπει να αυξηθεί ο αριθμός των φρουρών ασφαλείας, καθώς και τα συστήματα έκτακτης ανάγκης και προστασίας (συναγερμοί).
- Εγκατάσταση καμερών ασφαλείας σε όλο το κτίριο (και όχι μόνο στο δωμάτιο εκτροφής γαρίδων).

Προσωπικό: Αν και σχετικά χαμηλού βαθμού επικινδυνότητας, βρέθηκαν και απειλές που αφορούν το προσωπικό. Η πρώτη απειλή εντοπίζεται στην κοινωνική μηχανική. Αρκετοί εργαζόμενοι γνωρίζουν τους κωδικούς για την πρόσβαση στους υπολογιστές άλλων συναδέλφων τους, έχοντας έτσι πρόσβαση σε αρχεία και πληροφορίες που υπό κανονικές συνθήκες δεν θα έπρεπε να έχουν. Η δεύτερη απειλή προέρχεται από την πρώτη, και αφορά τον εκβιασμό ή κατάχρηση της πληροφορίας που μπορεί να αποκτήσει κάποιος εις βάρος άλλου εργαζόμενου.

Μέτρα αντιμετώπισης:

- Δημιουργία πολιτικής σχετικά με τη διαχείριση του προσωπικού (ασφάλεια).
- Δημιουργία των σχετικών διαδικασιών ασφάλειας (περιστατικών έκτακτης ανάγκης).
- Αντίδραση για την πρόληψη του εκβιασμού.
- Πρόληψη και αντιμετώπιση των επιθέσεων κοινωνικής μηχανικής

A9.4 Προτεινόμενο πλάνο ασφάλειας

Στη συνέχεια παρουσιάζονται ομαδοποιημένα τα κυριότερα σημεία του σχεδίου ασφάλειας. Το λεπτομερές σχέδιο ασφάλειας (μέτρα ασφάλειας) περιγράφεται σε επόμενη ενότητα. Όλα τα προτεινόμενα αντίμετρα έχουν επιλεγεί γιατί προσφέρουν υψηλότερο όφελος σε σχέση με το κόστος εφαρμογής τους (cost-effective). Συνεπώς, ενδεχόμενη αδρανοποίηση ορισμένων από αυτά θεωρείται ως συνειδητή ανάληψη του αντίστοιχου κινδύνου.

A9.5 Πρότυπα Μέτρα Ασφάλειας

Για την αντιμετώπιση και μετρίαση της επικινδυνότητας προτείνονται τα παρακάτω:

Τεκμηρίωση μη εξουσιοδοτημένης χρήσης των εφαρμογών

- Να θεωρείται σοβαρό αδίκημα η εγκατάσταση από εργαζόμενους οποιουδήποτε προγράμματος (software) στον υπολογιστή τους, είτε είναι για προσωπική χρήση ή για ψυχαγωγικούς σκοπούς.
- Για την πρόληψη προσβολής από ιομορφικό λογισμικό, οι εργαζόμενοι πρέπει να αποφεύγουν τη χρήση οποιουδήποτε λογισμικού δεν παρέχεται από τον ίδιο τον Οργανισμό
- Οι εργαζόμενοι καλούνται να επαληθεύουν ότι το αποθηκευτικό μέσο που πρόκειται να χρησιμοποιήσουν δεν περιέχει κάποιας μορφής ιομορφικό λογισμικό, προτού

διακινήσουν με αυτό οποιαδήποτε πληροφορία. Για το σκοπό αυτό ενδείκνυται η χρήση antivirus.

Τεκμηρίωση της ορθής χρήσης των υπολογιστών και του εξοπλισμού:

- Κάθε εργαζόμενος έχει εικωρηθεί σε μια ομάδα που είναι υπεύθυνη για το χειρισμό του εξοπλισμού.
- Οι εργαζόμενοι δεν πρέπει να μετακινούν τους υπολογιστές ή να εγκαθιστούν/απεγκαθιστούν συσκευές και εξοπλισμό. Μόνο το κατάλληλο προσωπικό πρέπει να έχει αυτή τη δυνατότητα.
- Ενώ ο υπολογιστής βρίσκεται σε χρήση, δεν πρέπει να καταναλώνεται οποιαδήποτε μορφή υγρού ή τροφής, πάρα μόνο αν αυτή βρίσκεται σε πλαστικό δοχείο.
- Αποφύγετε την τοποθέτηση αντικειμένων πάνω στον εξοπλισμό ή την κάλυψη των οπών εξαερισμού αυτού.
- Κρατήστε τους υπολογιστές σε ένα καθαρό περιβάλλον και απαλλαγμένο από υγρασία.
- Μόνο το κατάλληλο προσωπικό μπορεί να εκτελέσει συντήρηση ή να επισκευάσει τους υπολογιστές.
- Σε περίπτωση βλάβης από απροσεξία ή αμέλεια του εργαζομένου, αυτός υποχρεούται να καλύψει την αξία της επισκευής ή την αντικατάσταση του επηρεαζόμενου εξοπλισμού.

Τεκμηρίωση αντιγράφων ασφαλείας και προστασίας των δεδομένων:

- Η χρήση των CD είναι μόνο για δημιουργία αντιγράφου ασφάλειας πληροφοριών. Ο εργαζόμενος είναι υπεύθυνος για τη φύλαξη.
- Οι εργαζόμενοι θα πρέπει να δημιουργούν τακτικά αντίγραφα ασφάλειας της ευαίσθητης και κρίσιμης πληροφορίας που υπάρχει στους υπολογιστές τους.

Τεκμηρίωση της χρήσης των υπηρεσιών διαδικτύου:

- Οι εργαζόμενοι δεν πρέπει να χρησιμοποιούν λογαριασμούς e-mail άλλων συναδέλφων τους, ή να λαμβάνουν μηνύματα από άλλους λογαριασμούς.
- Οι εργαζόμενοι πρέπει να χειρίζονται τα μηνύματα και το περιεχόμενό τους ως πληροφορία που ανήκει στον Οργανισμό X.
- Απαγορεύεται η παραποίηση, η απόκρυψη, η αφαίρεση ή η αντικατάσταση της ταυτότητας ενός χρήστη ηλεκτρονικού ταχυδρομείου.
- Η χρήση του διαδικτύου πρέπει να σχετίζεται αποκλειστικά και μόνο με τις ανάγκες των δραστηριοτήτων της εκάστοτε θέσης και ρόλου.

Τεκμηρίωση προστασίας εγκαταστάσεων:

- Ρύθμιση προτύπων συμπεριφοράς για τις περιοχές γύρω από τους εξυπηρετητές και τους σταθμούς εργασίας.

Τεκμηρίωση της διαχείρισης του προσωπικού:

- Σε κάθε σύμβαση εργασίας πρέπει να υπάρχουν ρήτρες εμπιστευτικότητας για τη διασφάλιση των πληροφοριών της εταιρείας.
- Κάθε εργαζόμενος που χρησιμοποιεί τον εξοπλισμό και τις υπηρεσίες πληροφορικής, οφείλει η χρήση του να διεξάγεται σύμφωνα με τις αρχές της γνώσης και της εμπιστευτικότητας της πληροφορίας.
- Ο κάθε εργαζόμενος πρέπει να συμφωνεί με ένα χρονοδιάγραμμα εκτέλεσης εργασιών.
- Ρύθμιση προτύπων συμπεριφοράς για τους εργαζόμενους για τη διαμόρφωση ενός ορθού και αξιοπρεπούς περιβάλλοντος εργασίας για όλους.

Μέσω της μελέτης των υπαρχόντων αντιμέτρων και την εφαρμογή των προτεινόμενων, η επικινδυνότητα ενδέχεται να μειωθεί σημαντικά, όπως παρουσιάζεται στον ακόλουθο πίνακα.

ΑΓΑΘΟ	ΔΙΑΣΤΑΣΕΙΣ				
	Δ	Ακ	Ε	Ανθ	ΜηΑ
Εσωτερικές Υπηρεσίες					
[INTERNET_PIB] Διαδίκτυο	0	0	0		
Εφαρμογές					
[SIS_PIB] BIZNET		0	0		
[AV_PIB] Πρόγραμμα προστασίας από ιομορφικό λογισμικό - ANTIVIRUS		09,0	0,90		
[OS_PIB] Λειτουργικό Σύστημα Υπολογιστών		0,71	0,71		
Εξοπλισμός					
[SDB_PIB] Εξυπηρετητής της βάσης δεδομένων		0	0		
[PC_PIB] Προσωπικοί υπολογιστές		0,41	0,76		
Επικοινωνία					

[LAN_PIB] RED LAN		0,68	1,6	0	
Βοηθητικός Εξοπλισμός					
[CABLING_PIB] Καλωδίωση εγκαταστάσεων	1,6				
Εγκαταστάσεις					
Κεντρικό Κτίριο			0		

Πίνακας 278: Μείωση επικινδυνότητας

Εξάλειψη προφανών σημείων επικινδυνότητας

Ο διακομιστής της βάσης δεδομένων, έχει εγκατασταθεί εσφαλμένα, χωρίς να έχει ακολουθηθεί κατά την εγκατάστασή του στην τρέχουσα θέση κάποιο πρότυπο ασφάλειας. Πάνω από το διακομιστή υπάρχει ένα κουτί, στο οποίο βρίσκεται ο δρομολογητής, ενώ όλος ο εξοπλισμός βρίσκεται τοποθετημένος δίπλα στο τζάμι ενός γραφείου. Επιπλέον δεν υπάρχει πυροσβεστήρας στο συγκεκριμένο δωμάτιο.

Οι κωδικοί πρόσβασης φαίνεται να αποτελούν κοινή γνώση ανάμεσα στους εργαζόμενους του Οργανισμού, κάτι που κάνει το σύστημα επιρρεπές σε επιθέσεις κοινωνικής μηχανικής. Ιδανικά ο κωδικός πρόσβασης στο κάθε σύστημα έπρεπε να αλλάζει τακτικά.

Όσο αφορά τη χρήση ενημερωμένου antivirus, κάποιοι υπολογιστές δεν έχουν πρόσβαση στο διαδίκτυο, με αποτέλεσμα να τους έχουν παραμελημένους. Ακόμα όμως και σε υπολογιστές με πρόσβαση στο διαδίκτυο το antivirus βρέθηκε να μην έχει ενημερωθεί. Το ορθό θα ήταν να υπάρχει συχνή ενημέρωση του Antivirus.

A10 Εκτίμηση αντιμέτρων

Σε αυτό το στάδιο, προσδιορίζονται τα αντίμετρα που είναι αποτελεσματικά για τον Οργανισμό, προκειμένου να μετριάσουν την επικινδυνότητα. Στο πλαίσιο αυτής της μεθοδολογίας, η μελέτη των αντιμέτρων μπορεί και πρέπει να περιλαμβάνει μικρά ή μεγάλα χρονικά διαστήματα υλοποίησης, αλλά η μελέτη της περίπτωσής μας, περιλαμβάνει τρεις φάσεις:

- Πρώτο στάδιο ονομάζεται ΔΥΝΗΤΙΚΟ (Δυναμικό).
- Δεύτερο στάδιο ονομάζεται ΥΦΙΣΤΑΜΕΝΗ ΚΑΤΑΣΤΑΣΗ.
- Τρίτο στάδιο ονομάζεται ΣΤΟΧΟΣ.

Αυτή η δραστηριότητα αποτελείται από δύο δευτερεύουσες εργασίες:

- Προσδιορισμός των σχετικών εγγυήσεων.
- Αξιολόγηση αντιμέτρων.

A10.1 Προσδιορισμός των αντιμέτρων

Σε αυτό το στάδιο, χρησιμοποιείται το εργαλείο PILAR, που βοηθά στην επιλογή των αντιμέτρων για κάθε αγαθό, ανάλογα με τις απειλές που έχουν προσδιοριστεί.

Απαίτηση για έγκριση/εξουσιοδότηση: Ανήκει στον περιορισμό της πρόσβασης στις πληροφορίες που με τη σειρά του ανήκει στη Λογική Ελέγχου Πρόσβασης. Αυτό 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, σφάλματα ακολουθίας, αλλοίωση πληροφοριών, διαρροή πληροφοριών, ευπάθεια λογισμικού, λάθη στη συντήρηση/επικαιροποίηση προγραμμάτων (software), πλαστογράφηση της ταυτότητας του χρήστη, κατάχρηση στα προνόμια πρόσβασης, μη εξουσιοδοτημένη πρόσβαση, τροποποίηση κ.λπ..

Εργαλείο προστασίας από ιομορφικό λογισμικό: Η εταιρεία προσφέρει εργαλεία προστασίας από ιομορφικό λογισμικό, αλλά δεν είναι πάντα ενημερωμένα, ή έχουν περιπέσει σε αχρηστία. Ως εκ τούτου, τα ακόλουθα αντίμετρα επιλέχθηκαν:

- Το πρόγραμμα πρέπει να ενημερώνεται τακτικά.
- Η βάση δεδομένων του προγράμματος πρέπει να ενημερώνεται τακτικά (κατά προτίμηση σε κάθε εκκίνηση).
- Τα αντίμετρα αυτά εφαρμόζονται στο επίπεδο των εφαρμογών και του λογισμικού.

Διασφάλιση διαθεσιμότητας: Εντός αυτής της ομάδας των αντιμέτρων έχει προγραμματιστεί:

- Προστασία ενάντια στις επιθέσεις DoS.
- Λειτουργικές διαδικασίες.
- Μέτρα κατά των επιθέσεων στις φυσικές εγκαταστάσεις.

Από αυτά τα αντίμετρα, η εταιρεία δε διαθέτει κάποιο. Ωστόσο, μπορούν να εφαρμοστούν σε εσωτερικό επίπεδο και διασφαλίζουν τη διαθεσιμότητα.

Προστασία των εφαρμογών της πληροφορικής: Τα αντίμετρα επιλέχθηκαν με βάση ότι στην εταιρεία δεν υπάρχουν τα εξής:

- Κανονισμοί για την επιτρεπόμενη χρήση των εφαρμογών.
- Κανόνες σχετικά με την επιβολή των δικαιωμάτων.
- Κανόνες για την εγκατάσταση μη εξουσιοδοτημένου λογισμικού και προϊόντων με συγκεκριμένη άδεια.
- Διαδικασίες για τη δημιουργία αντιγράφων ασφάλειας.
- Εφαρμογή προφίλ ασφάλειας: Χάρη σε αυτό η εταιρεία μπορεί να προστατευθεί ενάντια από αυτές τις απειλές όπως λάθη χρηστών, διάδοση ιομορφικού λογισμικού, σφάλματα σε προγράμματα συντήρησης/ενημέρωσης (λογισμικό) και περιστατικά μη προβλεπόμενης χρήσης.
- Τα αρχεία δεδομένων της εφαρμογής πρέπει να προστατεύονται όπως επίσης και οι μηχανισμοί επικοινωνίας μεταξύ διεργασιών, εξασφαλίζοντας εμπιστευτικότητα και ακεραιότητα.
- Έλεγχος έκδοσης όλων των προγραμμάτων λογισμικού.

Προστασία του εξοπλισμού: Πρέπει να διασφαλιστεί η προστασία του εξοπλισμού με τους εξής τρόπους:

- Κανονισμοί για τη σωστή χρήση του εξοπλισμού.
- Διαδικασίες που είναι εξουσιοδοτημένες να χρησιμοποιήσουν τον εξοπλισμό.
- Προφίλ ασφαλείας.

Με αυτό το αντίμετρο, η εταιρεία ελαχιστοποιεί απειλές όπως: μη προβλεπόμενη χρήση και μη εξουσιοδοτημένη πρόσβαση, διασφαλίζοντας παράλληλα διαστάσεις όπως η ακεραιότητα και η εμπιστευτικότητα.

Διασφάλιση Επικοινωνιών: Έχουν επιλεγεί τα ακόλουθα αντίμετρα για την ελαχιστοποίηση της επικινδυνότητας:

- Προφίλ ασφαλείας: Επικοινωνία εντός της επιχείρησης για την αποφυγή απειλών όπως λάθη χρηστών, σφάλματα ακολουθίας, απρόβλεπτη χρήση, προώθηση μηνυμάτων, μη εξουσιοδοτημένη πρόσβαση.
- Με τα αντίμετρα αυτά προστατεύονται οι ιδιότητες της ασφάλειας: Ακεραιότητα, εμπιστευτικότητα και αυθεντικότητα.
- Έλεγχος της προέλευσης και του προορισμού των μηνυμάτων (φίλτρο), καθώς η εταιρεία δε διαθέτει κανόνες χρήσης των υπηρεσιών δικτύου.

Όλα τα παραπάνω αντίμετρα επικεντρώνονται στην αντιμετώπιση της μη εξουσιοδοτημένης πρόσβασης.

Για να εξασφαλίζεται η επικοινωνία κατά τη χρήση του διαδικτύου είναι απαραίτητα τα παρακάτω αντίμετρα:

- Ενημερωμένα φίλτρα.
- Anti spyware εργαλεία.
- Καταγραφή ιστορικού.
- Καταγραφή cookies.
- Κανονισμοί για τη χρήση των υπηρεσιών του Διαδικτύου.
- Εργαλείο παρακολούθησης της κυκλοφορίας.

Προστασία των Μέσων Αποθήκευσης Πληροφορίας

- Κρυπτογραφία.
- Τήρηση των κανόνων/συστάσεων του κατασκευαστή και του προμηθευτή.
- Προστασία από περιβαλλοντικούς παράγοντες.
- Έλεγχος κλίματος - περιβαλλοντικός έλεγχος (υγρασία, θερμοκρασία κ.λπ.).

Διαχείριση Προσωπικού: Πρέπει να εφαρμοστούν τα παρακάτω αντίμετρα:

- Κανόνες σχετικά με τη διαχείριση του προσωπικού.
- Διαδικασίες για τη διαχείριση του προσωπικού.
- Προδιαγραφές για την πρόσληψη ώστε να διασφαλίζεται εμπιστευτικότητα των δεδομένων, και να αποφεύγονται επιθέσεις εκ των έσω.

A10.2 Αξιολόγηση Αντιμέτρων

Για την εκτίμηση της αποτελεσματικότητας των αντιμέτρων χρησιμοποιείται ο εξής προσδιορισμός:

Αποτελεσματικότητα	Επίπεδο	Ωριμότητα	Κατάσταση
0%	L0	Ανύπαρκτη	Ανύπαρκτη
10%	L1	Αρχικό στάδιο	Αρχικό στάδιο
50%	L2	Μερική εφαρμογή	Διαισθητική εφαρμογή
90%	L3	Ορισμένη διαδικασία	Σε λειτουργία
95%	L4	Μετρήσιμη διαδικασία	Σε παρακολούθηση
100%	L5	Βελτιστοποιημένη	Συνεχής βελτίωση

Πίνακας 19: Εκτίμηση αποτελεσματικότητας αντιμέτρων