ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΩΝ ΔΙΑΤΑΞΕΩΝ ΚΑΙ
ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΦΑΣΕΩΝ

Η αξιολόγηση κινδύνου στην Ασφάλεια Πληροφοριών

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Στρουγγάρης Ζώης

Επιβλέπων : Δημήτριος Ασκούνης
Καθηγητής Ε.Μ.Π.

Αθήνα,Οκτώβριος 2020

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΩΝ ΔΙΑΤΑΞΕΩΝ ΚΑΙ
ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΦΑΣΕΩΝ

Η αξιολόγηση κινδύνου στην Ασφάλεια Πληροφοριών

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Στρουγγάρης Ζώης

Επιβλέπων : Δημήτριος Ασκούνης
Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 27η Οκτωβρίου 2020.

.....	.....	.....
Δημήτριος Ασκούνης	Ιωάννης Ψαρράς	Χρυσόστομος Δούκας
Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Επίκουρος Καθηγητής Ε.Μ.Π.

Αθήνα,Οκτώβριος 2020

.....

Στρουγγάρης Ζώης

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική εργασία πραγματοποιεί μια ανασκόπηση στο πεδίο της ασφάλειας πληροφοριών. Αρχικά, αναλύει βασικές έννοιες του χώρου, όπως η πληροφορία, ο κίνδυνος, η απειλή, η ευαλωτότητα, η διαχείριση κινδύνου, το ΣΔΑΠ (Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών) και το πρότυπο. Στη συνέχεια παρουσιάζει συνοπτικά τα πιο ευρέως διαδεδομένα πρότυπα ασφάλειας πληροφοριών και περιγράφει αναλυτικά τα χαρακτηριστικά και τις απαιτήσεις του πιο σημαντικού προτύπου, του ISO/IEC 27001. Επίσης, καταπιάνεται με τις διαδικασίες που συνθέτουν τη διαχείριση κινδύνου ενός ΣΔΑΠ συμβατού με το ISO/IEC 27001 και κυρίως με την αξιολόγηση κινδύνου, όπου και αναφέρονται ορισμένες βασικές μεθοδολογίες συμβατές με το πρότυπο. Τέλος, υλοποιεί μια σύγχρονη μέθοδο αξιολόγησης κινδύνου και την εφαρμόζει σε υποθετικά σενάρια.

Λέξεις-κλειδιά: οργανισμός, ασφάλεια πληροφοριών, κίνδυνος, απειλή, ευαλωτότητα, ΣΔΑΠ, πρότυπο, ISO27001, αξιολόγηση κινδύνου, μεθοδολογία

ABSTRACT

The current thesis carries out a review in the field of information security. For starters, the study assesses fundamental notions of the field, such as information, risk, threat, vulnerability, risk management, ISMS (Information Security Management System), as well as the information security standard. Next, the study displays briefly the most widely known information security standards and it describes in detail the characteristics and requirements of the most important one, the ISO/IEC 27001. Furthermore, the study delves into the processes, which compound risk management for an ISMS, compatible with ISO/IEC 27001, and primarily, into the risk assessment, where some basic methodologies, compatible with the standard, are mentioned. Finally, the study accomplishes a modern method of risk assessment and it implements it in hypothetical scenarios.

Keywords: organization, information security, risk, threat, vulnerability, ISMS, standard, ISO27001, risk assessment, methodology

Ευχαριστίες

Θα ήθελα να εκφράσω τις βαθύτερες ευχαριστίες μου σε όσους βοήθησαν άμεσα και έμμεσα στην εκπόνηση της παρούσας διπλωματικής εργασίας και ουσιαστικά στην ολοκλήρωση του κύκλου σπουδών μου.

Στον καθηγητή μου κ. Ασκούνη Δημήτριο, επιβλέποντα της εργασίας μου, για την ευκαιρία που μου έδωσε να ασχοληθώ με ένα άκρως ενδιαφέρον θέμα του τομέα του και την εν γένει συμπεριφορά του κατά τη διάρκεια συγγραφής.

Στον υποψήφιο διδάκτορα του εργαστηρίου κ. Μπούνα Κανάρη, συνεπιβλέποντα της εργασίας, που καθ'όλη τη διάρκεια εκπόνησης της ήταν συνεχώς στη διάθεση μου για οποιαδήποτε βοήθεια χρειάστηκα σε υλικό, ιδέες και συμβουλές. Χωρίς τη συμβολή του, δε θα υπήρχε αυτό το αποτέλεσμα και τον ευχαριστώ ιδιαίτερα για τη συνεργασία που είχαμε.

Τέλος, η στήριξη των φίλων και της οικογένειας μου όλα τα χρόνια φοίτησης μου ήταν καταλυτική και τους αξίζει ιδιαίτερη αναφορά. Η υπομονή τους, η στήριξη σε καλές και κακές περιόδους και η συμπεριφορά τους απέναντι μου ήταν καθοριστικοί παράγοντες των επιτυχιών αυτών των χρόνων.

Πίνακας περιεχομένων

Πίνακας σχημάτων

Εικόνες

Πίνακες

Κεφάλαιο 1: Εισαγωγή

1.1. Οι πληροφορίες ως περιουσιακό στοιχείο κάθε οργανισμού

Όλες οι πληροφορίες ενός οργανισμού ή μιας επιχείρησης, ανεξάρτητα από το σκοπό τους, πρέπει να λογίζονται ως περιουσιακό στοιχείο του οργανισμού όπως ακριβώς λογίζονται αντικείμενα, χώροι και εγκαταστάσεις και η διαχείριση τους θα πρέπει να γίνεται με τέτοιο τρόπο, ώστε να αποφέρει το μέγιστο όφελος για αυτόν. Αυτό υποστήριξε ο Dr. Robert Hawley και η επιτροπή του στην αναφορά τους (Hawley report) σε συνεργασία με την Ομοσπονδία της Βρετανικής Βιομηχανίας (CBI) σε μια εποχή όπου σε οργανωτικό επίπεδο η αξία της πληροφορίας δεν ήταν αναγνωρισμένη σε μεγάλο βαθμό (KPMG/IMPACT,1994). Σύμφωνα με την αναφορά, σε περίπτωση που δε δοθεί η απαραίτητη προσοχή στις πληροφορίες από τους διευθύνοντες απειλείται σε πρώτο βαθμό η συνοχή του οργανισμού σε επίπεδο στρατηγικής, σχεδιασμού και προϋπολογισμού αλλά και στο χειρότερο σενάριο η βιωσιμότητα του. Για το λόγο αυτό, η επιτροπή αναγνώρισε 8 κατηγορίες στοιχείων πληροφορίας και πιο συγκεκριμένα πληροφορίες που αφορούν:

- Την αγορά και τον καταναλωτή, π.χ. εμπορικά σήματα.
- Το προϊόν/υπηρεσία που παράγεται.
- Τη γνώση των ειδικών σε συγκεκριμένους τομείς, π.χ. ο τρόπος ανάπτυξης του δικτύου πωλήσεων μιας εταιρίας λόγω των επαφών του υπευθύνου με τους ιδιοκτήτες καταστημάτων λιανικής.
- Τις διαδικασίες εντός του οργανισμού, δηλαδή τις ανθρώπινες διεργασίες και πρωτόκολλα που ακολουθούνται.
- Το management, δηλαδή τον τρόπο διεύθυνσης του οργανισμού.
- Το τμήμα ανθρώπινου δυναμικού.
- Τους προμηθευτές, π.χ. συμβόλαια και εμπορικές συμφωνίες.

- Τομείς γενικότερης ευθύνης, όπως η συμμόρφωση με νομικά πλάισια, η συμπόρευση με την προστασία του περιβάλλοντος και η τήρηση κανόνων υγιεινής (KPMG/IMPACT,1994).

1.2. Τα Πληροφοριακά Συστήματα

Σύστημα ορίζεται ένα σύνολο μερών ή οντοτήτων που έχουν στενή σχέση αλληλεπίδρασης με σκοπό την πραγματοποίηση ενός στόχου ή την ολοκλήρωση μιας εργασίας. Ως εκ τούτου, πληροφοριακό σύστημα ονομάζεται ένα ολοκληρωμένο σύνολο από στοιχεία για τη συλλογή, αποθήκευση και επεξεργασία δεδομένων και την παροχή πληροφοριών, γνώσης και ψηφιακών προϊόντων. Όλοι οι σύγχρονοι οργανισμοί βασίζονται στα πληροφοριακά τους συστήματα για να αλληλεπιδράσουν με τους καταναλωτές και τους προμηθευτές τους, να ανταγωνιστούν την αγορά, να συμμετέχουν στο ηλεκτρονικό εμπόριο, να επεξεργαστούν οικονομικά δεδομένα, να διευθύνουν τα τμήματα τους και γενικότερα να φέρουν σε πέρας τις λειτουργίες τους. Ουσιαστικά, τα πληροφοριακά συστήματα είναι ένα από τα θεμέλια ενός οργανισμού στις μέρες μας, και μάλιστα υπάρχουν εταιρίες-κολοσσοί που εξ ολοκλήρου λειτουργούν με κύριο άξονα τους αυτά. Πιο συγκεκριμένα το eBay, στη μορφή μιας τεράστιας ψηφιακής αίθουσας δημοπρασιών, η Amazon σαν ένα ηλεκτρονικό mall, και η πιο διαδεδομένη μηχανή αναζήτησης παγκοσμίως, η Google, αποτελούν σημαντικά παραδείγματα τέτοιων οργανισμών (Zwass, 2017).

Τα βασικά στοιχεία κάθε πληροφοριακού συστήματος είναι τα ακόλουθα:

- **Υλικό υπολογιστών (Hardware):** Οι σύγχρονοι οργανισμοί ανάλογα με το μέγεθος τους, χρησιμοποιούν ένα σύνολο κατανεμημένων υπολογιστικών συστημάτων, από μεγάλους servers παράλληλης επεξεργασίας έως προσωπικούς υπολογιστές, tablets και smartphones. Ταυτόχορνα, σένσορες συλλογής δεδομένων και περιφερειακές συσκευές αποθήκευσης και εισόδου-εξόδου συμπληρώνουν το πληροφοριακό υποσύστημα του υλικού.
- **Λογισμικό (Software):** Αναλυτικότερα, το Software κατηγοριοποιείται σε λογισμικό συστήματος (system software) και σε λογισμικό εφαρμογών (application software). Το πρώτο σχετίζεται με το λειτουργικό σύστημα που χρησιμοποείται για τη διαχείριση του υλικού, των δεδομένων και των

αρχείων του υπολογιστή. Το δεύτερο αφορά προγράμματα για το χειρισμό συγκεκριμένων λειτουργιών, όπως για παράδειγμα τα προγράμματα επεξεργασίας κειμένου ή ένα πρόγραμμα βαρδιολόγησης εργαζομένων σε μια εταιρία.

- **Τηλεπικοινωνίες:** Οι τηλεπικοινωνίες χρησιμοποιούνται για τη διασύνδεση υπολογιστικών συστημάτων και για τη μεταφορά δεδομένων. Οι σύγχρονες τεχνολογίες περιλαμβάνουν ενσύρματες και ασύρματες συνδέσεις και εξελίσσονται ραγδαία προς την ταχύτερη επικοινωνία και μεταφορά όλο και περισσότερου όγκου δεδομένων.
- **Βάσεις Δεδομένων (Databases):** Πολλά πληροφοριακά συστήματα αποτελούν οχήματα μεταφοράς δεδομένων που είναι αποθηκευμένα σε βάσεις δεδομένων. Βάση δεδομένων ονομάζεται μια συλλογή από συσχετισμένα δεδομένα οργανωμένα με τέτοιο τρόπο, ώστε συγκεκριμένες καταχωρήσεις ή σύνολο καταχωρήσεων να ανακτάται με βάση ένα συγκεκριμένο ή συγκεκριμένα κριτήρια.
- **Ανθρώπινο δυναμικό και διεργασίες:** Όλοι οι εργαζόμενοι ενός οργανισμού αποτελούν στοιχείο ζωτικής σημασίας για ένα πληροφοριακό σύστημα. Από το τεχνικό προσωπικό, όπως υπευθύνους ασφαλείας δικτύων, μηχανικούς software, σχεδιαστές ιστοσελίδων και αναλυτές μέχρι τους εργαζόμενους σε θέσεις μη σχετικές με το τεχνικό κομμάτι των υπολογιστών είναι σημαντικό να αξιοποιούνται στο μέγιστο δυνατό οι δυνατότητες του πληροφοριακού συστήματος. Όσο αφορά τις διαδικασίες, αυτές αποτελούν έγγραφες λειτουργίες του συστήματος. Για παράδειγμα, οδηγίες απαιτείται να υπάρχουν για το ποιός είναι υπεύθυνος να εκτελέσει ένα πρόγραμμα μισθοδοσίας, πότε, και ποιός έχει τη δικαιοδοσία να δει το αποτέλεσμα (Zwass, 2017).

1.3. Ασφάλεια Πληροφοριών

Σύμφωνα με τους Susanto, Almunawar και Tuan (2011), οι πληροφορίες αποτελούν τη ψυχή κάθε οργανισμού στις χώρες με εξελιγμένες τεχνολογίες πληροφοριών (IT – Information Technology) και για αυτό η ασφάλεια τους δε μπορεί να είναι μια απλή διαδικασία χρήσης ονομάτων χρήστη και κωδικών (username /

passwords). Παρομοίως, η Ashenden (2008) αναφέρει πως η ασφάλεια πληροφοριών (information security) πρέπει να εξελιχθεί από αρμοδιότητα των τεχνικών του τμήματος IT σε ένα πεδίο ευρύτερης προσοχής και σημασίας με στόχο την προστασία κάθε πληροφορίας σε οποιαδήποτε μορφή εντός του οργανισμού.

Αναλυτικότερα, ως ασφάλεια πληροφοριών ορίζεται η μείωση των κινδύνων για πιθανή νόθευση, κλοπή, έλλειψη και κακή χρήση οποιασδήποτε πληροφορίας μέσα σε έναν οργανισμό (Pinheiro & Ribeiro, 2015). Σύμφωνα με το πρότυπο ISO 17799:2006 που θα περιγραφεί στα επόμενα κεφάλαια, η ιδέα της ασφάλειας πληροφορίων βασίζεται στην προστασία της πληροφορίας από ποικίλες απειλές για την εξασφάλιση της συνέχειας του οργανισμού (business continuity), την ελαχιστοποίηση των κινδύνων και τη μεγιστοποίηση των οφελών και ευκαιριών. Παράλληλα, υπάρχουν τρεις βασικές αρχές στις οποίες υπακούει η ασφάλεια πληροφοριών, τρεις απαιτήσεις με τις οποίες κάθε οργανισμός οφείλει να συμμορφώνεται, αφού σε διαφορετική περίπτωση προμηνύονται εξαιρετικά αρνητικές συνέπειες. Ειδικότερα, οι τρεις αυτές βασικές αρχές είναι οι παρακάτω:

- **Εμπιστευτικότητα (Confidentiality):** Οι πληροφορίες πρέπει να είναι γνωστές μόνο στα άτομα του οργανισμού που έχουν τη δικαιοδοσία να τις γνωρίζουν.
- **Ακεραιότητα (Integrity):** Οι πληροφορίες πρέπει να διατηρούνται στην πρωτότυπη μορφή τους χωρίς αλλαγές.
- **Διαθεσιμότητα (Availability):** Η πρόσβαση σε οποιαδήποτε πληροφορία πρέπει να είναι εφικτή κάθε φορά που απαιτείται (Pinheiro & Ribeiro, 2015).

1.4. Βασικές έννοιες στην ασφάλεια πληροφοριών

1.4.1. Απειλές (Threats)

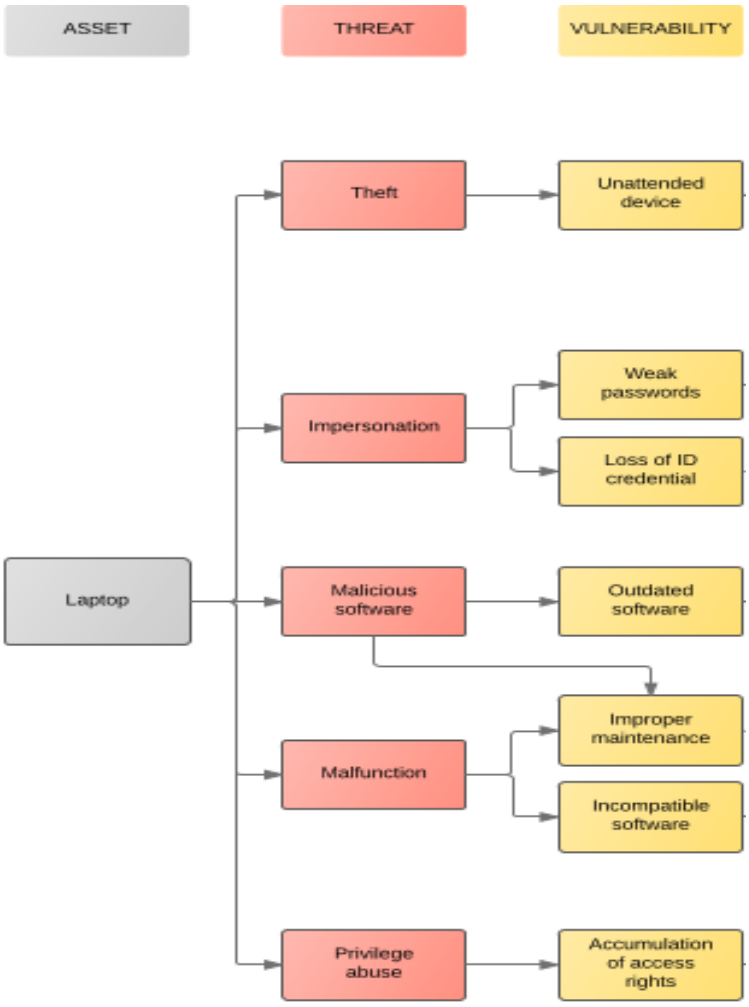
Απειλή ονομάζεται κάθε ενέργεια ή κατάσταση που οδηγεί σε καταστροφή, απώλεια ή/και αλλοίωση πληροφοριών μέσα σε έναν οργανισμό (Young, 2016). Υπάρχουν πολλές διαφορετικές περιπτώσεις απειλών για το πληροφοριακό σύστημα (βλ. Εικόνα 1).

Threats to information security
Act of human error or failure (accidents, employee mistakes)
Compromises to intellectual property (piracy, copyright infringement)
Deliberate acts of espionage or trespass (unauthorized access and/or data collection)
Deliberate acts of information extortion (blackmail of information disclosure)
Deliberate acts of sabotage or vandalism (destruction of systems or information)
Deliberate acts of theft (illegal confiscation of equipment or information)
Deliberate software attacks (viruses, worms, macros, denial of service)
Forces of nature (fire, flood, earthquake, lightning)
Quality of service deviations from service providers (power and WAN Quality of Service issues)
Technical hardware failures or errors (equipment failure)
Technical software failures or errors (bugs, code problems, unknown loopholes)
Technological obsolescence (antiquated or outdated technologies)

Εικόνα 1 - Παραδείγματα απειλών της ασφάλειας πληροφοριών ενός οργανισμού

1.4.2. Ευαλωτότητες (Vulnerabilities)

Ευαλωτότητα στην ασφάλεια πληροφοριών ονομάζεται η αδυναμία ή ευπάθεια στοιχείων του οργανισμού, που με πρόθεση ή χωρίς μια απειλή μπορεί να εκμεταλλευτεί για να πραγματοποιηθεί (Chandrashekar et al., 2015). Ακολουθεί ένα παράδειγμα (βλ. Εικόνα 2) που συνδέει τις απειλές και τις εαυλωτότητες σε σχέση με ένα τυχαίο προσωπικό υπολογιστή σε μια εταιρία:



Εικόνα 2 – Σύνδεση απειλών και ευαλωτοτήτων (threats - vulnerabilities) σε σχέση με τον προσωπικό υπολογιστή κάποιου τυχαίου εργαζομένου

1.4.3. Κίνδυνοι (Risks)

Κίνδυνος (risk) στην ασφάλεια πληροφοριών ορίζεται η πιθανότητα πραγματοποίησης μια απειλής (threat) ύστερα από την εκμετάλλευση μιας αδυναμίας (vulnerability) του οργανισμού που θα προκαλέσει αλλοίωση ή απώλεια πληροφοριών με αποτέλεσμα την άμεση παραβίαση των τριών θεμελιωδών αρχών της ασφάλειας πληροφοριών (Young, 2016).

1.4.4. Διαχείριση Κινδύνου (Risk Management)

Η θεωρία του risk management υποστηρίζει ότι μέσω της ανάλυσης και εκτίμησης του κινδύνου, οι απειλές και οι ευαλωτότητες που αφορούν την ασφάλεια πληροφοριών μπορούν να υπολογιστούν και να αξιολογηθούν. Με αυτόν τον τρόπο, τα αποτελέσματα της αξιολόγησης είναι ικανά να καθορίσουν το σχεδιασμό των απαιτήσεων και των μέτρων προστασίας του πληροφοριακού συστήματος ενός οργανισμού. Ο στόχος της διαχείρισης κινδύνου είναι να περιορίσει τους κινδύνους που αφορούν την ασφάλεια πληροφοριών σε ένα αποδεκτό επίπεδο (Hong et al., 2003).

Στο κεφάλαιο 4 θα αναλυθεί εκτενώς η θεωρία διαχείρισης κινδύνου με μεγάλη έμφαση στην αξιολόγηση (risk assessment).

Κεφάλαιο 2: Το πεδίο των προτύπων Ασφάλειας Πληροφοριών

2.1. Το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) – Information Security Management System (ISMS)

Σύμφωνα με τον παραδοσιακό ορισμό της λέξης, management ονομάζεται ο τρόπος που κάτι, στην περίπτωση μας οι εργασίες μέσα σε έναν οργανισμό, διεξάγονται, ελέγχονται και επιβλέπονται. Πιο συγκεκριμένα πρόκειται για τον έλεγχο μιας δραστηριότητας μέσα στον οργανισμό με σκοπό τη συνεχή βελτίωση της απόδοσης της που αποβλέπει στην πραγματοποίηση των στόχων του οργανισμού. Συνεπώς, το management στην ασφάλεια πληροφοριών (ISM) είναι ένα σύνολο από γνώσεις, εμπειρία, ανάλυση και αξιολόγηση κινδύνων, στρατηγικές, πολιτικές, διαδικασίες, μεθοδολογίες, εκπαιδεύσεις, ελέγχους και συμβόλαια που επιβλέπουν τη συνεχή προστασία κάθε πληροφορίας μέσα σε έναν οργανισμό και διατηρούν τις τρεις βασικές αρχές ασφάλειας πληροφοριών (Ashenden, 2008). Το ISMS σύμφωνα με τους Brykczynski και Small (2003) είναι ο κύκλος ζωής μιας προσέγγισης στην ασφάλεια πληροφοριών με την υλοποίηση, διατήρηση και βελτίωση μιας σειράς πολιτικών, ελέγχων και διαδικασιών που εξασφαλίζει την ασφάλεια των πληροφοριακών στοιχείων ενός οργανισμού με τον κατάλληλο τρόπο.

Ένα ISMS αποτελείται από τέσσερα επιμέρους στοιχεία, σύμφωνα με τους Al-Dahri, Al-Sarti και Aziz (2017), τις αρχές του management, τους υλικούς πόρους, το προσωπικό και τις διαδικασίες. Ο Alfantookh (2009) όρισε έντεκα συγκεκριμένους τομείς που θα πρέπει να ελέγχονται από κάθε ISMS, ώστε το σύστημα να εκπληρώνει τις απαιτήσεις της ασφάλειας πληροφοριών. Πιο συγκεκριμένα:

- **Information Security Policy:** Ουσιαστικά πρόκειται για τον τρόπο που η ηγεσία ενός οργανισμού κάνει γνωστές τις προθέσεις της γύρω από την ασφάλεια πληροφοριών και δίνει κατεύθυνση στη διοίκηση και στους εργαζομένους σχετικά με αυτή.
- **Communications and Operations Management:** Η πολιτική του οργανισμού σε σχέση με την ασφαλή και σωστή λειτουργία των εγκαταστάσεων που αφορούν την επεξεργασία πληροφοριών.

- **Access Control:** Το σύστημα που επιτρέπει ή μη την πρόσβαση ατόμων σε μέρη του οργανισμού είτε σε φυσικές εγκαταστάσεις είτε στους υπολογιστικούς πόρους του πληροφοριακού συστήματος.
- **Information System Acquisition, Development and Maintenance:** Μια ολοκληρωμένη διαδικασία που αφορά την απόκτηση αρχικά και στη συνέχεια την εξέλιξη και διατήρηση του πληροφοριακού συστήματος σε τεχνικό επίπεδο.
- **Organization of Information Security:** Η υλοποίηση της ασφάλειας πληροφοριών εντός του οργανισμού με διαφοροποίηση για τους εργαζομένους σε αυτόν και τα συνεργαζόμενα μέλη εκτός αυτού.
- **Asset Management:** Αφορά την αναγνώριση, την ταξινόμηση και την εκχώρηση υλικών πόρων σε μια δομή ώστε να εξασφαλιζεται η προστασία τους.
- **Information Security Incident Management:** Αποτελεί ένα πρόγραμμα διαχείρισης συμβάντων ή ατυχημάτων σε σχέση με την ασφάλεια πληροφοριών. Αναγνωρίζει τους πόρους που απαιτούνται για τη διαχείριση ενός συμβάντος και φροντίζει για τη μελλοντική αποτροπή παρόμοιου περιστατικού.
- **Business Continuity Management:** Διασφαλίζει τη συνέχεια και την επιβίωση της εταιρίας κάτω από μη κανονικές και προβληματικές συνθήκες, σχεδίαζει την άμεση ανόρθωση του οργανισμού και ελαχιστοποιεί τη ζημία σε όλα τα επίπεδα ως απόρροια αυτών των συνθηκών.
- **Human Resources Security:** Σχετίζεται με τη διασφάλιση πως όλοι οι εργαζόμενοι γνωρίζουν το ρόλο και τα καθήκοντα τους όσον αφορά την ασφάλεια πληροφοριών. Επίσης η άδεια πρόσβασης σε χώρους και συστήματα του οργανισμού αφαιρείται με τον τερματισμό της εργασίας σε αυτόν.
- **Physical and Environmental Security:** Μέτρα που απαιτούνται για την προστασία συστημάτων, πόρων και κτηριακών εγκαταστάσεων από φυσικές απειλές που προέρχονται από ανθρώπους ή το περιβάλλον.
- **Compliance:** Αφορά τη συμμόρφωση του οργανισμού αφενός με νομικές διατάξεις, κανόνες και συμβόλαια και αφετέρου με τις πολιτικές, τα πρότυπα

και τις διαδικασίες της ασφάλειας πληροφοριών (Information Security Management System ISO 27001:2005, 2015).

Μια προσέγγιση της ασφάλειας πληροφοριών χωρίς το απαραίτητο management είναι πολύ πιθανό να οδηγήσει σε μια μερική υλοποίηση ελέγχων ασφαλείας και σαν αποτέλεσμα δε θα αναγνωριστούν όλοι οι κίνδυνοι ή/και κάποια μέτρα που θα παρθούν θα είναι ακατάλληλα ή μη αποτελεσματικά (Ashenden, 2008).

2.2. Τα πρότυπα Ασφάλειας Πληροφοριών (Information Security Standards)

Πρότυπο καλείται ένα έγγραφο που παρέχει πληροφορίες σχετικά με τις απαιτήσεις, τις προδιαγραφές και τις οδηγίες που μπορούν να ακολουθηθούν με συνέπεια, ώστε να εξασφαλιστεί πως τα υλικά, τα προϊόντα, οι διαδικασίες και οι υπηρεσίες ενός οργανισμού λειτουργούν ή χρησιμοποιούνται ορθολογικά και με κυρίαρχο κριτήριο το λόγο ύπαρξης τους. Ουσιαστικά, η προτυποποίηση αποτελεί μια δραστηριότητα που δίνει λύσεις σε υπαρκτά ή προσδοκώμενα προβήματα από την οπτική της δημιουργίας των ρεαλιστικά πιο ευνοϊκών συνθηκών λειτουργίας. Με βάση τα παραπάνω, τα πρότυπα στην ασφάλεια πληροφοριών παρέχουν μια προσέγγιση του ISMS με σκοπό την υιοθέτηση των καλύτερων δυνατών πρακτικών, την προσοτικοποίηση του αποδεκτού ορίου κινδύνων και την υλοποίηση κατάλληλων μέτρων για την προστασία της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των πληροφοριών (Pinheiro & Ribeiro, 2015). Για παράδειγμα, ο Παγκόσμιος Οργανισμός Προτυποποίησης (ISO – International Organization for Standardization) έχει δημιουργήσει για την ασφάλεια πληροφοριών το πρότυπο ISO/IEC 27001, που παρέχει πληροφορίες σχετικά με τα χαρακτηριστικά και τις απαιτήσεις που χρειάζεται ένας οργανισμός για να κατασκευάσει το δικό του ISMS. Το πρότυπο ISO/IEC 27001 θα περιγραφεί εκτενώς στο Κεφάλαιο 3.

Σύμφωνα με το πρότυπο ISO/IEC 27003 που αποτελεί τον οδηγό της υλοποίησης του ISO/IEC 27001 για το ISMS ενός οργανισμού, υπάρχουν 5 βασικά βήματα που πρέπει να γίνουν από τον οργανισμό για την ολοκλήρωση της διαδικασίας απόκτησης ISMS σύμφωνα με το πρότυπο. Αυτά είναι:

1. Απόκτηση άδειας από τη διοίκηση για την εκκίνηση του ISMS πρότζεκτ.
2. Ορισμός της έκτασης και των ορίων του ISMS και δημιουργία της πολιτικής που θα ακολουθηθεί.
3. Υλοποίηση της ανάλυσης των απαιτήσεων για την ασφάλεια πληροφοριών.
4. Υλοποίηση της αξιολόγησης κινδύνων και σχεδιασμός της αντιμετώπισης τους.
5. Σχεδιασμός του ISMS (Asosheh et al., 2013).

Υπάρχουν κάποια κριτήρια που αποδεικνύουν πως το πρότυπο που ακολουθεί ένας οργανισμός για το σύστημα διαχείρισης της ασφάλειας πληροφοριών του είναι επιτυχημένο και κατά συνέπεια είναι επιτυχημένο και το ISMS του. Πιο συγκεκριμένα, ένα τέτοιο συμπέρασμα μπορεί να εξαχθεί από τις ακόλουθες παρατηρήσεις:

- Το πρότυπο ακολουθείται πιστά χωρίς να δημιουργεί επιπλοκές στις καθημερινές λειτουργίες του οργανισμού.
- Η υλοποίηση του προτύπου αποφέρει θετική απόδοση της επένδυσης.
- Τα μέτρα προστασίας των πληρογοριακών στοιχείων του οργανισμού είναι οικονομικά προσιτά για τον οργανισμό.
- Το πρότυπο είναι εφαρμόσιμο σε όλα τα τμήματα του οργανισμού.
- Ο έλεγχος τήρησης του προτύπου από επιτροπή εκτός του οργανισμού είναι μια ασφαλής διαδικασία για τον οργανισμό (Humphreys, 2011).

Στην επόμενη ενότητα θα περιγραφούν τα πιο σημαντικά πρότυπα στο πεδίο της ασφάλειας πληροφοριών.

2.3. Περιγραφή των σημαντικότερων προτύπων

Τα δέκα σημαντικότερα πρότυπα στην ασφάλεια πληροφοριών είναι το BS7799, το ISO27001, το PCI-DSS, το COBIT, το ITIL, το SOA, το PRINCE2, το COSO, το OPM3 και το CMMI. Ακολουθεί αναλυτική περιγραφή τους.

- **BS7799**

Το BS αποτελεί συντομογραφία του British Standard (Βρετανικό Πρότυπο). Εκδόθηκε απο το Βρετανικό Ινστιτούτο Προτυποποίησης (BSI) το 1995. Ένας από τους κύριους συγγραφείς του προτύπου αναφέρει το 1993 πως εκπρόσωποι 7 διαφορετικών κλάδων της βρετανικής βιομηχανίας εγκρίνουν την ιδέα της έκδοσης ενός συνόλου από μέτρα ελέγχου της ασφάλειας πληροφοριών και την παραγωγή ενός εγγράφου με τη συλλογή 100 περίπου τέτοιων μέτρων (Tajammul & Parveen, 2017). Στο μέρος πρώτο αυτού του προτύπου (Info technology – Code for practice for ISM), που κυκλοφόρησε το 1998, βασίστηκε το ISO/IEC 1799:2000, το πρώτο πρότυπο της σειράς ISO-27K και στη συνέχεια το δεύτερο μέρος που εκδόθηκε το 1999 (ISMS – Specification with guidance for use) αργότερα απορροφήθηκε από το ISO27001 το 2005 και έκτοτε δε χρησιμοποιείται (Susanto et al., 2011).

- **ISO/IEC-27001 Series**

Αποτελεί τον καλύτερο και πιο εκσυγχρονισμένο οδηγό διαχείρισης ασφάλειας πληροφοριών και βασίζεται στη διαχείριση κινδύνου μέσω της ανάληψης κατάλληλων μέτρων προστασίας. Η ιδέα του προτύπου και τα όρια εφαρμογής του είναι αρκετά πιο ευρεία από το πεδίο της ασφάλειας του τμήματος IT (cyber security). Ακόμη, πρόκειται για ένα πρότυπο εφαρμόσιμο σε όλους τους οργανισμούς ανεξάρτητα από το μέγεθος τους. Οι οργανισμοί που επιθυμούν να ακολουθήσουν το πρότυπο και να πιστοποιηθούν μαζί του οφείλουν να αξιολογήσουν τους κινδύνους που αφορούν την ασφάλεια πληροφοριών τους και να τους αντιμετωπίσουν λαμβάνοντας τα κατάλληλα μέτρα (Tajammul & Parveen, 2017).

Το πρότυπο αυτό θα αναλυθεί εκτενώς στο κεφάλαιο 3.

- **PCI-DSS**

Αποτελεί συντομογραφία του Payment Card Industry and Data Security Standard. Οποιοσδήποτε οργανισμός, πριν επεξεργαστεί τη χρεωστική ή την

πιστωτική κάρτα κάποιου πελάτη, πρέπει να έχει πιστοποιηθεί από το PCI-DSS. Το συγκεκριμένο πρότυπο σχεδιάστηκε αποκλειστικά για να σταματήσει την κλοπή ή την απάτη που σχετίζεται με χρεωστικές και πιστωτικές κάρτες. Ορισμένες από τις βασικές λειτουργίες που ορίζει το πρότυπο είναι η προστασία των δεδομένων κάθε χρήστη κάρτας, η διατήρηση ενός ασφαλούς δικτύου συναλλαγών με συνεχές testing και μετρήσεις και οι αυστηροί κανόνες πρόσβασης όσον αφορά τις κάρτες. Πρόκειται για πρότυπο στην ασφάλεια πληροφοριών που χρησιμοποιείται σε παγκόσμια κλίμακα, εφαρμόσιμο σε κάθε οργανισμό που κατέχει, επεξεργάζεται ή ανταλλάζει πληροφορίες πιστωτικών και χρεωστικών καρτών (Tajammul & Parveen, 2017).

- **COBIT**

Δημιουργήθηκε από το IT Governance Institute το 1996 και αποτελεί μια βάση γνώσης πάνω στο management και στη δομή διοίκησης του IT (IT Governance). Δίνεται έμφαση σε πέντε τομείς:

1. Strategic alignment: Επικεντρώνεται στην ομαλή σύνδεση των στόχων του οργανισμού με τα πλάνα του τμήματος IT.
2. Value delivery: Αφορά την ελαχιστοποίηση των εξόδων και την απόδειξη της ουσιαστικής αξίας του IT.
3. Resource Management: Επιδιώκει τη βέλτιστη χρησιμοποίηση των πόρων.
4. Risk Management: Ασχολείται με πιθανούς κινδύνους για τον οργανισμό.
5. Performance Measurement: Καταγράφει και αξιολογεί την υλοποίηση της στρατηγικής σε όλα τα στάδια (Susanto et al., 2011).

- **ITIL**

Πρόκειται για μια συλλογή βιβλίων, το καθένα από τα οποία επικεντρώνεται σε μια συγκεκριμένη πρακτική που αφορά τη διαχείρηση των υπηρεσιών του τμήματος IT (IT services management), το IT development και το IT operations με έμφαση την ασφάλεια. Έχει οκτώ βασικά περιεχόμενα:

1. Application Management.
2. Security Management.
3. ICT Infrastructure Management.

4. Secure Supply.
5. Secure Delivery.
6. Planning to implement secure management.
7. Assets Management.
8. Small Scale Implementation (Susanto et al., 2011).

- **SOA**

Αποτελεί ένα είδος λογισμικού , όπου οι εφαρμογές χρησιμοποιούν τις διάφορες υπηρεσίες στο δίκτυο βάσει ενός πρωτόκολλου επικοινωνίας. Η ιδέα του SOA (Service Oriented Architecture) μοιάζει με δύο βασικές αρχές του software engineering. Αρχικά, όπως για την υλοποίηση ενός μικρού προγράμματος ή πρότζεκτ δεν απαιτούνται επίσημες καταγραφές στο software engineering, έτσι και για τη χρησιμοποίηση μιας μικρής υπηρεσίας δεν απαιτείται η υλοποίηση του SOA. Ωστόσο, για παράδειγμα για μια μεγάλη υπηρεσία cloud computing το SOA πρέπει να υλοποιείται. Δεύτερον, όπως για τη δημιουργία ενός προϊόντος λογισμικού απαιτείται στην αρχή ένα επίσημο έγγραφο το SRS (Software Requirement Specification), έτσι και το SOA αποτελεί ένα νόμιμο έγγραφο που αποδεικνύει τη συμφωνία μεταξύ client και server στο κομμάτι των υπηρεσιών cloud computing. Ουσιαστικά, στο SOA εμπλέκονται τρία μέλη: ο service provider, ο broker(διαχειριστής της υπηρεσίας) και ο service requester (Aljazzaf & et al., 2016).

- **PRINCE2**

Το PRINCE2 προκύπτει από συντομογραφία του Project in Controlled Environment. Πρόκειται για μια αποδοτική μέθοδο για την ανάπτυξη ενός πρότζεκτ ή με πιο απλά λόγια ένα είδος project management. Αποτελείται από 21 στοιχεία και συγκεκριμένα από επτά αρχές, επτά θέματα και από επτά διαδικασίες που σχηματίζει ο συνδυασμός των προηγούμενων δύο.

Οι επτά αρχές:

1. Έμφαση στο προϊόν.
2. Διαχείριση με στάδια.

3. Προσαρμογή στο περιβάλλον του πρότζεκτ.
4. Προσοχή στις εξαιρέσεις.
5. Ορισμός ρόλων και ευθυνών.
6. Εκμάθηση μέσω εμπειρίας.
7. Συνέχεια των λόγων ύπαρξης του πρότζεκτ.

Τα επτά θέματα:

1. Business case.
2. Ποιότητα.
3. Πρόοδος.
4. Οργανισμός.
5. Αλλαγή.
6. Σχέδιο.
7. Κίνδυνος.

Οι επτά διαδικασές:

1. Αρχικοποίηση του πρότζεκτ.
2. Εκκίνηση του πρότζεκτ.
3. Καταγραφή του πρότζεκτ.
4. Παρακολούθηση των σταδίων.
5. Διαχείριση θεμάτων που σχετίζονται με τη διανομή του προϊόντος.
6. Διατήρηση των ορίων κάθε στάδιου.
7. Επιτυχής τερματισμός του πρότζεκτ (Tajammul & Parveen, 2017).

- **COSO**

Το πρότυπο COSO (Committee Of Sponsory Organization) αποτελεί ένα ολοκληρωμένο πλαίσιο βασισμένο στη διοίκηση που παρέχει γνώση και οδηγίες γύρω από την ηγεσία. Σε αντίθεση με τις προσεγγίσεις που βασίζονται σε μετρικές κινδύνου, θέτει το risk management ως μια διαδικασία που επηρεάζεται από τους διευθύνοντες και το υπόλοιπο προσωπικό και εφαρμόζεται στη δημιουργία στρατηγικής παντού μέσα στον οργανισμό με σκοπό την αναγνώριση πιθανών κινδύνων. Ακόμη, οριοθετεί τον κίνδυνο βάσει της διάθεσης που επιδεικνύει ο οργανισμός ώστε να επιτύχει τους διάφορους στόχους του. Οι τρεις θεμελιώδεις ιδέες

του είναι: η αντίληψη του οργανισμού γύρω από τους κινδύνους, το θέσιμο στόχων εκ των προτέρων που πιθανοί μελλοντικοί κίνδυνοι δε θα επηρεάσουν και η αναγνώριση εσωτερικών και εξωτερικών παραγόντων που μπορεί να επηρεάσουν την εξέλιξη του προϊόντος (Hayne & Free, 2014).

- **OPM3**

Το OPM3 (Organizational Project Management Maturity Model) είναι ένα ευρέως αποδεκτό πρότυπο ως η καλύτερη πρακτική να υλοποιήσει ένας οργανισμός τις πολιτικές και στρατηγικές του όσον αφορά το portfolio management (διαχείριση χρημάτων και επενδύσεων). Αυτό το επιτυγχάνει μέσα από μια σειρά κατάλληλων προτύπων διοίκησης, ολοκληρωμένων διαδικασιών και μέτρα μέτρησης της επίδοσης (Tajammul & Parveen, 2017).

- **CMMI**

Το CMMI προκύπτει από τη συντομογραφία του Capability Maturity Model Integration και περιλαμβάνει μεθόδους αξιολόγησης, μοντέλα βελτίωσης των διαδικασιών και εκπαιδευτικό υλικό με στόχο την ανάπτυξη παραγωγικής και αποδοτικής συμπεριφοράς μέσα στον οργανισμό που μειώνει τους κινδύνους που αφορούν το λογισμικό, τα προϊόντα και τις υπηρεσίες. Το CMMI ουσιαστικά είναι ένα σύνολο από ποικίλλα μοντέλα, ώστε κάθε οργανισμός να αναγνωρίζει αυτό που του ταιριάζει περισσότερο, και αποσκοπεί στη βελτίωση της απόδοσης είτε αυτό αφορά το λογισμικό είτε τα προϊόντα και τις υπηρεσίες (Wallshein & Loerch, 2015).

2.4. Σύγκριση βασικών χαρακτηριστικών των σημαντικότερων προτύπων

Παρακάτω (βλ. Εικόνα 3) επιχειρείται μια σύγκριση των προτύπων ISO27001, BS7799, PCIDSS, ITIL και COBIT σε σχέση με τους έντεκα θεμελιώδεις τομείς που θα πρέπει να εξυπηρετεί το ISMS ενός οργανισμού, όπως περγράφηκαν στην πρώτη ενότητα του Κεφαλαίου 2.

		ISO 27001	BS 7799	PCIDSS V2.0	ITIL V4.0	COBIT V4.1
1.	*Information Security Policy*	√	√	√	√	√
2.	*Communications and Operations Management*	√	√	√	●	√
3.	*Access Control*	√	√	√	√	√
4.	*Information Systems Acquisition, Development and Maintenance*	√	√	√	●	√
5.	*Organization of Information Security*	√	√	√	√	√
6.	*Asset Management*	√	√	√	√	√
7.	*Information Security Incident Management*	√	●	√	√	√
8.	*Business Continuity Management*	√	√	√	√	√
9.	*Human Resources Security*	√	√	√	●	√
10.	*Physical and Environmental Security*	√	√	√	●	√
11.	*Compliance*	√	√	√	√	√

Εικόνα 3 - Σύγκριση βασικών χαρακτηριστικών στα πρότυπα ασφάλειας πληροφοριών

Όπως παρατηρούμε, με εξαίρεση το πρότυπο ITIL που ομολογουμένως δίνει αποκλειστικά έμφαση στο τμήμα IT του κάθε οργανισμού, τα υπόλοιπα πρότυπα ικανοποιούν σε καθολικό βαθμό τους έντεκα τομείς, κάτι που αποδεικνύει βέβαια το λόγο που είναι τόσο ευρέως διαδεδομένα στον κόσμο των οργανισμών και των επιχειρήσεων.

Κάθε πρότυπο έχει συγκεκριμένο ρόλο και θέση στην υλοποίηση ενός ISMS. Μερικά πρότυπα όπως το ISO27001 και το BS7799 δίνουν έμφαση στην ασφάλεια πληροφοριών ως βασικό πυλώνα του οργανισμού, ενώ το PCIDSS εξετάζει την ασφάλεια πληροφοριών σε σχέση με τις συναλλαγές μέσω καρτών και τα ITIL και COBIT σε σχέση με τη διαχείρηση πρότζεκτ και τη διοίκηση του τμήματος IT. Αδιαμφισβήτητα, το ISO/IEC 27001 αποτελεί τον κύριο εκπρόσωπο των προτύπων

στην ασφάλεια πληροφοριών, μια παγκόσμια γλώσσα στα πρότυπα ISMS, με το μέγεθος χρήσης και εμπιστοσύνης να αγγίζει το 80% του σύγχρονου κόσμου (Susanto et al., 2011).

Κεφάλαιο 3: Το πρότυπο ISO/IEC 27001

3.1. Ιστορική αναδρομή και εξέλιξη

Ο Παγκόσμιος Οργανισμός Προτυποποίησης (International Organization for Standardization) ή εν συντομία ISO ιδρύθηκε το 1947 και αποτελεί τον μεγαλύτερο δημιουργό διεθνών προτύπων παγκοσμίως. Από την ίδρυση του μέχρι και σήμερα έχει εκδώσει 23418 διεθνή πρότυπα που καλύπτουν σχεδόν όλα τα θέματα των επιχειρήσεων και της τεχνολογίας. Στις μέρες μας, διατηρεί μέλη από τουλάχιστον 165 χώρες, ενώ τα κεντρικά γραφεία του οργανισμού βρίσκονται στη Γενεύη της Ελβετίας. Η αλληλοεπικάλυψη θεμάτων προτυποποίησης σχετικά με την τεχνολογία πληροφοριών με τη Διεθνή Ηλεκτροτεχνική Επιτροπή (IEC – Electrotechnical Commision) οδήγησε στη δημιουργία μιας κοινής τεχνικής επιτροπής ISO/IEC σχετική με τον τομέα τεχνολογίας πληροφορίας (http://www.iso.org/the-iso-story.html).

Το διεθνές πρότυπο ISO/IEC 27001 προέρχεται από το BS7799, μια βρετανική διάταξη με το όνομα “Information security management – Code of practice for information security management” που εκδόθηκε από το BSI (British Standard Institute) το 1995 εξαιτίας της ανάγκης των οργανισμών στη Βρετανία να διαθέτουν έναν επίσημο κατάλογο από ελέγχους ασφαλείας για την προστασία των πληροφοριών τους. Το 1998, το BSI δημιουργεί μια νέα έκδοση το BS7799-2:1998 “Information security management system – Specifications” , όπου εισάγονται κάποιες νέες έννοιες σχετικές με την ασφάλεια πληροφοριών, όπως για παράδειγμα ο έλεγχος πρόσβασης στο σύστημα και η συμμόρφωση. Λόγω της τεχνολογικής εξέλιξης, που δημιούργησε την ανάγκη για ανανέωση των ελέγχων ασφαλείας, το 1999 το BS7799-2 αναβαθμίζεται και το ίδιο συμβαίνει και το 2002, ώστε το πρότυπο να συμβαδίζει με τα ISO 9002 (διαχείριση ποιότητας) και ISO 14001 (περιβαλλοντική διαχείριση). Το 2005 η επιτροπή του ISO/IEC υιοθετεί το πρότυπο BS7799-2 και εκδίδει την πρώτη έκδοση ISO/IEC 27001:2005 που δεν έχει σημαντικές αλλαγές σε σχέση με το βρετανικό πρότυπο κυρίως λόγω σεβασμού. Τελικά, το 2013 κυκλοφορεί η τρέχουσα έκδοση, το ISO/IEC 27001:2013, που περιέχει νέες προϋποθέσεις για την αξιολόγηση απόδοσης μαζί με την αφαίρεση

κάποιων προληπτικών ενεργειών και τη μείωση των προαπαιτούμενων που σχετίζονται με την αξιολόγηση κινδύνου (Accerboni & Sartor, 2019).

Το πρότυπο ISO/IEC 27001 αποτελεί μέλος της οικογένειας προτύπων ISO/IEC 2700x-series που σχετίζεται με την ασφάλεια πληροφοριών. Πιο συγκεκριμένα σε αντιστοίχιση με το σκοπό τους τα πρότυπα της οικογένειας διαιρούνται σε τέσσερις κύριες περιοχές:

1. Ορολογία: Εδώ ανήκει το πρότυπο ISO/IEC 27000, που αποτελεί στην ουσία ένα λεξικό των όρων που χρησιμοποιεί η σειρα των 2700x.
2. Προαπαιτούμενα: Εκτός από το ISO/IEC 27001, σε αυτή την κατηγορία εμπίπτουν και τα ISO/IEC 27006 και ISO/IEC 27009 που περιέχουν τις προαπαιτήσεις του σώματος ελέγχου και πιστοποίησης και της εφαρμογής του ISO/IEC 27001 σε συγκεκριμένο τομέα αντίστοιχα.
3. Γενικές οδηγίες: Το ISO/IEC 27002 παρέχει γενικές οδηγίες σχετικές με την υλοποίηση της ασφάλειας πληροφοριών, το ISO/IEC 27003 σχετικές με τον ορισμό της υλοποίησης ενός ISMS πρότζεκτ, το ISO/IEC 27004 σχετικές με τη μέτρηση της απόδοσης και της επίδρασης του ISMS, το ISO/IEC 27005 σχετικές με την αξιολόγηση κινδύνου, το ISO/IEC 27007 σχετικές με τον τρόπο που μια επιτροπή αξιολόγησης προτυποποίησης ελέγχει τη συμμόρφωση ή όχι ενός ISMS με το ISO/IEC 27001 και τέλος το ISO/IEC 27008 σχετικές αποκλειστικά με τις διαδικασίες ελέγχων των μέτρων ασφαλείας. Όλα τα παραπάνω πρότυπα ουσιαστικά παρέχουν οδηγίες που βασίζονται στις απαιτήσεις του ISO/IEC 27001.
4. Οδηγίες τομέα: Αφορά μια σειρά οδηγιών που αφορούν ένα συγκεκριμένο τομέα. Για παράδειγμα το ISO/IEC 27011 παρέχει κατευθυντήριες γραμμές για τον τομέα τηλεπικοινωνιών ενός οργανισμού (Accerboni & Sartor, 2019).

3.2. Βασικές έννοιες και χαρακτηριστικά

Το ISO/IEC 27001, γνωστό και ως The Standard, είναι σχεδιασμένο για χρήση σε οργανισμούς όλων των μεγεθών, ειδών και φύσης και σε κάθε τμήμα αυτών σε οποιαδήποτε χώρα στον κόσμο. Πρόκειται για ένα σύστημα διοίκησης (management system) και όχι για μια εξειδίκευση στην τεχνολογία, κάτι που αντανακλάται και στον επίσημο τίτλο του προτύπου, ο οποίος είναι Information

technology – Security techniques – Information Security Management Systems – Requirements. Ακόμη, το ISO/IEC 27001 ορίζει τις προδιαγραφές για το ISMS σε έναν οργανισμό και καθορίζει απαιτήσεις. Ένα σύνολο οδηγιών ή πρακτικών επιτρέπει σε έναν οργανισμό να επιλέξει ποια στοιχεία ενός προτύπου θα υλοποιήσει και ποια όχι, ωστόσο το ISO/IEC 27001 δεν αφήνει τέτοια περιθώρια. Οποιοσδήποτε οργανισμός θέλει να υλοποιήσει ένα ISMS σύμφωνα με το ISO/IEC 27001 πρέπει να ακολουθήσει τις προδιαγραφές που περιέχονται στο πρότυπο (Vasudevan et al., 2015).

Το πρότυπο ορίζει πως ο σχεδιασμός και η υλοποίηση του ISMS είναι άρρηκτα συνδεδεμένα με τις ανάγκες και στόχους, τις απαιτήσεις για ασφάλεια, τις οργανωτικές διαδικασίες και τη δομή και μέγεθος κάθε οργανισμού. Το ISO/IEC 27001 δεν είναι μια ίδια λύση για όλους και το σημαντικότερο είναι πως δεν είναι στατικό. Αναγνωρίζει ότι το ISMS θα αναπτυχθεί με κριτήριο τις ανάγκες του οργανισμού και ότι αν αυτές οι ανάγκες αλλάξουν με το πέρασμα του χρόνου τότε και το ISMS θα τροποποιηθεί (Vasudevan et al., 2015).

Με απλά λόγια, το ISO/IEC 27001 είναι ένα χρήσιμο μοντέλο για την εγκαθίδρυση, την υλοποίηση, τη διατήρηση και τη συνεχή βελτίωση ενός ISMS. Είναι ένα μοντέλο που μπορεί να εφαρμοστεί και να κατανοηθεί παντού παγκοσμίως (Vasudevan et al., 2015). Σύμφωνα με τους Accerboni και Sartor (2019) το ISO/IEC 27001 είναι ένα εθελοντικό, διεθνές και πιστοποιήσιμο πρότυπο για τη δημιουργία και τη διαχείριση ενός ISMS που περιλαμβάνει πολλές πτυχές σχετικά με:

- Την ασφάλεια σε λογικό επίπεδο: Σύνολο μέτρων για την προστασία της ακεραιότητας και της εμπιστευτικότητας των ψηφιακών πληροφοριών.
- Την ασφάλεια σε φυσικό επίπεδο: Σύνολο λύσεων που στοχεύουν στην αποτροπή της μη εξουσιοδοτημένης πρόσβασης σε φυσικές τοποθεσίες.
- Την ασφάλεια σε οργανωτικό επίπεδο: Σύνολο ρόλων, καθηκόντων και υποχρεώσεων που ορίζουν τις πολιτικές και διαδικασίες ασφαλείας σε έναν οργανισμό.

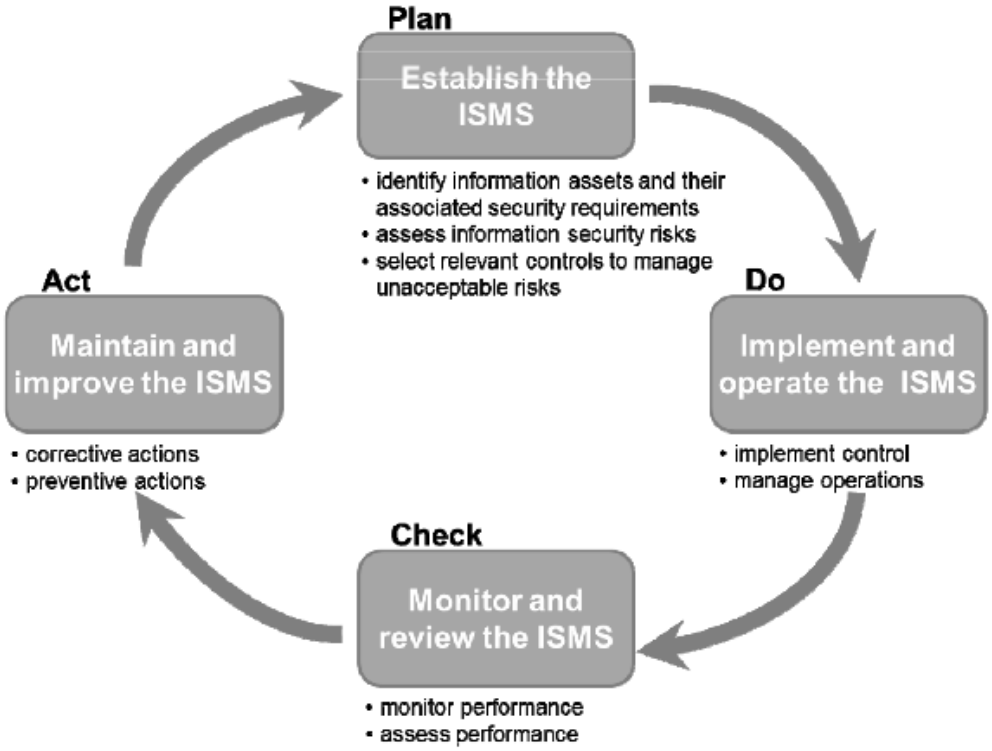
Οποιοσδήποτε οργανισμός επιθυμεί την πιστοποίηση με το ISO/IEC 27001 για το ISMS του θα χρειαστεί μια προσέγγιση στην αξιολόγηση κινδύνου (risk assessment) που καλύπτει τις απαιτήσεις του προτύπου. Το ISO/IEC 27001 ορίζει ως απαίτηση την αναλυτική αξιολόγηση κινδύνου για την επιλογή κατάλληλων ελέγχων

ασφάλειας πληροφοριών (Vasudevan et al., 2015).

Όσον αφορά τη δομή του προτύπου, το ISO/IEC 27001 χωρίζεται σε δέκα κεφάλαια και ένα παράρτημα. Τα πρώτα τρία κεφάλαια σχετίζονται με το πεδίο και την εμβέλεια του ISMS και τους όρους και ορισμούς που χρησιμοποιεί το πρότυπο σε πλήρη αντιστοίχιση με το ISO/IEC 27000. Τα υπόλοιπα επτά κεφάλαια αφορούν τις βασικές απαιτήσεις του ISMS που ορίζει το πρότυπο, όπως το περιεχόμενο του οργανισμού, η ηγεσία, ο σχεδιασμός, η υποστήριξη, η αξιολόγηση της απόδοσης και η βελτίωση (Accerboni & Sartor, 2019). Το παράρτημα έχει την ονομασία Annex A και περιλαμβάνει 39 στόχους ασφάλειας και 134 μέτρα για την ασφάλεια πληροφοριών (Disterer, 2013).

3.3. Ο κύκλος PDCA (PDCA cycle)

Η κύρια ιδέα του ISO/IEC 27001 είναι ο σχεδιασμός, η υλοποίηση, η λειτουργία και η συνεχής παρακολούθηση και βελτίωση του ISMS. Η προσέγγιση αυτών πρέπει να είναι συνυφασμένη με τον κύκλο PDCA (βλ. Εικόνα 4). Ο κύκλος PDCA περιλαμβάνει τα στάδια Plan, Do, Check και Act (Disterer, 2013).



Εικόνα 4 – Ο κύκλος PDCA σύμφωνα με το ISO27000

Πιο αναλυτικά για το ISO/IEC 27001 ο κύκλος αυτός σημαίνει:

1. **Plan (Ίδρυση του ISMS):** Ορισμός των ορίων του πεδίου, των πολιτικών, των σκοπών και των διαδικασιών σχετικών με την ασφάλεια πληροφοριών και υλοποίηση της αξιολόγησης κινδύνου, τα αποτελέσματα της οποίας θα καθορίσουν τους στόχους του οργανισμού στην ασφάλεια πληροφοριών σε συνδυασμό με τους γενικούς στόχους του.
2. **Do (Υλοποίηση και λειτουργία του ISMS):** Στο στάδιο αυτό βρίσκεται σε λειτουργία το ISMS, εκτελούνται οι διαδικασίες και διεργασίες σύμφωνα με την πολιτική ασφαλείας που αποφασίστηκε στο σχεδιασμό και υλοποιούνται τα μέτρα ελέγχου που πάρθηκαν ύστερα από την αξιολόγηση κινδύνων.
3. **Check (Καταγραφή και αξιολόγηση του ISMS):** Αξιολόγηση της απόδοσης του ISMS ακόμα και με μετρικές όπου είναι δυνατόν αυτό και αποστολή αναφοράς σχετικά με τα αποτελέσματα στη διοίκηση. Αυτή η αναφορά κρίνει την αποτελεσματικότητα του ISMS και των μέτρων ελέγχου που έχουν παρθεί και εκτελούνται.
4. **Act (Διατήρηση και βελτίωση του ISMS):** Στο στάδιο αυτό λαμβάνονται διορθωτικές και προληπτικές αποφάσεις με βάση τα αποτελέσματα της αναφοράς που δόθηκε στη διοίκηση με σκοπό τη βελτίωση του ISMS (Vasudevan et al., 2015).

3.4. Οι απαιτήσεις του προτύπου

Όπως αναφέρθηκε στην ενότητα 3.2. το πρότυπο ISO/IEC 27001 χωρίζεται σε δύο μέρη. Το πρώτο μέρος περιλαμβάνει την εισαγωγή και δέκα ακόμα κεφάλαια και το δεύτερο το παράρτημα Annex A με τον κατάλογο των στόχων και των μέτρων ελέγχου. Η Giesler (2019) και οι Accerboni και Sartor (2019) περιγράφουν τις βασικές απαιτήσεις του προτύπου, που αποτελούν τα κεφάλαια τέσσερα έως δέκα, και είναι υποχρεωτικές αν κάποιος οργανισμός θέλει να αποκτήσει ένα ISMS συμβατό με το πρότυπο.

Κεφάλαιο 4: Context of the organization (Περιεχόμενο του οργανισμού)

Η κατανόηση των περιεχομένων του οργανισμού αποτελεί μία από τις βασικές απαιτήσεις του ISO/IEC 27001, δηλαδή η αναγνώριση και η γνώση των εσωτερικών και εξωτερικών πτυχών και θεμάτων του οργανισμού όσο και των άμεσα ή έμμεσα ενδιαφερόμενων εντός και εκτός αυτού (interested parties). Για το λόγο αυτό ο οργανισμός πρέπει αρχικά να ορίσει με ακρίβεια το πεδίο εφαρμογής του ISMS του (Scope). Σε πολλές περιπτώσεις οργανισμών το ISMS εφαρμόζεται μόνο σε ένα ή περισσότερα τμήματά τους.

Κεφάλαιο 5: Leadership (Ηγεσία)

Οι απαιτήσεις που ορίζει το πρότυπο σχετικά με την επαρκή ηγεσία είναι ποικίλλες. Η αφοσίωση των πολύ υψηλά ιστάμενων στην επιτυχία του ISMS είναι απαραίτητη. Το top management, όπως καλούνται οι άνθρωποι σε πολύ υψηλές θέσεις μέσα στον οργανισμό, οφείλουν να εξασφαλίζουν τους, απαραίτητους για το ISMS, υλικούς και ανθρώπινους πόρους καθώς και τις απαραίτητες υπηρεσίες από εξωτερικά συνεργαζόμενα σώματα και άλλους οργανισμούς. Επίσης, οι στόχοι του ISMS πρέπει να συμβαδίζουν με τους γενικούς στόχους του οργανισμού. Η έγγραφη δημιουργία πολιτικής γύρω από την ασφάλεια πληροφοριών είναι υποχρεωτική και η πολιτική αυτή πρέπει να είναι γνωστή σε όλους τους άμεσα και έμμεσα εμπλεκόμενους με τον οργανισμό. Τέλος, το πρότυπο απαιτεί τον καθορισμό των ρόλων και υποχρεώσεων, ώστε να αξιολογείται και η απόδοση των αντίστοιχων ανθρώπων.

Κεφάλαιο 6: Planning (Σχεδιασμός)

Ο στρατηγικός σχεδιασμός μέσα στο περιβάλλον ενός ISMS απαιτεί την υλοποίηση αξιολόγησης κινδύνου που γνωστοποιεί και κατατάσσει απειλές και κινδύνους. Η αξιολόγηση αυτή καθορίζει και τους στόχους της ασφάλειας πληροφοριών του οργανισμού και στη συνέχεια παράγεται το πλάνο αντιμετώπισης κινδύνων βασισμένο στο Annex A. Σε αυτό το στάδιο παράγεται το SoA (Statement of Applicability) που περιέχει τα μέτρα που έχουν ληφθεί σύμφωνα με το Annex A που είναι εφαρμόσιμα και υλοποιήσιμα στο πλαίσιο του οργανισμού.

Κεφάλαιο 7: Support (Υποστήριξη)

Οι πόροι, οι ικανότητες και η συναίσθηση των εργαζομένων και η καλή επικοινωνία είναι πολύ σημαντικά θέματα για την υποστήριξη του ISMS. Εξίσου σημαντική είναι η αρχειοθέτηση και η εγγραφή των πληροφοριών που χρειάζονται κατά την καθημερινή λειτουργία του οργανισμού. Ένα οργανωμένο σύνολο εγγράφων συνεισφέρει στην επιτυχημένη πορεία του ISMS. Για παράδειγμα, η καταγραφή των αποτελεσμάτων μιας συνάντησης (meeting) απαιτεί την υπογραφή όσων παρευρέθηκαν για την εγκυρότητα του εγγράφου.

Κεφάλαιο 8: Operation (Λειτουργία)

Οι καθημερινές διαδικασίες, που αφορούν την ασφάλεια πληροφοριών, απαιτείται να σχεδιαστούν, να υλοποιηθούν και να ελέγχονται. Σε αυτή τη φάση, το πρότυπο απαιτεί την υλοποίηση ενεργειών για την επίτευξη των στόχων που ορίστηκαν έπειτα από την αξιολόγηση κινδύνου στο κεφάλαιο έξι. Όλες αυτές οι ενέργειες πρέπει να καταγράφονται και να παρακολουθούνται.

Κεφάλαιο 9: Performance Evaluation (Αξιολόγηση Απόδοσης)

Οι απαιτήσεις του ISO/IEC 27001 σε αυτό το κεφάλαιο αφορούν την παρακολούθηση, τη μέτρηση, την ανάλυση και την αξιολόγηση του ISMS. Παραδείγματα μετρήσεων είναι η αλλαγή του επιπέδου ενός κινδύνου, ο αριθμός συμβάντων αποτυχίας συστήματος (system failure) και το διάστημα που μεσολάβησε για την εμφάνιση συμβάντων κινδύνου. Εσωτερικοί έλεγχοι απαιτείται να διεξάγονται για αυτό το σκοπό. Οι έλεγχοι αυτοί πρέπει να γίνονται σύμφωνα με τον τρόπο που ορίζει το πρότυπο.

Κεφάλαιο 10: Improvement (Βελτίωση)

Η βελτίωση ακολουθεί την αξιολόγηση. Οποιοδήποτε αρνητικό αποτέλεσμα της αξιολόγησης απαιτείται να αναγνωρίζεται και οι αιτίες του να εντοπίζονται και να αντιμετωπίζονται. Ένα αρνητικό αποτέλεσμα της αναφοράς αξιολόγησης μπορεί να αφορά μια διαδικασία που δεν είναι συμβατή με το πρότυπο, τη μη συμμόρφωση με το πρότυπο των προδιαγραφών ενός προϊόντος ή ενός πρότζεκτ, παράπονα πελατών ή μη τήρηση των συμφωνηθέντων όσον αφορά κάποια προμήθεια. Από τη στιγμή που κάποιο από τα παραπάνω υπάρξει στα αποτελέσματα αξιολόγησης της απόδοσης,

απαιτούνται διορθωτικές ενέργειες για να εξασφαλίσουν ότι το συγκεκριμένο συμβάν δε θα ξανασυμβεί.

Στη συνέχεια καταγράφονται τα υποχρεωτικά έγγραφα που ορίζουν οι απαιτήσεις του ISO/IEC 27001 (Dejan Kosutic, 2013). Όσον αφορά τα έγγραφα που αναφέρονται από το Annex A, είναι υποχρεωτικά μόνο αν υπάρχουν οι αντίστοιχοι κίνδυνοι που απαιτούν την υλοποίηση τους.

- Scope of the ISMS (clause 4.3)
- Information security policy and objectives (clauses 5.2 and 6.2)
- Risk assessment and risk treatment methodology (clause 6.1.2)
- Statement of Applicability (clause 6.1.3 d)
- Risk treatment plan (clauses 6.1.3 e and 6.2)
- Risk assessment report (clause 8.2)
- Definition of security roles and responsibilities (clauses A.7.1.2 and A.13.2.4)
- Inventory of assets (clause A.8.1.1)
- Acceptable use of assets (clause A.8.1.3)
- Access control policy (clause A.9.1.1)
- Operating procedures for IT management (clause A.12.1.1)
- Secure system engineering principles (clause A.14.2.5)
- Supplier security policy (clause A.15.1.1)
- Incident management procedure (clause A.16.1.5)
- Business continuity procedures (clause A.17.1.2)
- Statutory, regulatory, and contractual requirements (clause A.18.1.1)

Επίσης καταγράφει και τις υποχρεωτικές καταχωρήσεις αρχείων:

- Records of training, skills, experience and qualifications (clause 7.2)
- Monitoring and measurement results (clause 9.1)
- Internal audit program (clause 9.2)
- Results of internal audits (clause 9.2)
- Results of the management review (clause 9.3)
- Results of corrective actions (clause 10.1)
- Logs of user activities, exceptions, and security events (clauses A.12.4.1 and A.12.4.3)

3.5. Annex A

Το annex A περιλαμβάνει 39 στόχους και 134 μέτρα για τη διαχείριση της ασφάλειας πληροφοριών. Οι στόχοι μπορούν να καταταγούν σε έντεκα βασικούς τομείς σύμφωνα με τον Disterer (2013) και όσων αναφέρει το ISO/IEC 27001. Ακολουθούν οι στόχοι που αναφέρονται ξεχωριστά σε κάθε τομέα:

Security Policy

- Η παροχή κατεύθυνσης και υποστήριξης από τη διοίκηση για την ασφάλεια πληροφοριών σύμφωνα με τις απαιτήσεις του οργανισμού και σε συμμόρφωση με τα νομικά πλαίσια.

Organization of information security

- Η επίτευξη της ασφάλειας πληροφοριών μέσα στον οργανισμό.
- Η διατήρηση της ασφάλειας πληροφοριών μέσα στον οργανισμό και των περιοχών που σχετίζονται με πληροφορίες εκτός αυτού και επηρεάζονται από εξωτερικούς συνεργάτες.

Asset Management

- Η επίτευξη και η διατήρηση της προστασίας των πληροφοριακών στοιχείων του οργανισμού.
- Η διασφάλιση πως η προστασία των πληροφοριών βρίσκεται σε ένα κατάλληλο επίπεδο.

Human Resources security

- Η διασφάλιση πως οι εργαζόμενοι, οι εξωτερικοί συνεργάτες και άλλοι ενδιαφερόμενοι κατανοούν τις υποχρεώσεις και ευθύνες τους στη διαχείρηση της ασφάλειας πληροφοριών.
- Η διασφάλιση πως οι παραπάνω ομάδες ανθρώπων είναι ενήμεροι για τις απειλές και τις ανησυχίες σχετικά με την ασφάλεια πληροφοριών και είναι εξοπλισμένοι με τα απαραίτητα εφόδια για να εκτελούν τις καθημερινές εργασίες τους τηρώντας την πολιτική ασφαλείας.
- Σε περίπτωση εξόδου από τον οργανισμό (τερματισμός εργασίας) κάποιου από τις παραπάνω ομάδες, αυτό γίνεται με ομαλό τρόπο.

Physical and environmental security

- Η αποτροπή μη εξουσιοδοτημένης πρόσβασης στις πληροφορίες του οργανισμού.
- Η αποτροπή απώλειας, βλάβης ή κλοπής των στοιχείων πληροφορίας του οργανισμού.

Communications and operations management

- Η διασφάλιση της σωστής και ασφαλούς λειτουργίας των εγκαταστάσεων επεξεργασίας πληροφοριών.
- Η απόκτηση και διατήρηση κατάλληλου επιπέδου ασφάλειας πληροφοριών σχετικά με την παροχή υπηρεσιών σε εξωτερικούς συνεργάτες.
- Η ελαχιστοποίηση του κινδύνου όσον αφορά τις αποτυχίες συστήματος (system failure).
- Η προστασία της ακεραιότητας του λογισμικού.
- Η προστασίας της ακεραιότητας και διαθεσιμότητας των εγκαταστάσεων επεξεργασίας πληροφοριών.
- Η προστασία των πληροφοριών στο δίκτυο.

- Η αποτροπή μη εξουσιοδοτημένης τροποποίησης, αφαίρεσης ή καταστροφής στοιχείων πληροφορίας.
- Η διατήρηση της ασφάλειας λειτουργίας του λογισμικού μεταξύ των ενδιαφερόμενων εντός και εκτό του οργανισμού.
- Η προστασία των υπηρεσιών ηλεκτρονικού εμπορίου και της χρήσης τους.
- Η ανίχνευση μη εξουσιοδοτημένων ενεργειών σχετικά με την επεξεργασία πληροφοριών.

Access control

- Ο έλεγχος πρόσβασης στις πληροφορίες.
- Η προστασίας των πληροφοριακών συστημάτων από μη εξουσιοδοτημένη πρόσβαση.
- Η αποτροπή μη εξουσιοδοτημένης πρόσβασης χρήστη στις εγκαταστάσεις επεξεργασίας πληροφοριών.
- Η αποτροπή μη εξουσιοδοτημένης πρόσβασης στις υπηρεσίες δικτύου.
- Η αποτροπή μη εξουσιοδοτημένης πρόσβασης στα λειτουργικά συστήματα.
- Η αποτροπή μη εξουσιοδοτημένης πρόσβασης σε πληροφορίες που περιέχουν τα συστήματα εφαρμογών.
- Η διασφάλιση της ασφάλειας πληροφοριών στην περίπτωση τηλεργασίας.

Information systems acquisition, development and maintenance

- Η διασφάλιση πως η ασφάλεια αποτελεί θέμα καίριας σημασίας για το πληροφοριακό σύστημα.
- Η αποτροπή λαθών, απώλειας ή μη εξουσιοδοτημένης τροποποίησης πληροφριών στις εφαρμογές.
- Η προστασία των πληροφοριών μέσω της κρυπτογραφίας.
- Η προστασίας της ασφάλειας του συστήματος αρχείων.
- Η διατήρηση της ασφάλειας του συστήματος λογισμικού εφαρμογών.
- Η μείωση των κινδύνων που προέρχονται από τεχνικές ευαλωτότητες.

Information security incident management

- Η διασφάλιση πως συμβάντα απειλής της ασφάλειας του πληροφοριακού συστήματος αντιμετωπίζεται έγκαιρα με τις κατάλληλες διορθωτικές κινήσεις.
- Η εξασφάλιση πως η προσέγγιση που ακολουθείται στη διαχείριση συμβάντων είναι αποδοτική.

Business continuity management

- Η δράση ενάντια σε ενέργειες που διαταράσσουν τον οργανισμό και η προστασία των κρίσιμων διαδικασιών από τις συνέπειες μεγάλων σφαλμάτων ή καταστροφής του πληροφοριακού συστήματος ώστε να πραγματοποιείται η έγκαιρη συνέχιση της λειτουργίας του οργανισμού.

Compliance

- Η αποφυγή παραβιάσεων νόμων, θεσμών ή υποχρεώσεων συμβολαίων και οποιασδήποτε από τις απαιτήσεις ασφαλείας.
- Η εξασφάλιση της συμμόρφωσης των συστημάτων με πολιτικές και πρότυπα.
- Η μεγιστοποίηση της αποτελεσματικότητας των διαδικασιών ελέγχου και η ελαχιστοποίηση των παρεμβάσεων αυτών.

3.6. Πιστοποίηση (Certification)

Ένας οργανισμός για να πιστοποιήσει τη συμμόρφωση του ISMS του με το ISO/IEC 27001 πρέπει να περάσει μια συγκεκριμένη διαδικασία που κατευθύνεται από έναν εξουσιοδοτημένο οργανισμό πιστοποίησης (RCB – Registered Certification Bodies). Η διαδικασία αυτή αποτελείται από επιμέρους στάδια. Αρχικά γίνεται έλεγχος όλων των εγγράφων που αφορούν την ασφάλεια πληροφοριών και στη συνέχεια λαμβάνουν χώρα εντός του οργανισμού συνεντεύξεις με τα υπεύθυνα άτομα. Οι συνεντεύξεις αυτές κρατάνε αρκετές ημέρες και περιλαμβάνουν ερωτήσεις γύρω από την εξήγηση της πολιτικής που ακολουθείται, την περιγραφή των διαδικασιών, την ανάλυση των λεπτομερειών και των χαρακτηριστικών του ISMS και τη συζήτηση γνωστών αδυναμιών του συστήματος και μέτρων βελτίωσης. Ύστερα από το πέρας αυτών των συναντήσεων, ο οργανισμός πιστοποίησης εξάγει μια αναφορά, όπου τα αποτελέσματα εξηγούνται αναλυτικά και περιγράφονται τα μέτρα

βελτίωσης που υποχρεωτικά πρέπει να ληφθούν πριν από τον επόμενο έλεγχο. Σε περίπτωση που το συνολικό αποτέλεσμα της αναφοράς είναι θετικό, ο οργανισμός λαμβάνει το επίσημο πιστοποιητικό. Αυτό το πιστοποιητικό διαρκεί συνήθως τρία χρόνια και ύστερα από αυτά ο οργανισμός πρέπει να ξαναπεράσει τη διαδικασία πιστοποίησης για να το ανανεώσει. Είναι σημαντικό να αναφερθεί πως η υλοποίηση ενός ISMS μπορεί να διαρκέσει μήνες έως και χρόνια ανάλογα την περίπτωση (Disterer, 2019).

3.7. Τα οφέλη του ISO/IEC 27001

Η υλοποίηση ενός ISMS βασισμένο στο ISO/IEC 27001 προσφέρει στον οργανισμό μια σειρά από οφέλη. Οι Pinheiro και Ribeiro (2015) αναφέρουν ως κέρδη τη μείωση ή ακόμα και την εξαφάνιση κάποιων κινδύνων, την ευελιξία χρήσης του προτύπου στα διάφορα τμήματα του οργανισμού και την αναγνώριση του οργανισμού στην αγορά. Οι Al-Dhahri, Al-Sarti και Aziz (2017) σημειώνουν την αυξημένη απόδοση του οργανισμού, το μειωμένο επιχειρηματικό ρίσκο, τη διασφάλιση των πληροφοριών, τη χρησιμοποίηση του πιστοποιητικού ως σύμβολο εμπιστοσύνης για τους πελάτες και τους συνεργάτες και την ανάπτυξη συναίσθησης των εργαζομένων ως οφέλη. Τέλος, οι Accerboni και Sartor (2019) αναλύουν τη θετική επίδραση του ISMS στη μείωση του κόστους που προέρχεται από δυσλειτουργίες, στη βελτίωση της φήμης της εταιρίας και των δεσμών με τους πελάτες και συνεργάτες, στην αποφυγή νομικών παραβάσεων που επιφέρουν επιπλέον έξοδα και βλάβη φήμης και στην καθημερινή εργασία των ανθρώπινων πόρων.

Κεφάλαιο 4: Η αξιολόγηση κινδύνου στο ISO/IEC 27001

4.1. Γενικά στοιχεία

Ένας από τους καλύτερους τρόπους να εξετάσει ένας οργανισμός τα προβλήματα ασφάλειας πληροφοριών στον επιχειρηματικό κόσμο είναι η προσέγγιση βασισμένη στη διαχείριση κινδύνου (risk management). Η διαχείριση κινδύνου στην ασφάλεια πληροφοριών είναι μια συνεχής διαδικασία που προσφέρει στον οργανισμό τη γνώση των πιθανών κινδύνων που αφορούν τα στοιχεία πληροφορίας του (information assets) και των εργαλείων για την αντιμετώπιση τους. Ωστόσο, στις συνθήκες του σύγχρονου κόσμου, αποτελεί και μια διαδικασία γεμάτη προκλήσεις, καθώς οι παράγοντες κινδύνου εξελίσσονται και μεταβάλλονται συνεχώς. Εξαιτίας της ραγδαίας εξέλιξης της τεχνολογίας και της συνεχούς βελτίωσης της γνώσης αυτών που θέλουν να βλάψουν τον οργανισμό, τα αποτελέσματα μιας διαχείρισης κινδύνου μπορεί ακόμα και σε βάθος λίγων μηνών να θεωρηθούν ξεπερασμένα. Ο απόλυτος στόχος της διαχείρισης κινδύνου στην ασφάλεια πληροφοριών είναι η μεγιστοποίηση της απόδοσης του οργανισμού σε συνδυασμό με την ελαχιστοποίηση των μη αναμενόμενων αρνητικών αποτελεσμάτων που επιφέρουν πιθανοί κίνδυνοι. Με το κατάλληλο risk management, μπορεί να επέλθει η ισορροπία μεταξύ πιθανών και αποδεκτών κινδύνων. Είναι σημαντικό να αναφερθεί πως η διαδικασία διαχείρισης κινδύνου οφείλει να είναι συνεχής, μετρήσιμη και ελεγχόμενη (Shameli-Sendi et al., 2015).

Η αξιολόγηση κινδύνου στην ασφάλεια πληροφριών (Information Security Risk Assessment – ISRA) αποτελεί την πιο σημαντική διαδικασία της διαχείρισης κινδύνου και ένα από τα σημαντικότερα στοιχεία του ISMS. Προσφέρει τη δυνατότητα στον οργανισμό να αναγνωρίσει απειλές και ευαλωτότητες (threats and vulnerabilities) και στη συνέχεια να επιλέξει το μέτρο που θα αντιμετωπίσει τον πιθανό κίνδυνο. Ο στόχος της αξιολόγησης κινδύνου είναι η αντιστοίχιση των πιθανών κινδύνων με τα στοιχεία πληροφορίας του οργανισμού, η ακριβής κατάταξη τους με βάση κάποιο κριτήριο και τελικά η άμβλυνση τους (Shameli-Sendi et al., 2015).

Το αντικείμενο της αξιολόγησης κινδύνου είναι τα περιουσιακά στοιχεία πληροφορίας του οργανισμού, δηλαδή οτιδήποτε έχει αξία για τον οργανισμό. Η εύρεση της σχέσης μεταξύ απειλής και ευαλωτότητας κάθε στοιχείου αποτελεί ένα πολύ κρίσιμο θέμα. Αρχικά, η αξιολόγηση κινδύνου αποφασίζει την αξία αυτών των στοιχείων και αναγνωρίζει τις πιθανές απειλές και ευαλωτότητες. Στη συνέχεια, εκτιμά τα διαθέσιμα μέτρα και την επίδραση τους στον κίνδυνο που προκύπτει. Τέλος, θέτει προτεραιότητες στους πιθανούς κινδύνους και τους κατηγοριοποιεί σύμφωνα με τα κριτήρια αξιολόγησης που υπάρχουν στο περιεχόμενο της αξιολόγησης (Wei et al., 2017).

Οι αποφάσεις στη διαχείριση ασφάλειας πληροφοριών (information security management) κατευθύνονται εξ ολοκλήρου από τα αποτελέσματα της αξιολόγησης κινδύνου, κάτι που αναδεικνύει τη διαδικασία αυτή ως τον κεντρικό πυρήνα της ασφάλειας πληροφοριών. Στις πρώτες σελίδες του, το ISO27002 αναφέρει πως οι απαιτήσεις ασφάλειας πληροφοριών σε έναν οργανισμό καθορίζονται από τα αποτελέσματα μιας μεθοδικής αξιολόγησης κινδύνου και πως οι αρνητικές συνέπειες εμφάνισης κινδύνων θα πρέπει να γίνουν αντικείμενο περισσότερης σκέψης από τα έξοδα που χρείαζονται για να ληφθούν μέτρα ασφάλειας. Το ISO27001, το πιο δημοφιλές και χρήσιμο πρότυπο για την ανάπτυξη ενός ISMS, παρέχει μια προσέγγιση στη διαχείριση κινδύνου που έρχεται σε αρμονία με όλες τις γνωστές οδηγίες, προσέγγιση την οποία ένας συνεχώς αυξανόμενος αριθμός οργανισμών υιοθετεί. Το πρότυπο καθιστά σαφές, πως η αξιολόγηση κινδύνου πρέπει να γίνει πριν την επιλογή και την υλοποίηση των μέτρων ελέγχου και πως κάθε επιλογή και υλοποίηση μέτρου πρέπει να αιτιολογείται απόλυτα από την αξιολόγηση κινδύνου (Calder & Watkins, 2010).

Συμπερασματικά, το ISO27001 καθορίζει τις προδιαγραφές του ISMS και βασίζεται στην αξιολόγηση κινδύνου τόσο σε αρχική φάση όσο και μετέπειτα. Το πρότυπο συγκεκριμενοποιεί τα βήματα της διαδικασίας εξαγωγής της αξιολόγησης καθώς και το βαθμό λεπτομέρειας της. Παρά το γεγονός πως υπάρχουν πολλές αναγνωρισμένες και έγκυρες μεθοδολογίες αξιολόγησης κινδύνου, ένας οργανισμός που θέλει να πιστοποιηθεί με το ISO27001 πρέπει να ακολουθήσει τις σχετικές απαιτήσεις που ορίζει το πρότυπο. Δεν υπάρχει το περιθώριο ημίμετρων, είτε η μεθοδολογία αξιολόγησης κινδύνου που επιλέγει ο οργανισμός είναι συμβατή με τις απαιτήσεις του προτύπου και ακολουθεί η επίσημη πιστοποίηση είτε όχι και η πιστοποίηση είναι αδύνατον να πραγματοποιηθεί (Calder & Watkins, 2010).

4.2. Τα στάδια της διαχείρισης κινδύνου (risk management)

Η διαχείριση κινδύνου (risk assessment), σύμφωνα με τους Shameli-Sendi, Aghababei-Barzegar και Cheriet (2015), αποτελείται από τέσσερις φάσεις:

- **Πλαισίωση του κινδύνου (framing risk)**

Σχετίζεται με τον τρόπο που ο οργανισμός αντιλαμβάνεται τους κινδύνους. Το κύριο αποτέλεσμα αυτής της διαδικασίας είναι η δημιουργία μιας στρατηγικής διαχείρισης κινδύνων που επίσης καθορίζει τα όρια εφαρμογής της μέσα στον οργανισμό. Τα στοιχεία πληροφορίας και οι πόροι που είναι άνευ σημασίας δε χρειάζεται να αξιολογηθούν περαιτέρω. Ο καθορισμός μεγαλύτερων ή μικρότερων ορίων εφαρμογής της στρατηγικής μπορεί να αποβεί επικίνδυνος για τη μετ'έπειτα αξιολόγηση γι'αυτό η φάση αυτή είναι αρκετά κρίσιμη.

- **Αξιολόγηση κινδύνου (assessing risk)**

Η αξιολόγηση κινδύνου αποτελείται από την ανάλυση κινδύνου (risk analysis και την αποτίμηση κινδύνου (risk evaluation). Παρέχει τη δυνατότητα στον οργανισμό να αποκτήσει μια εμπεριστατωμένη άποψη γύρω από τους υπάρχοντες κινδύνους στην ασφάλεια πληροφοριών, των συνεπειών τους και των μέτρων που μπορεί να λάβει για να τους αντιμετωπίσει. Η διαδικασία αυτή περιλαμβάνει όλους τους κινδύνους που σχετίζονται με όλα τα είδη στοιχείων πληροφορίας του οργανισμού, όπως πλατφόρμες, λειτουργικά συστήματα, εφαρμογές, δίκτυα, ανθρώπους, διεργασίες. Τα λάθη σε αυτή τη φάση μπορεί να αποβούν μοιραία, καθώς η υποτίμηση κάποιου κινδύνου μπορεί να αφήσει τον οργανισμό εκτεθειμένο σε σημαντικές απειλές.

Η ανάλυση κινδύνου γνωστοποιεί τις ευαλωτότητες των πολύτιμων στοιχείων πληροφορίας του οργανισμού, αποκαλύπτει τις απειλές που μπορούν να εκμεταλλευτούν αυτές τις ευαλωτότητες και να τον θέσουν σε καθεστώς κινδύνου. Τέλος, υπολογίζει την πιθανή ζημία και απώλειες ως αποτελέσματα εμφάνισης αυτών των κινδύνων. Πιο αναλυτικά, τα βήματα της ανάλυσης κινδύνου είναι τα εξής:

1. **Εκτίμηση και αναγνώριση των πόρων (Resources identification and valuation):** Περιλαμβάνει την καταγραφή και αποτίμηση όλων των στοιχείων πληροφορίας του οργανισμού που έχουν κάποια αξία για αυτόν. Το ISO/IEC 27001 απαιτεί από τους οργανισμούς την τακτική και συχνή ενημέρωση του καταλόγου αυτών των στοιχείων. Μερικά παραδείγματα πόρων αποτελούν οι καθημερινές διεργασίες, το υλικό και το λογισμικό, τα δίκτυα, το προσωπικό, τα έγγραφα ακόμα και η φήμη του οργανισμού. Τα στοιχεία αυτά ασφαλώς έχουν διαφορετική αξία που εξαρτάται από τη σημασία τους μέσα στην επιχείρηση.
2. **Εξακρίβωση κινδύνου (Risk identification):** Ο στόχος αυτής της φάσης είναι η αναγνώριση όλων των πιθανών κινδύνων σχετιζόμενων με τους πόρους. Αυτό προϋποθέτει την αναγνώριση των ευαλωτοτήτων και των απειλών. Κύριες περιπτώσεις απειλών αποτελούν η καταστροφή, η αλλοίωση, η μη έγκυρη τροποποίηση, η κλοπή, η αφαίρεση και η παράνομη δημοσιοποίηση πληροφοριών.
3. **Μέτρηση κινδύνου (Risk measurement):** Σε αυτό το στάδιο, επιλέγεται ένα μοντέλο για τη μέτρηση των κινδύνων. Ένα τέτοιο μοντέλο αφορά τον τρόπο μέτρησης της σχέσης μεταξύ των παραγόντων κινδύνου, δηλαδή την αξία του στοιχείου πληροφορίας, την επίδραση της ευαλωτότητας, τον αντίκτυπο της απειλής και την πιθανότητα πραγματοποίησης της απειλής. Ανάλογα το μοντέλο, υπολογίζεται και το μέγεθος του κάθε κινδύνου.

Η αποτίμηση κινδύνου είναι η διαδικασία βαθμολόγησης των κινδύνων σε μία κλίμακα ανάλογα με τα κριτήρια που έχουν οριστεί, ώστε να καθοριστεί η σημασία και η κρισιμότητα τους. Σε αυτό το στάδιο, αποφασίζονται τα κατάλληλα βήματα για την αντιμετώπιση τους και δίνονται οι αντίστοιχες προτεραιότητες ανάλογα με την πιθανότητα εμφάνισης και το νομικό, οικονομικό ή σχετικό με τη φήμη του οργανισμού αντίκτυπο κάθε κινδύνου. Υπάρχουν τέσσερις επιλογές για την κατάταξη ενός κινδύνου:

1. **Αποδοχή (Accept):** Ο οργανισμός αποδέχεται τον κίνδυνο και τις συνέπειες του και αποφασίζει να συμβιβαστεί με την ύπαρξη του.
2. **Αποφυγή (Avoid):** Η δραστηριότητα που εκθέτει τον οργανισμό στο συγκεκριμένο κίνδυνο τερματίζεται.

3. **Μεταφορά (Transfer):** Ολόκληρη η δραστηριότητα ή μέρος της που σχετίζεται με το συγκεκριμένο κίνδυνο μεταφέρεται σε άλλη ομάδα εντός ή εκτός του οργανισμού.
4. **Άμβλυνση (Mitigate):** Ο κίνδυνος ελέγχεται και περιορίζεται σε ένα επίπεδο που θεωρείται αποδεκτός από τον οργανισμό.

- **Αντίδραση στον κίνδυνο (Responding to risk)**

Οι κίνδυνοι που χαρακτηρίζονται ως υψηλότεροι από το όριο αποδοχής του οργανισμού αντιμετωπίζονται όπως αναφέρθηκε προηγουμένως με την αποφυγή,τη μεταφορά ή την άμβλυνση τους. Στην περίπτωση που ένας μη αποδεκτός κίνδυνος δε μπορεί να αποφευχθεί ή να μεταφερθεί, λαμβάνονται κατάλληλα μέτρα για τη μετρίαση του.

Πιο συγκεκριμένα, μέτρο προστασίας στην ασφάλεια πληροφοριών ονομάζεται η διαδικασία ή η τεχνική δραστηριότητα που χρησιμοποιείται για τη μείωση του κινδύνου. Τα μέτρα αυτά περιλαμβάνουν ενέργειες πρόληψης, ανίχνευσης ή διόρθωσης και επιλέγονται για έναν μη αποδεκτό κίνδυνο με κριτήριο το κόστος και το επίπεδο που μειώνουν τον κίνδυνο. Μετά την επιλογή και την υλοποίηση ενός μέτρου προστασίας, κάποιοι κίνδυνοι απομένουν και αυτοί καλούνται κατάλοιπα κινδύνων (residual risks). Βασικός στόχος της διαχείρισης κινδύνου στον οργανισμό είναι η συνεχής μέτρηση και διατήρηση αυτών των κινδύνων κάτω από το αποδεκτό όριο.

- **Παρακολούθηση του κινδύνου (Monitoring risk)**

Η συνεχής παρακολούθηση κατέχει σπουδαίο ρόλο στο πεδίο της ασφάλειας πληροφοριών. Σχεδόν για κάθε πρότυπο ή μοντέλο ασφάλειας υπάρχει κάποιο είδος παρακολούθησης που πραγματοποιείται τακτικά και τα αποτελέσματα της καταγράφονται προσεκτικά. Σε αυτή τη φάση, εξασφαλίζεται η αποτελεσματικότητα της διαχείρισης κινδύνων και η συμμόρφωση της με τους στόχους, τις πολιτικές, τα πρότυπα και τη στρατηγική του οργανισμού (Shameli-Sendi et al., 2015).

Σύμφωνα με τους Calder και Watkins (2010), οι παραπάνω φάσεις της διαχείρισης κινδύνου μπορούν να συμπτυχθούν σε δύο βασικά στάδια. Αυτά είναι η αξιολόγηση ή ανάλυση κινδύνου (risk assessment) και το σχέδιο αντιμετώπισης κινδύνου (risk treatment plan). Αναλυτικότερα, η αξιολόγηση κινδύνου είναι η διαδικασία αναγνώρισης απειλών και ο υπολογισμός της πιθανότητας (likelihood) πραγματοποίησης αυτών εξαιτίας κάποιας ευαλωτότητας του οργανισμού, καθώς και αντίκτυπος (impact) πραγματοποίησης τους. Το σχέδιο αντιμετώπισης του κινδύνου είναι ο τρόπος με τον οποίο αποκρίνεται ο οργανισμός στους πιθανούς κινδύνους που έχουν αναγνωριστεί. Συνοπτικά, η αξιολόγηση κινδύνου είναι το στάδιο όπου οι κίνδυνοι γνωστοποιούνται και αποτιμάται η κρισιμότητα τους, ενώ οι αποφάσεις και οι ενέργειες για την αντίκρουση τους αποτελούν μέρος του σχεδίου αντιμετώπισης.

Οι στόχοι της διαχείρισης κινδύνου συνήθως είναι η εξάλειψη κινδύνων όταν είναι εφικτό και όταν δεν είναι η μείωση τους σε ένα βαθμό που θεωρείται αποδεκτός. Οι αποδεκτοί κίνδυνοι είτε παραμένουν αποδεκτοί με τη συνεχή χρήση των κατάλληλων μέτρων είτε μεταφέρονται σε άλλη ομάδα ή οργανισμό (Calder & Watkins, 2010).

Όσο μεγαλύτερη είναι η πιθανότητα εμφάνισης ενός κινδύνου και όσο αρντικότερες είναι οι συνέπειες εμφάνισης του, τόσο σημαντικότερος θεωρείται και ο κίνδυνος. Για το λόγο αυτό, τα μέτρα προστασίας που λαμβάνονται θα πρέπει να μετριάζουν την πιθανότητα ή/και τον αντίκτυπο του κινδύνου σε τέτοιο βαθμό όπου η σπουδαιότητα του να μη ξεπερνά τα όρια ανοχής του οργανισμού. Αυτά τα όρια ονομάζονται επίπεδο αποδοχής κινδύνου (risk acceptance level). Ο οργανισμός οφείλει να καθορίσει τα κριτήρια που αποδέχεται έναν κίνδυνο ή λαμβάνει μέτρα για αυτόν. Για παράδειγμα, μπορεί να θεωρείται γενικά αποδεκτός ένας κίνδυνος, που ο αντίκτυπος του σε κόστος οικονομικών όρων είναι μικρότερος από το κόστος λήψης μέτρων για τον έλεγχο του αλλά να απαιτείται λήψη μέτρων για έναν κίνδυνο με εξίσου μεγάλη πιθανότητα εμφάνισης και αρνητική επίδραση (Calder & Watkins, 2010).

4.3. Μεθοδολογίες αξιολόγησης κινδύνου συμβατές με το ISO/IEC 27001

4.3.1. Η αξιολόγηση κινδύνου ως διαδικασία του προτύπου

Μεθοδολογία ή μέθοδος ονομάζεται με απλά λόγια ο τρόπος που γίνεται κάτι. Μια μεθοδολογία περιέχει αρχές και διαδικασίες που περιγράφουν τι πρέπει να γίνει και πώς. Συνεπώς, μια μεθοδολογία αξιολόγησης κινδύνου είναι μια περιγραφή αρχών και διαδικασιών που αφορά τον τρόπο που οι κίνδυνοι στην ασφάλεια πληροφοριών πρέπει να αξιολογηθούν και να αποτιμηθούν (Calder & Watkins, 2010).

Μια αποτελεσματική μεθοδολογία αξιολόγησης κινδύνου στην ασφάλεια πληροφοριών, συμβατή με το ISO/IEC 27001, πρέπει να εναρμονίζεται με τις απαιτήσεις που ορίζει το πρότυπο και να παρέχει στον οργανισμό τη βεβαιότητα πως όλοι οι σχετικοί κίνδυνοι έχουν αξιολογηθεί από τη διαδικασία και πως τα αποτελέσματα της έχουν κατανοηθεί σε πλήρη βαθμό (Calder & Watkins, 2010).

Υπάρχουν πολλές δημοσιευμένες μεθοδολογίες αξιολόγησης κινδύνου, ωστόσο μια μέθοδος συμβατή με το ISO/IEC 27001 πρέπει να περιλαμβάνει κάποια συγκεκριμένα βήματα και πολλές αναγνωρισμένες σύγχρονες μέθοδοι δεν ακολουθούν αυτές τις απαιτήσεις. Αυτό συμβαίνει διότι είτε για παράδειγμα δεν περιλαμβάνουν όλα τα απαραίτητα βήματα είτε σε μερικές περιπτώσεις περιγράφουν διαδικασίες με αποκλειστική έμφαση σε θέματα τεχνολογίας. Το ISO/IEC 27001 υποστηρίζει ότι μια αξιολόγηση κινδύνου, κατάλληλη για ένα ISMS, περιέχει την αναγνώριση: των στοιχείων πληροφορίας στα όρια εφαρμογής του ISMS μέσα στον οργανισμό, των υπευθύνων για αυτά τα στοιχεία, των απειλών προς αυτά, των ευαλωτήτων αυτών και του αντίκτυπου της απώλειας της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας τους. Η αναγνώριση αυτή καθορίζει το βαθμό του κινδύνου. Το ISO/IEC 27002 παρέχει ουσιώδεις οδηγίες στην αξιολόγηση κινδύνου, αλλά δεν ορίζει κάποιον ακριβή τρόπο που αυτή θα παραχθεί, καθώς κάθε οργανισμός παροτρύνεται να επιλέξει ποια προσέγγιση είναι η καταλληλότερη για αυτόν. Στην εισαγωγή του, το πρότυπο ορίζει ως αξιολόγηση κινδύνου τη συστηματική μελέτη των στοιχείων, απειλών, ευαλωτοτήτων και αντικτύπου για την αξιολόγηση της πιθανότητας και των συνεπειών των κινδύνων (Calder & Watkins,

2010).

Η αξιολόγηση κινδύνου αποτελεί μια αυστηρά επίσημη διαδικασία. Αυτό σημαίνει πως τα δεδομένα εισόδου της διαδικασίας, η ανάλυση τους και τα αποτελέσμα πρέπει να καταγράφονται εξ ολοκλήρου. Η πολυπλοκότητα της διαδικασίας εξαρτάται από την πολυπλοκότητα του οργανισμού και το μέγεθος των κινδύνων που εξετάζονται. Οι τεχνικές υλοποίησης της θα πρέπει να είναι συνεπείς με αυτή την πολυπλοκότητα (Calder & Watkins, 2010).

Ο κίνδυνος είναι συνάρτηση της πιθανότητας εμφάνισης του και του αρνητικού αντίκτυπου του (likelihood, impact). Ο τύπος που παράγει το βαθμό κινδύνου στην αξιολόγηση είναι:

Κίνδυνος = Πιθανότητα x Αντίκτυπος

Ή με ξένους όρους:

Risk = Likelihood x Impact

Η εξίσωση αυτή πρακτικά σημαίνει πως ο κίνδυνος προκύπτει από το γινόμενο της πιθανότητας να πραγματοποιηθεί μια απειλή εκμεταλλευόμενη μια ευαλωτότητα και των συνολικών αρνητικών συνεπειών αυτού του συμβάντος. Με αυτόν τον τρόπο ο τύπος επεκτείνεται ακολούθως:

Κίνδυνος = (πιθανότητα μια απειλή να πραγματοποιηθεί από την εκμετάλλευση μια ευαλωτότητας) x (συνολικός αντίκτυπος από τη μεταβολή του στοιχείου πληροφορίας)

Ή με ξένους όρους:

Risk = (probability of threat exploiting vulnerability) x (impact cost of asset being exploited)

Η μεθοδολογία αξιολόγησης κινδύνου που θα ακολουθήσει ένας οργανισμός πρέπει να αποδίδει περιεχόμενο στους παράγοντες της παραπάνω εξίσωσης (Calder & Watkins, 2010).

Άλλοι τύποι υπολογισμού του βαθμού κινδύνου είναι οι ακόλουθοι (Ghazouani et al., 2014):

Κίνδυνος = (Απειλή) x (Ευαλωτότητα) x (Αξία του στοιχείου πληροφορίας)

Κίνδυνος = (Απειλή) x (Ευαλωτότητα) x (Αντίκτυπος)

4.3.2. Οι δύο βασικές προσεγγίσεις

Οι δύο βασικές μέθοδοι αξιολόγησης κινδύνου στην ασφάλεια πληροφοριών είναι η ποσοτική (quantitative) και η ποιοτική (qualitative) μέθοδος. Η ποσοτική αξιολόγηση χρησιμοποιεί για στοιχεία εισόδου και επεξεργασίας μαθηματικά δεδομένα, ενώ η ποιοτική λαμβάνει μη μαθηματικές εισόδους (Calder & Watkins, 2010).

Ποσοτική μέθοδος αξιολόγησης κινδύνου

Η προσέγγιση αυτή σχετίζεται με δύο αριθμούς. Ο ένας αφορά την πιθανότητα εμφάνισης ενός συμβάντος απειλής και ο άλλος αφορά την πιθανή απώλεια από αυτό το συμβάν. Το γινόμενο αυτών των δύο παράγει έναν νέο αριθμό που αποτελεί τον βαθμό κινδύνου. Η πιθανή απώλεια μετράται συνήθως σε οικονομικούς όρους και η πιθανότητα του συμβάντος σε κάποιες περιπτώσεις περιγράφεται ως φορές πραγματοποίησης ανά χρόνο. Το γινόμενο τους σε αυτές τις περιπτώσεις είναι κάποια μεγέθη όπως το ALE (Annual Loss Expectancy) ή το EAC (Estimated Annual Cost). Είναι ξεκάθαρο πως όσο μεγαλύτερη είναι η τιμή που αποδίδεται στον κίνδυνο, τόσο σοβαρότερος αποτελεί για τον οργανισμό. Ανάλογα με την απόδοση τιμών στους διάφορους κινδύνους, προκύπτει η ταξινόμηση τους και στη συνέχεια η λήψη αποφάσεων (Calder & Watkins, 2010).

Το βασικό πλεονέκτημα αυτής της προσέγγισης είναι ότι παρέχει μαθηματική μέτρηση του αντίκτυπου ενός συμβάντος απειλής, δηλαδή εκτιμά τις οικονομικές απώλειες από την καταστροφή ή την αλλοίωση ενός στοιχείου πληροφορίας. Αυτά τα οικονομικά μεγέθη βοηθούν σημαντικά στην παραγωγή ενός επωφελούς σχεδίου αντιμετώπισης. Ωστόσο ο αντίκτυπος σε απώλεια φήμης και αξιοπιστίας δε μπορεί να οριστεί με αριθμούς (Calder & Watkins, 2010).

Το κύριο πρόβλημα με αυτή τη μεθοδολογία είναι πως η παραγωγή των μαθηματικών αριθμών μπορεί να απαιτεί υπερβολικά μεγάλο χρόνο και η υλοποίηση και πρόοδος του ISMS καθυστερεί σημαντικά. Επίσης, η παραγωγή αριθμητικών αποτελεσμάτων σχετικά με τους κινδύνους μπορεί να προκαλέσει έναν εφησυχασμό

δυσανάλογο της κρισιμότητας συγκεκριμένων κινδύνων (Calder & Watkins, 2010).

Ένα άλλο σημαντικό μειονέκτημα της ποσοτικής μεθόδου είναι η υποκειμενικότητα της. Πολλές φορές, οι οικονομικές απώλειες ενός συμβάντος κινδύνου αξιολογούνται υποκειμενικά και σύμφωνα με την άποψη συγκεκριμένων ατόμων. Σαν αποτέλεσμα, το γινόμενο των δύο στοιχείων που αποδίδουν αριθμητική τιμή στον κίνδυνο προκύπτει από μια προσωπική εκτίμηση. Είναι βέβαιο πως αν τα αποτελέσματα που παράγει η αξιολόγηση βασίζονται σε μεγάλο βαθμό σε ατομικές αποφάσεις και είναι πολύ πιθανό ότι θα διαφέρουν σε σχέση με τις αποφάσεις ενός άλλου ατόμου, τότε τα αποτελέσματα αυτά θα είναι μη αναπαράξιμα και μη συγκρίσιμα στο μέλλον. Το παραπάνω αποτέλεσμα έρχεται σε αντίθεση με τις απαιτήσεις του ISO/IEC 27001 (Calder & Watkins, 2010).

Οι έλεγχοι και τα μέτρα που λαμβάνονται ύστερα από μια αξιολόγηση κινδύνου συχνά σχετίζονται με αρκετά πιθανά συμβάντα, κάτι που αναδεικνύει τη μεγάλη συσχέτιση ορισμένων κινδύνων. Για το λόγο αυτό μια πιθανή κατάταξη κινδύνων με βάση την προσδοκία ετήσιας απώλειας (ALE), όπως αναφέρθηκε παραπάνω, μπορεί να κάνει αυτές τις συσχετίσεις δύσκολο να παρατηρηθούν. Αυτό έχει σαν αποτέλεσμα τη λήψη λανθασμένων αποφάσεων σχετικά με τα μέτρα (Calder & Watkins, 2010).

Ποιοτική μέθοδος αξιολόγησης κινδύνου

Το ISO 27002 αναφέρει πως η η μεθοδολογίας αξιολόγησης κινδύνου πρέπει να δίνει τη δυνατότητα στον οργανισμό να αξιολογεί την κρισιμότητα των κινδύνων ασφάλειας πληροφοριών και να αξιοποιεί αυτή τη γνώση για τη λήψη αποφάσεων και κατάλληλων μέτρων ελέγχου. Οι δύο υπογραμμισμένες έννοιες αποτελούν τα θεμέλια μιας ποιοτικής μεθοδολογίας αξιολόγησης κινδύνου. Η συγκεκριμένη προσέγγιση κατατάσσει τους κινδύνους χρησιμοποιώντας μια ποιοτική ή ιεραρχική κλίμακα, για παράδειγμα Πολύ σοβαρός-Σοβαρός-Ανεκτός-Καθόλου πρόβλημα. Η κλίμακα που χρησιμοποιείται είναι η ίδια και για την απόδοση τιμής στην πιθανότητα εμφάνισης συμβάντος και στον αντίκτυπο (likelihood – impact) (Calder & Watkins, 2010).

Η ποιοτική μέθοδος είναι με διαφορά η πιο ευρέως διαδεδομένη μεθοδολογία και έρχεται σε αρμονία με τις απαιτήσεις που ορίζει το πρότυπο ISO/IEC 27001. Το επίπεδο κινδύνου προκύπτει από τις ποιοτικές εκτιμήσεις της πιθανότητας και του αντικτύπου με τέτοιο τρόπο που δεν απαιτούνται ακριβείς μαθηματικοί υπολογισμοί. Το ISO 27005 περιγράφει την ποιοτική μέθοδο ως τη χρήση μιας κλίμακας

προσδιοριστικών γνωρισμάτων με σκοπό την περιγραφή της κρισιμότητας ενός κινδύνου. Τέτοια γνωρίσματα, για παράδειγμα, είναι το σχήμα low-medium-high δηλαδή ο χαμηλός, μέτριος ή υψηλός βαθμός κινδύνου. Είναι σημαντικό τα γνωρίσματα που χρησιμοποιούνται να έχουν οριστεί επαρκώς ώστε να μην αφήνονται περιθώρια παρερμηνείας και ακόμα τα αποτελέσματα να είναι αναπαράξιμα και συγκρίσιμα (Calder & Watkins, 2010).

Το κύριο πλεονέκτημα της ποιοτικής προσέγγισης είναι ο τρόπος αξιοποίησης των ευαλωτοτήτων και των απειλών για την άμεση κατηγοριοποίηση των κινδύνων και έγκαιρη λήψη διορθωτικών μέτρων και αποφάσεων. Συνήθως η παραγωγή της διαρκεί ένα λογικό χρονικό διάστημα. Επιπρόσθετα, η μεθοδολογία αυτή αναγνωρίζει τα περιθώρια της υποκειμενικότητας μιας αξιολόγησης κινδύνου και καθορίζει το πλαίσιο που τα αποτελέσματα της παραμένουν αναπαράξιμα και συγκρίσιμα. Το μειονέκτημα της είναι η μη παροχή αριθμητικών μετρήσεων που βοηθούν στην παραγωγή ενός οικονομικά επωφελούς σχεδίου αντιμετώπισης κινδύνων (Calder & Watkins, 2010).

Ακολουθεί ένα παράδειγμα κλίμακας πέντε επιπέδων για την κατάταξη των κινδύνων ενός οργανισμού (βλ. Πίνακας 1).

Βαθμός κινδύνου	Ενέργεια αντιμετώπισης που απαιτείται
Πολυ υψηλός	Μη αποδεκτός κίνδυνος. Απαιτούνται άμεσες ενέργειες.
Υψηλός	Μη αποδεκτός κίνδυνος. Απαιτούνται ενέργειες το συντομότερο δυνατόν.
Μεσαίος	Απαιτούνται ενέργειες εντός λογικού χρονικού διαστήματος.
Χαμηλός	Αποδεκτός κίνδυνος. Οποιαδήποτε απόφαση ληφθεί θα αποτελεί μέρος της συνολικής οικονομικής ανάλυσης.
Πολύ χαμηλός	Αποδεκτός κίνδυνος. Καμία ενέργεια δεν απαιτείται.

Πίνακας 1 - Παράδειγμα κλίμακας ποιοτικής μεθοδολογίας αξιολόγησης κινδύνου

Η παραπάνω κλίμακα πέντε επιπέδων είναι ένα πιθανό αποτέλεσμα που μπορεί να παράγει η επεξεργασία κλιμάκων τριών επιπέδων για την πιθανότητα και τον αρνητικό αντίκτυπο συμβάντων απειλών (βλ. Πίνακας 2).

Πιθανότητα				
	Υψηλή	Μεσαίος κίνδυνος	Υψηλός κίνδυνος	Πολύ υψηλός κίνδυνος
	Μεσαία	Χαμηλός κίνδυνος	Μεσαίος κίνδυνος	Υψηλός κίνδυνος
	Χαμηλή	Πολύ χαμηλός κίνδυνος	Χαμηλός κίνδυνος	Μεσαίος κίνδυνος
		Χαμηλός	Μεσαίος	Υψηλός
		Αντίκτυπος		

Πίνακας 2 - Παράδειγμα κατάταξης κινδύνων σε κλίμακα πέντε επιπέδων σύμφωνα με κλίμακες τριών επιπέδων για την πιθανότητα και τον αντίκτυπο

4.3.3. Σύγκριση ποιοτικής και ποσοτικής μεθοδολογίας

Σύμφωνα με τους Kiran, Reddy και Haritha (2013) τα πλεονεκτήματα και τα μειονεκτήματα των δύο βασικών προσεγγίσεων μεθοδολογίας αξιολόγησης κινδύνου είναι τα ακόλουθα (βλ. Πίνακας 3):

Ποσοτική μέθοδος	Ποιοτική μέθοδος
+Οι κίνδυνοι κατατάσσονται με κριτήριο τον οικονομικό τους αντίκτυπο.	+Κάνει δυνατή την ευρεία κατανόηση της κατάταξης κινδύνων.
+Τα αποτελέσματα διευκολύνουν τη διαχείριση κινδύνου μέσω του δείκτη απόδοσης της επένδυσης (ROI).	+Διευκολύνει τη γενική συμφωνία των ανθρώπων που πραγματοποιούν την αξιολόγηση.
+Τα αποτελέσματα μπορούν να εκφραστούν σε ορολογίες της διαχείρισης κινδύνου.	+Δεν είναι απαραίτητο να ποσοτικοποιήσεις την πιθανότητα

	εμφάνισης απειλής.
+Επιτυγχάνεται όλο και περισσότερη ακρίβεια σε επόμενες αξιολογήσεις λόγω της ύπαρξης των προηγούμενων καταγεγραμμένων αποτελεσμάτων.	+Δεν είναι απαραίτητο να εκτιμηθούν οι οικονομικές αξίες των στοιχείων πληροφορίας.
-Τα μεγέθη αντικτύπων βασίζονται σε υποκειμενικές απόψεις των ατόμων που διεξάγουν την αξιολόγηση.	+Μπορούν να συμμετέχουν στη διαδικασία άτομα που δεν είναι ειδικοί σε θέματα ασφαλείας.
-Η διαδικασία είναι αρκετά χρονοβόρα.	-Ανεπαρκής διαφοροποίηση μεταξύ των κρίσιμων κινδύνων.
-Οι μαθηματικοί υπολογισμοί μπορούν να αποδειχθούν πολυσύνθετοι και χρονοβόροι.	-Είναι δύσκολο να δικαιολογήσεις την επένδυση σε μέτρα ελέγχου λόγω της μη ύπαρξης οικονομικών μεγεθών.
-Τα αποτελέσματα παρουσιάζονται μόνο σε αριθμητικούς και κυρίως οικονομικούς όρους, κάτι που δυσχεραίνει την κατανόηση τους από όλο το εύρος του οργανισμού.	-Τα αποτελέσματα εξαρτώνται σε μεγάλο βαθμό από τις ικανότητες της ομάδας που πραγματοποιεί την αξιολόγηση.
-Η διαδικασία πραγματοποιείται κυρίως από εξειδικευμένους σε θέματα ασφάλειας.	

Πίνακας 3 - Σύγκριση ποιοτικής και ποσοτικής μεθοδολογίας

4.3.4. Άλλες μεθοδολογίες

CRAMM

Η μεθοδολογία CctaRAMM (Central Computer and Telecommunications Agency Risk Analysis and Management Method) δημιουργήθηκε το 1985. Η έκδοση 5.1 έγινε διαθέσιμη το 2005 και περιλαμβάνει τρία στάδια:

1. Αναγνώριση και εκτίμηση των στοιχείων πληροφορίας του οργανισμού.
2. Αξιολόγηση ευαλωτοτήτων και απειλών.
3. Επιλογή μέτρων προστασίας.

Εφαρμόζει ένα είδος ποιοτικής μεθοδολογίας αξιολόγησης κινδύνου σε επίπεδο στοιχείου πληροφορίας (asset-driven) και αξιολογεί τα στοιχεία με κύριο άξονα τον αντίκτυπο στον οργανισμό που θα έχει μια ενδεχόμενη παραβίαση των τριών αρχών της ασφάλειας πληροφοριών, δηλαδή της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας. Η μεθοδολογία CRAMM έρχεται σε συμφωνία με τις απαιτήσεις που ορίζει το ISO/IEC 27001 (Calder & Watkins, 2010).

Όσον αφορά τον υπολογισμό του βαθμού κινδύνου, η μέθοδος χρησιμοποιεί μια κλίμακα απο το ένα έως το επτά συνδυάζοντας την αξία κάθε στοιχείου πληροφορίας με το μέγεθος της απειλής και της ευαλωτότητας του. Σε αυτή την κλίμακα ο αριθμός ένα αντιστοιχεί σε έναν πολύ χαμηλό κίνδυνο και ο αριθμός επτά σε έναν πάρα πολύ υψηλό (Yazar, 2002).

OCTAVE

Η συγκεκριμένη προσέγγιση μπορεί να σχεδιαστεί και να υλοποιηθεί με τέτοιο τρόπο ώστε να καλύπτει πλήρως τις απαιτήσεις του ISO/IEC 27001, αφού στην αρχική της μορφή δεν τις ικανοποιεί. Το OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) είναι ένα σύνολο από κριτήρια που μπορεί να αναπτυχθεί σε πολλές διαφορετικές μεθοδολογίες, είτε ποσοτικές είτε ποιοτικές. Από τη στιγμή που μια μεθοδολογία τηρεί τα συγκεκριμένα κριτήρια, τότε είναι μια μέθοδος συμβατή με OCTAVE. Για να εφαρμόσει μια τέτοια μέθοδο, ο οργανισμός σχηματίζει μια μικρή ομάδα από όλο το φάσμα των τμημάτων του που έχει στόχο να εξετάσει τους κινδύνους, τις πρακτικές προστασίας και την τεχνολογία για να επιτύχει την ασφάλεια πληροφοριών. Το OCTAVE απαιτεί από αυτή την ομάδα συγκεκριμένα βήματα:

- Αναγνώριση των πόρων του οργανισμού που σχετίζονται με πληροφορίες και είναι σημαντικοί.
- Έμφαση στους πόρους που είναι υψηλότερης κρισιμότητας.
- Ανάλυση των σχέσεων των κρίσιμων στοιχείων πληροφορίες με τις απειλές και τις ευαλωτότητες τους.
- Αξιολόγηση κινδύνων στο επίπεδο της καθημερινής χρήσης των στοιχείων πληροφορίας του οργανισμού.
- Δημιουργία στρατηγικής προστασίας και σχεδίων άμβλυνσης κινδύνων (Calder & Watkins, 2010).

Το Carnegie Mellon University που ανέπτυξε τα κριτήρια OCTAVE εξέδωσαν τρεις μεθοδολογίες: την πρωτότυπη Octave Method για πολύ μεγάλους και σύνθετους οργανισμούς, την Octave-S για μικρούς οργανισμούς που απασχολούν 20 έως 80 άτομα και την Octave-Allegro μια βέλτιστη προσέγγιση στην ασφάλεια πληροφοριων (Calder & Watkins, 2010).

Οι λόγοι που στην αρχική της μορφή ως μέθοδος δεν έρχεται σε συμφωνία με το πρότυπο ISO/IEC 27001 είναι δύο. Πρώτον, απαιτεί την αναγνώριση των πιο σημαντικών και κρίσιμων στοιχείων πληροφορίας του οργανισμού, ενώ το πρότυπο απαιτεί την αναγνώριση όλων των πόρων. Δεύτερον, εξετάζει τις ευαλωτότητες των στοιχείων κυρίως σε επίπεδο τεχνολογίας και δικτύων, ενώ το πρότυπο απαιτεί την αναζήτηση όλων των πιθανών ευαλωτοτήτων. Για τους λόγους αυτούς, απαιτείται μια προσαρμογή του OCTAVE στις απαιτήσεις του ISO/IEC 27001 ώστε η μεθοδολογία να είναι συμβατή με το πρότυπο (Calder & Watkins, 2010).

IRAM, SARA, SPRINT και FIRM

Ο ISF (Information Security Forum) είναι ένας αρκετά κλειστός οργανισμός που παρέχει πρόσβαση στα περιεχόμενα του μόνο στα περίπου 260 μέλη του παγκοσμίως. Έχει αναπτύξει ένα σύνολο μεθοδολογιών και εργαλείων γύρω από την αξιολόγηση κινδύνων που μπορούν να χρησιμοποιηθούν συμπληρωματικά. Αυτά τα εργαλεία είναι:

- IRAM: Information Risk Analysis Methodologies
- SARA: Simple to Apply Risk Analysis, σχεδιασμένο για την αντιμετώπιση των κρίσιμων επιχειρησιακών συστημάτων
- SPRINT: Simplified Process for Risk Identification, σχεδιασμένο για τα σημαντικά, αλλά όχι μόνο τα πιο κρίσιμα, συστήματα.
- FIRM: Fundamental Information Risk Management

Το σύνολο εργαλείων του ISF υποστηρίζει όλες τις θεμελιώδεις φάσεις της διαχείρισης κινδύνου, και περιέχει αρκετά χρήσιμα στοιχεία για την ανάπτυξης μιας μεθοδολογίας συμβατής με το ISO/IEC 27001. Ωστόσο, τα εργαλεία αυτά δίνουν έμφαση στα επιχειρησιακά συστήματα (business-driven) και όχι στα ατομικά στοιχεία πληροφοριών (asset-driven) του οργανισμού όπως ορίζει το ISO/IEC 27001, και για

το λόγο αυτό μια προσέγγιση συμβατή με το πρότυπο θα πρέπει να χρησιμοποιήσει τα εργαλεία αυτά με τέτοιο τρόπο που να καλύπτει τις απαιτήσεις του (Calder & Watkins, 2010).

CORAS

Η προσέγγιση αυτή βασίζεται στη μοντελοποίηση (model-driven) και ακολουθεί τη διαδικασία που ορίζει το ISO 31000, ένα διεθνές πρότυπο για τη διαχείριση κινδύνου. Σε αυτό το πρότυπο είναι βασισμένο το ISO 27005, που όπως έχει ήδη αναφερθεί, εξηγεί αναλυτικά τη διαδικασία διαχείρισης κινδύνου που απαιτεί το ISO/IEC 27001. Η μέθοδος αυτή περιλαμβάνει τρία μέρη, το CORAS method, το CORAS language και το CORAS tool. Το πρώτο περιέχει τεχνικές και οδηγίες χρήσης, το δεύτερο τη μοντελοποίηση για όλα τα στάδια της μεθόδου και το τρίτο αποτελεί ένα εργαλείο δημιουργίας των διαγραμμάτων CORAS (Beckers et al., 2014).

Όσον αφορά την αξιολόγηση κινδύνου, αυτή περιλαμβάνει την αναγνώριση των κινδύνων, τον υπολογισμό τους και την αποτίμηση τους. Η αναγνώριση των ανεπιθύμητων συμβάντων μαζί με τις απειλές και τις ευαλωτότητες που μπορούν να τα προκαλέσουν πραγματοποιείται με τη βοήθεια του διαγράμματος απειλών. Ο υπολογισμός του κινδύνου, δηλαδή ο υπολογισμός της πιθανότητας και του αντικτύπου τέτοιων συμβάντων γίνεται επίσης με τη χρήση του διαγράμματος απειλών, που περιλαμβάνει υποθετικά σενάρια απειλων. Τα αποτελέσματα αυτής της διαδικασίας καταγράφονται χρησιμοποιώντας τα διαγράμματα κινδύνου (CORAS risk diagrams). Η αποτίμηση των κινδύνων κατατάσσει τους αναγνωρισμένους κίνδυνους σε σύγκριση με τα κριτήρια που έχουν οριστεί πριν την αξιολόγηση και αποφασίζεται ποια είναι μη αποδεκτά (Beckers et al., 2014).

Το πλεονέκτημα της μεθόδου CORAS είναι ότι μπορεί να επεξεργαστεί πολλά και διαφορετικά στοιχεία εισόδου όπως στατιστικά στοιχεία, ερωτηματολόγια και αρχεία ασφάλειας (Beckers et al., 2014).

Η συγκεκριμένη προσέγγιση ακολουθεί μια διαδικασία παρόμοια με τα ISO 31000 και ISO 27005 και κατά συνέπεια εκπληρώνει πολλές από τις απαιτήσεις του ISO/IEC 27001, συνεπώς είναι συμβατή με το πρότυπο (Beckers et al., 2014).

Κεφάλαιο 5: Μια πρόταση μεθοδολογίας αξιολόγησης κινδύνου

5.1. Περιγραφή της μεθοδολογίας

Στο συγκεκριμένο κεφάλαιο παρουσιάζεται μια μεθοδολογία αξιολόγησης κινδύνου που μπορεί να χρησιμοποιηθεί από μικρούς και μεσαίους οργανισμούς ή αντίστοιχου μεγέθους τμήματα οργανισμού. Πρόκειται για μια μεθοδολογία που συνδυάζει ποιοτικούς και ποσοτικούς όρους, και πιο συγκεκριμένα ποσοτικοποιεί ποιοτικούς όρους για την καλύτερη υλοποίηση της.

Η παρούσα αξιολόγηση περιλαμβάνει τα παρακάτω στάδια:

- Αναγνώριση των στοιχείων/πόρων πληροφορίας (Asset identification).
- Αναγνώριση των απειλών και ευαλωτοτήτων κάθε στοιχείου (Threats – Vulnerabilities).
- Καθορισμός της πιθανότητας πραγματοποίησης ενός συμβάντος απειλής (Likelihood).
- Καθορισμός του αντίκτυπου στον οργανισμό της πραγματοποίησης ενός συμβάντος απειλής (Impact).
- Υπολογισμός βαθμού κινδύνου κάθε συμβάντος (Risk evaluation).
- Καθορισμός των κριτηρίων αποδοχής κινδύνου (Criteria of risk acceptance).

Στη συνέχεια περιγράφονται αναλυτικά τα στάδια της μεθόδου.

Αναγνώριση των στοιχείων/πόρων πληροφορίας (Asset identification)

Η μεθοδολογία αυτή αξιολογεί τον κίνδυνο σε επίπεδο στοιχείου πληροφορίας (asset-driven). Για το λόγο αυτό το στάδιο της αναγνώρισης των στοιχείων είναι πολύ σημαντικό για την ολοκληρωμένη χρήση της. Ειδικότερα, είναι ένα κρίσιμο κομμάτι της μεθόδου καθώς ενδεχόμενη μη κάλυψη όλων των σημαντικών στοιχείων εγκυμονεί τεράστιους κινδύνους στην ασφάλεια πληροφοριών του οργανισμού. Στην

περίπτωση που κάποιος σημαντικός πόρος δεν αναγνωριστεί, είναι πολύ πιθανό οι απειλές που σχετίζονται με αυτόν να εκμεταλλευτούν συγκεκριμένες ευαλωτότητες και να πραγματοποιηθούν.

Η συγκεκριμένη μέθοδος προτείνει την κατηγοριοποίηση των στοιχείων σε έξι τομείς με σκοπό τη διευκόλυνση της ταυτοποίησης των στοιχείων. Ακολουθούν οι έξι τομείς και παραδείγματα τους:

1. **Οργανωτική δομή** *(Structure of the organization).* Αφορά τον τρόπο που λειτουργεί καθημερινά ο οργανισμός. Παραδείγματα αυτού του τομέα αποτελούν ενέργειες, διαδικασίες, λειτουργίες, έγγραφα αρχεία, άδειες χρήσης λογισμικού, συμβόλαια με συνεργάτες και προμηθευτές, οδηγίες χρήσης εξοπλισμού και εγκαταστάσεων και γενικά ό,τι σχετίζεται με τη δομή της καθημερινής λειτουργίας του οργανισμού.
2. **Υλικό** *(Hardware).* Στην κατηγορία αυτή ανήκουν όλα τα στοιχεία hardware του οργανισμού. Αυτά μπορεί να είναι στοιχεία γενικού υλικού (για παράδειγμα υπολογιστές και servers), φορητά στοιχεία (για παράδειγμα προσωπικοί υπολογιστές, εξωτερικοί σκληροί δίσκοι, usb sticks), εξοπλισμός δικτύου (για παράδειγμα ρούτερ και μεταγωγείς) και υλικό προστασίας (για παράδειγμα γεννήτριες και ups).
3. **Λογισμικό** *(Software).* Αφορά κάθε είδος λογισμικού απαραίτητο για τη χρήση των υπολογιστικών συστημάτων του οργανισμού. Παραδείγματα λογισμικού αποτελούν τα λειτουργικά συστήματα, οι εφαρμογές και τα προγράμματα χωρίς ή με σύνδεση στο δίκτυο και το λογισμικό που σχετίζεται με βάσεις δεδομένων.
4. **Τηλεπικοινωνίες** *(Communications).* Σχετίζεται με την επικοινωνία εντός και εκτός του οργανισμού και περιλαμβάνει κυρίως τους δίαυλους μεταφοράς δεδομένων όπως κεραίες, οπτικές ίνες και το διαδίκτυο.
5. **Φυσικό περιβάλλον** *(Physical Environment).* Περιλαμβάνει όλους τους φυσικούς χώρους του οργανισμού, όπως δωμάτια, γραφεία, εγκαταστάσεις και αποθήκες.
6. **Προσωπικό** *(Personell).* Σε αυτή την κατηγορία κατατάσσονται όλοι οι ανθρώπινοι πόροι, όπως διευθυντές τμημάτων, υπεύθυνοι πρότζεκτ, χρήστες των συστημάτων, αναλυτές, προγραμματιστές και άλλοι εργαζόμενοι.

Αναγνώριση των απειλών και ευαλωτοτήτων (Threats – Vulnerabilities).

Ύστερα από την αναγνώριση των στοιχείων πληροφορίας του οργανισμού, η αξιολόγηση προχωρά στη διαδικασία αναγνώρισης των ζεύγων απειλών και ευαλωτοτήτων για καθένα από αυτά. Η μέθοδος προτείνει ένα ευρύ πεδίο κατηγοριών απειλών, στο οποίο μπορεί ο οργανισμός να εντοπίσει και να αναγνωρίσει τις απειλές που αφορούν τα στοιχεία πληροφορίας τους. Το πεδίο αυτό περιλαμβάνει:

- Κακόβουλες επιθέσεις στο λογισμικό (π.χ. ιοί, hacking).
- Σφάλματα και αποτυχίες του λογισμικού (π.χ. bugs, σφάλματα κώδικα).
- Σφάλματα και αποτυχίες του υλικού (π.χ. αποτυχίες στη λειτουργία εξοπλισμού).
- Ακούσια καταστροφή ή αλλοίωση πληροφοριών (π.χ. ατυχήματα, λάθη εργαζομένων).
- Κακόβουλες ενέργειες κατασκοπείας (π.χ. μη εξουσιοδοτημένη πρόσβαση σε χώρους ή δεδομένα).
- Κακόβουλες ενέργειες βανδαλισμού (π.χ. καταστροφή πόρων).
- Κακόβουλες ενέργειες κλοπής (π.χ. κλοπή προσωπικού υπολογιστή ή εγγράφων).
- Φυσικές καταστροφές (π.χ. φωτιά, πλημμύρα, σεισμός).
- Παραβίαση της πνευματικής ιδιοκτησίας (π.χ. παράνομη χρήση μιας πατέντας του οργανισμού).

Επίσης, η μέθοδος προτείνει μια σειρά κατηγοριών ευαλωτοτήτων στις οποίες ο οργανισμός μπορεί ενδεχομένως να αντιστοιχίσει τις απειλές που έχει εντοπίσει. Οι κατηγορίες που προτείνονται είναι οι ακόλουθες:

- Ελλειπής ή μηδενική προστασία φυσικών χώρων (π.χ. μη ύπαρξη ασφάλειας εγκαταστάσεων).
- Ελλειπής ή μηδενική προστασία από φυσικές καταστροφές (π.χ. σύστημα πυρόσβεσης, αντιπλημμυρικό σύστημα).
- Μη καθορισμός των εξουσιοδοτημένων ατόμων για την πρόσβαση σε φυσικούς χώρους ή συστήματα (π.χ. μπορούν όλοι οι εργαζόμενοι να εισέλθουν στο δωμάτιο των servers).

- Μη επαρκής εκπαίδευση των εργαζομένων σε σχέση με την ασφάλεια πληροφοριών (π.χ. εργαζόμενοι αγνοούν τη σημασία της προστασίας των πληροφοριών μέσα στον οργανισμό).
- Ελλειπή μέτρα προστασίας από κακόβουλες επιθέσεις λογισμικού (π.χ. απαρχαιωμένα προγράμματα antivirus).
- Μη ύπαρξη δευτερογενούς και τριτογενούς χώρου αποθήκευσης δεδομένων και πληροφοριών (π.χ. οι εργαζόμενοι αποθηκεύουν πληροφορίες μόνο σε φακέλους του υπολογιστή τους).
- Χαμηλή απόδοση μέτρων προστασίας προηγούμενου σχεδίου αντιμετώπισης κινδύνων.
- Ανθρώπινες αδυναμίες (π.χ. εφησυχασμός, απροσεξία).
- Τερματισμός εργασίας (π.χ. πρώην εργαζόμενος πηγαίνει σε ανταγωνιστή και διατηρεί ακόμα πρόσβαση σε δεδομένα του οργανισμού).
- Μη ξεκάθαρος ορισμός των ρόλων και των υποχρεώσεων σε σχέση με την ασφάλεια πληροφοριών (π.χ. η διοίκηση δεν έχει καθορίσει συγκεκριμένο κανόνα που υποχρεώνει τον εργαζόμενο να κλείνει ή να θέτει σε αδράνεια τον υπολογιστή του όταν κάνει μεσημεριανό διάλειμμα).

Συνεπώς, όταν ολοκληρωθεί και η διαδικασία αναγνώρισης των ευαλωτοτήτων για κάθε απειλή, ουσιαστικά έχει καθοριστεί και η σχέση στοιχείο πληροφορίας - απειλή/ες – ευαλωτότητα/ες (asset – threats – vulnerabilities) και πλέον είναι δυνατή η εξαγωγή υπολογισμών για τα μεγέθη πιθανότητα – αντίκτυπος – κίνδυνος (likelihood – impact – risk). Είναι σημαντικό να αναφερθεί πως μια απειλή μπορεί να αντιστοιχίζεται με πολλές διαφορετικές ευαλωτότητες και πως μια ευαλωτότητα μπορεί να σχετίζεται μια διάφορες απειλές.

Η πιθανότητα πραγματοποίησης ενός συμβάντος απειλής (Likelihood)

Η συγκεκριμένη μεθοδολογία αξιολόγησης κινδύνου αποτιμά την πιθανότητα πραγματοποίησης ενός συμβάντος απειλής σύμφωνα με την κλίμακα ένα (1) έως πέντε (5) και αντιστοιχίζει αυτές τις τιμές στο σχήμα Πολύ μικρή – Μικρή – Μεσαία – Μεγάλη – Πολύ μεγάλη σύμφωνα με τα παρακάτω (βλ. Πίνακας 4).

Πολύ Μικρή πιθανότητα	1	Χαμηλά κίνητρα του ατόμου που σχετίζεται με την απειλή, μη ευνοϊκές συνθήκες για να εκμεταλλευτεί τις ευαλωτότητες ή επαρκή μέτρα προστασίας του οργανισμού καθιστούν το συγκεκριμένο συμβάν σχεδόν απίθανο.
Μικρή πιθανότητα	2	Χαμηλά κίνητρα του ατόμου που σχετίζεται με την απειλή, μη ευνοϊκές συνθήκες για να περατωθεί ή επαρκή μέτρα προστασίας του οργανισμού προσδίδουν στο συγκεκριμένο συμβάν λίγες πιθανότητες πραγματοποίησης.
Μεσαία πιθανότητα	3	Τα κίνητρα του ατόμου που σχετίζεται με την απειλή είναι υπαρκτά ή οι συνθήκες μπορεί να γίνουν ευνοϊκές για την εκμετάλλευση ευαλωτοτήτων ή τα υπάρχοντα μέτρα ασφάλειας είναι σε μέτριο επίπεδο. Το συμβάν είναι πιθανό να πραγματοποιηθεί.
Μεγάλη πιθανότητα	4	Τα κίνητρα του ατόμου που σχετίζεται με την απειλή ειναι υψηλά ή οι συνθήκες εκμετάλλευσης ευαλωτοτήτων είναι ευνοϊκές ή τα μέτρα ασφάλειας πληροφοριών του οργανισμού είναι μη αποτελεσματικά. Το συμβάν έχει υψηλές πιθανότητες να πραγματοποιηθεί.
Πολύ Μεγάλη πιθανότητα	5	Πολύ υψηλά κίνητρα του ατόμου που σχετίζεται με την απειλή, εξαιρετικά ευνοϊκές συνθήκες για να εκμεταλλευτεί τις ευαλωτότητες ή πολύ ανεπαρκή μέτρα προστασίας του οργανισμού καθιστούν το συγκεκριμένο συμβάν σχεδόν βέβαιο.

Πίνακας 4 - Η αποτίμηση της πιθανότητας πραγματοποίησης απειλής

Η συγκεκριμένη μεθοδολογία δεν καθορίζει τα κριτήρια με τα οποία ο οργανισμός θα αποφασίσει την τιμή της πιθανότητας πραγματοποίησης ενός συμβάντος απειλής. Αντίθετα του δίνει τη δυνατότητα να επιλέξει αυτόνομα με ποιο τρόπο θα αξιολογήσει το κάθε συμβάν. Τέτοιοι τρόποι μπορούν να αποτελέσουν για παράδειγμα ο αριθμός προηγούμενων ίδιων συμβάντων ανά μήνα, εξάμηνο ή χρόνο, το πόσο ισχυρές είναι κάποιες ευαλωτότητες, ερωτηματολόγια στους εργαζομένους και αθροιστικά συμπεράσματα ή η υποκειμενική άποψη του ατόμου που υλοποιεί την αξιολόγηση.

Ο αντίκτυπος πραγματοποίησης ενός συμβάντος απειλής (Impact)

Αυτό το στάδιο είναι πολύ σημαντικό για τα αποτελέσματα της αξιολόγησης κινδύνων. Έχει επιλεχθεί μια πολυδιάστατη αποτίμηση του αντίκτυπου ενός συμβάντος απειλής σε πέντε επίπεδα, και πιο συγκεκριμένα:

- Ο αντίκτυπος στην παροχή προϊόντων/υπηρεσιών.
- Ο αντίκτυπος στο σχεδιασμό.
- Ο αντίκτυπος στη συμμόρφωση με τα νομικά πλαίσια.
- Ο αντίκτυπος στη φήμη του οργανισμού.
- Ο αντίκτυπος στις οικονομικές απώλειες.

Η μεθοδολογία που προτείνεται αποτιμά κάθε μία από παραπάνω κατηγορίες συνεπειών στην κλίμακα ένα (1) έως δεκαπέντε (15) και τις αντιστοιχεί στο ποιοτικό σχήμα Αμελητέας σημασίας – Μικρής σημασίας – Μεσαίας σημασίας – Μεγάλης σημασίας – Ύψιστης σημασίας ως εξής:

Παροχή προϊόντων/υπηρεσιών

Η παροχή προϊόντων και υπηρεσιών σε πελάτες του οργανισμού μπορεί να επηρεαστεί άμεσα και πολύ αρνητικά από την πραγματοποίηση κάποιου συμβάντος απειλής στην ασφάλεια πληροφοριών. Συνήθως ο αρνητικός αυτός αντίκτυπος αφορά τη δημιουργία εμποδίων στη διαδικασία με αποτέλεσμα την καθυστέρηση της ή ακόμα και τη μη δυνατότητα ολοκλήρωσης της. Για παράδειγμα, αν η ιστοσελίδα μιας εταιρίας ηλεκτρονικού εμπορίου δεχτεί επίθεση από χάκερς και υπολειτουργεί για ώρες, γίνεται εύκολα κατανοητό το πόσο αρνητικά επηρεάζεται η διαδικασία αγοράς από τους καταναλωτές. Στον Πίνακα 5 που ακολουθεί παρουσίαζεται ο τρόπος που αποτιμάται ο συγκεκριμένος αντίκτυπος.

Αμελητέας σημασίας αντίκτυπος	1-3	Οι αρνητικές συνέπειες του συμβάντος απειλής στην παροχή προϊόντων/υπηρεσιών είναι σχεδόν μη υπαρκτές.
Μικρής σημασίας αντίκτυπος	4-6	Οι αρνητικές συνέπειες του συμβάντος απειλής στην παροχή προϊόντων/υπηρεσιών είναι ελάσσονος σημασίας.
Μεσαίας σημασίας αντίκτυπος	7-9	Οι αρνητικές συνέπειες του συμβάντος απειλής στην παροχή προϊόντων/υπηρεσιών είναι ορατές και ως ένα βαθμό ανεκτές.
Μεγάλης σημασίας αντίκτυπος	10-12	Οι αρνητικές συνέπεις του συμβάντος απειλής στην παροχή προϊόντων/υπηρεσιών είναι πολύ σημαντικές και επηρέαζουν άμεσα τη διαδικασία.
Ύψιστης σημασίας αντίκτυπος	13-15	Οι αρνητικές συνέπειες του συμβάντος απειλής στην παροχή προϊόντων/υπηρεσιών είναι τέτοιου βαθμού, που επιφέρουν πολύ σοβαρό πλήγμα στη διαδικασία.

Πίνακας 5 - Η κλίμακα μέτρησης του αντίκτυπου στην παροχή προϊόντων/υπηρεσιών

Σχεδιασμός

Με τον όρο σχεδιασμό η παρούσα μεθοδολογία αναφέρεται κυρίως στην εκπλήρωση βραχυπρόθεσμων και μεσοπρόθεσμων στόχων του οργανισμού. Για παράδειγμα, στο ίδιο παράδειγμα με προηγουμένως, η εταιρία ηλεκτρονικού εμπορίου μπορεί να έχει ημερήσιο στόχο ένα συγκεκριμένο αριθμό πωλήσεων. Η απειλή που αναφέρθηκε οδηγεί αυτό το πλάνο σε αποτυχία. Στον Πίνακα 6 που ακολουθεί παρουσίαζεται ο τρόπος που αποτιμάται ο συγκεκριμένος αντίκτυπος.

Αμελητέας σημασίας αντίκτυπος	1-3	Το συμβάν απειλής δεν επηρεάζει σχεδόν καθόλου το σχεδιασμό.
Μικρής σημασίας αντίκτυπος	4-6	Οι αρνητικές συνέπειες του συμβάντος απειλής στο σχεδιασμό είναι άμεσα διαχειρίσιμες.
Μεσαίας σημασίας αντίκτυπος	7-9	Οι αρνητικές συνέπειες του συμβάντος απειλής στο σχεδιασμό είναι ορατές και ως ένα βαθμό ανεκτές.
Μεγάλης σημασίας αντίκτυπος	10-12	Το συμβάν απειλής είναι πολύ πιθανό να οδηγήσει στην αποτυχία σχεδίων.
Ύψιστης σημασίας αντίκτυπος	13-15	Το συμβάν απειλής είναι σχεδόν βέβαιο ότι θα οδηγήσει σε αποτυχία το σχεδιασμό.

Πίνακας 6 - Η κλίμακα μέτρησης του αντίκτυπου στο σχεδιασμό

Συμμόρφωση με νομικά πλαίσια

Η πραγματοποίηση ενός συμβάντος απειλής μπορεί να έχει αρνητικό αντίκτυπο στη συμμόρφωση του οργανισμού με νόμους και διατάξεις. Για παράδειγμα, αν σε έναν οργανισμό κλαπεί κάποιος προσωπικός υπολογιστής που περιέχει τα στοιχεία ανθρώπων ενός πελατολογίου και αυτά τα στοιχεία βρίσκονται πλέον σε κατοχή τρίτων προσώπων, τότε πρόκειται για άμεση παραβίαση των προσωπικών δεδομένων. Στον Πίνακα 7 που ακολουθεί παρουσίαζεται ο τρόπος που αποτιμάται ο συγκεκριμένος αντίκτυπος.

Αμελητέας σημασίας αντίκτυπος	1-3	Το συμβάν απειλής δεν επηρεάζει σχεδόν καθόλου τη συμμόρφωση του οργανισμού με το νόμο.
Μικρής σημασίας αντίκτυπος	4-6	Το συμβάν απειλής προκαλεί ένα άμεσα διαχειρίσιμο πρόβλημα στη συμμόρφωση του οργανισμού με το νόμο.
Μεσαίας	7-9	Οι αρνητικές συνέπειες του συμβάντος απειλής στη

σημασίας αντίκτυπος		συμμόρφωση του οργανισμού με το νόμο είναι ορατές και ως ένα βαθμό αντιμετωπίσιμες.
Μεγάλης σημασίας αντίκτυπος	10-12	Το συμβάν απειλής είναι πολύ πιθανό να οδηγήσει σε νομικές παραβάσεις.
Ύψιστης σημασίας αντίκτυπος	13-15	Το συμβάν απειλής είναι σχεδόν βέβαιο ότι θα οδηγήσει σε νομικές παραβάσεις.

Πίνακας 7 - Η κλίμακα μέτρησης του αντίκτυπου στη συμμόρφωση με νομικά πλαίσια

Φήμη του οργανισμού

Η ασφάλεια πληροφοριών αποτελεί καθοριστικό παράγοντα διατήρησης της φήμης ενός οργανισμού σε ένα υψηλό επίπεδο. Ένα συμβάν απειλής μπορεί να επιφέρει πλήγμα στη φήμη. Για παράδειγμα, η διαρροή απόρρητων πληροφοριών του οργανισμού ως αποτέλεσμα κακόβουλης ενέργειας ευρέως στο διαδίκτυο σίγουρα προκαλεί πλήμα στην αξιοπιστία του ως προς το κοινό. Στον Πίνακα 8 που ακολουθεί παρουσίαζεται ο τρόπος που αποτιμάται ο συγκεκριμένος αντίκτυπος.

Αμελητέας σημασίας αντίκτυπος	1-3	Το συμβάν απειλής δεν επιφέρει πλήγμα στη φήμη του οργανισμού.
Μικρής σημασίας αντίκτυπος	4-6	Το συμβάν απειλής προκαλεί ένα μικρό πλήγμα στη φήμη του οργανισμού που μπορεί εύκολα να αποκατασταθεί.
Μεσαίας σημασίας αντίκτυπος	7-9	Οι αρνητικές συνέπειες του συμβάντος απειλής στη φήμη του οργανισμού είναι ως ένα βαθμό διαχειρίσιμες.
Μεγάλης σημασίας αντίκτυπος	10-12	Το συμβάν απειλής επιφέρει σημαντικό πλήγμα στη φήμη και στην αξιοπιστία του οργανισμού.
Ύψιστης σημασίας αντίκτυπος	13-15	Το συμβάν απειλής επιφέρει πολύ σοβαρό πλήγμα στη φήμη και στην αξιοπιστία του οργανισμού.

Πίνακας 8 - Η κλίμακα μέτρησης του αντίκτυπου στη φήμη του οργανισμού

Οικονομικές απώλειες

Ένα από τα πιο κοινά αρνητικά αποτελέσματα της πραγματοποίησης μιας απειλής αφορά τις οικονομικές απώλειες. Οι απώλειες αυτές μπορεί να οφείλονται στην αποτυχία οικονομικών στόχων λόγω της απειλής ή στην ανάγκη αποκατάστασης του αλλοιωμένου στοιχείου πληροφορίας του οργανισμού. Για παράδειγμα, στην πρώτη περίπτωση ενδεχόμενη βλάβη του λογισμικού που χρησιμοποιείται για τις τραπεζικές πληρωμές πελατών προς τον οργανισμό για την αγορά των προϊόντων του θα έχει σαν άμεσο αποτέλεσμα τη μείωση των πωλήσεων και συνεπώς των εσόδων του. Στη δεύτερη περίπτωση, ένα συμβάν φυσικής απειλής όπω είναι η φωτιά που δε θα αποτραπεί θα δημιουργήσει ανυπολόγιστες οικονομικές απώλειες λόγω της καταστροφής εγκαταστάσεων και εξοπλισμού. Στον Πίνακα 9 που ακολουθεί παρουσίαζεται ο τρόπος που αποτιμάται ο συγκεκριμένος αντίκτυπος.

Αμελητέας σημασίας αντίκτυπος	1-3	Οι οικονομικές απώλειες του οργανισμού είναι μηδαμινές.
Μικρής σημασίας αντίκτυπος	4-6	Το συμβάν απειλής προκαλεί μικρές οικονομικές απώλειες στον οργανισμό.
Μεσαίας σημασίας αντίκτυπος	7-9	Οι οικονομικές απώλειες λόγω του συμβάντος απειλής είναι διακριτές και ως ένα βαθμό ανεκτές.
Μεγάλης σημασίας αντίκτυπος	10-12	Το συμβάν απειλής επιφέρει μεγάλες οικονομικές απώλειες στον οργανισμό.
Ύψιστης σημασίας αντίκτυπος	13-15	Το συμβάν απειλής επιφέρει πολύ σοβαρό οικονομικό πλήγμα στον οργανισμό.

Πίνακας 9 - Η κλίμακα μέτρησης του αντίκτυπου σε οικονομικές απώλειες

Η επιλογή της κλίμακας 1 έως 15 έγινε για την καλύτερη διάκριση του κάθε αντίκτυπου σύμφωνα με τις πέντε κατηγορίες που παρουσιάστηκαν. Ενδεχόμενη μικρότερη κλίμακα, για παράδειγμα 1 έως 5, δεν αναδεικνύει σε μεγάλο βαθμό τις

διαφορές ανάμεσα στις κατηγορίες. Η χρησιμότητα της κλίμακας αυτής οφείλεται και στην έμφαση που δίνει η μεθοδολογία στον αντίκτυπο της απειλής σε σχέση με την πιθανότητα πραγματοποίησης της και αποτυπώνεται στον υπολογισμό του γινομένου του βαθμού κινδύνου.

Ο υπολογισμός βαθμού κινδύνου (Risk evaluation)

Εφόσον έχουν αποδοθεί τιμές στην πιθανότητα και στον αντίκτυπο πραγματοποίησης κάθε συμβάντος απειλής σύμφωνα με τις απειλές και ευαλωτότητες που αναγνωρίστηκαν για κάθε στοιχείο πληροφορίας του οργανισμού, ακολουθεί το στάδιο υπολογισμού του κινδύνου. Η συγκεκριμένη μεθοδολογία ακολουθεί έναν από τους πλέον παραδοσιακούς τύπους υπολογισμού του κινδύνου:

Κίνδυνος = (Πιθανότητα συμβάντος απειλής) x (Αντίκτυπος συμβάντος απειλής)

Ή

Risk = Likelihood x Impact

Η διαφοροποίηση της συγκεκριμένης μεθοδολογίας από άλλες πραγματοποιείται στο μέγεθος του αντικτύπου, καθώς επιλέγεται η μεγαλύτερη τιμή αντικτύπου από τις πέντε κατηγορίες που αναλύθηκαν στην προηγούμενη ενότητα. Με αυτόν τον τρόπο ο τύπος υπολογισμού του βαθμού κινδύνου κάθε συμβάντος είναι ο ακόλουθος:

Κίνδυνος = (Πιθανότητα συμβάντος απειλής) x (Ο μεγαλύτερος σε τιμή αντίκτυπος από τις πέντε κατηγορίες αντικτύπων)

Ή

Risk = Likelihood x max(Impacts)

Ο βαθμός κινδύνου κυμαίνεται, λόγω της πράξης του γινομένου από 1 έως 75. Η κλίμακα αυτή προκύπτει από το χαμηλότερο δυνατό γινόμενο (1 x 1 = 1) και το υψηλότερο δυνατό (5 x 15 = 75). Ωστόσο τα αριθμητικά αποτελέσματα αυτά πρέπει να μεταφραστούν με κάποιο τρόπο σε μια πιο κατανοητή μορφή και συγκεκριμένα σε

ένα ποιοτικό σχήμα. Το σχήμα που έχει επιλεχθεί για το βαθμό κινδύνου είναι το Πολύ Χαμηλός – Χαμηλός – Μεσαίος – Υψηλός – Πολύ Υψηλός και προκύπτει από τους παρακάτω συνδυασμούς πιθανότητας – αντικτύπου (βλ. Πίνακας 10).

Πιθανότητα \ Αντίκτυπος	Αμελητέας σημασίας	Μικρής σημασίας	Μεσαίας σημασίας	Μεγάλης σημασίας	Ύψιστης σημασίας
Πολύ Μικρή	Πολύ Χαμηλός κίνδυνος	Πολύ Χαμηλός κίνδυνος	Πολύ Χαμηλός κίνδυνος	Χαμηλός κίνδυνος	Χαμηλός κίνδυνος
Μικρή	Πολύ Χαμηλός κίνδυνος	Χαμηλός κίνδυνος	Χαμηλός κίνδυνος	Μεσαίος κίνδυνος	Μεσαίος κίνδυνος
Μεσαία	Πολύ Χαμηλός κίνδυνος	Χαμηλός κίνδυνος	Μεσαίος κίνδυνος	Μεσαίος κίνδυνος	Υψηλός κίνδυνος
Μεγάλη	Χαμηλός κίνδυνος	Μεσαίος κίνδυνος	Μεσαίος κίνδυνος	Υψηλός κίνδυνος	Πολύ Υψηλός κίνδυνος
Πολύ Μεγάλη	Χαμηλός κίνδυνος	Μεσαίος κίνδυνος	Υψηλός κίνδυνος	Πολύ Υψηλός κίνδυνος	Πολύ Υψηλός κίνδυνος

Πίνακας 10 - Ποιοτική εκτίμηση του βαθμού κινδύνου

Παρατηρήσεις

- Μια πολύ μικρή πιθανότητα πραγματοποίησης καθιστά τον κίνδυνο από πολύ χαμηλό έως χαμηλό ανεξάρτητα από το μέγεθος αντικτύπου.
- Ένας αμελητέας σημασίας αντίκτυπος καθιστά τον κίνδυνο από πολύ χαμηλό έως χαμηλό ανεξάρτητα από το μέγεθος πιθανότητας.
- Πολύ υψηλός βαθμός κινδύνου προκύπτει μόνο αν τουλάχιστον ένας από τους δύο όρους του γινομένου είναι η ακραία προς τα επάνω τιμή της αντίστοιχης κλίμακας.

Ιδιαίτερη αναφορά πρέπει να γίνει σχετικά με τις απειλές που έχουν πολύ μικρή πιθανότητα πραγματοποίησης αλλά ταυτόχρονα καταστροφικές συνέπειες για τον οργανισμό σε πολλαπλά επίπεδα. Παραδείγματα τέτοιων απειλών αποτελούν μια οικονομική κρίση, μια πανδημία, ένας μεγάλης έκτασης σεισμός και φυσικές καταστροφές εκτός των ορίων που μπορούν να προβλεφθούν και να θεωρούνται λογικού μεγέθους. Τα συμβάντα αυτά αντιμετωπίζονται ξεχωριστά από τους

υπόλοιπους κινδύνους και σχετίζονται άμεσα με τη συνέχεια του οργανισμού (Business continuity). Η συγκεκριμένη μεθοδολογία δε διαθέτει μέτρα αξιολόγησης των παραγόμενων, από αυτές τις απειλές, κινδύνων.

Στη συνέχεια γίνεται η αντιστοίχιση της κλίμακας 1 – 75 με το σχήμα Πολύ Χαμηλός – Χαμηλός – Μεσαίος – Υψηλός – Πολύ Υψηλός σύμφωνα με τον Πίνακα 10 (βλ. Πίνακας 11). Η κλίμακα 1 – 75 βοηθά σε μια αρκετά διακριτή κατάταξη των κινδύνων και διευκολύνει την τοποθέτηση προτεραιοτήτων στο μετέπειτα πλάνο αντιμετώπισης.

Αντίκτυπος \ Πιθανότητα	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25
6	6	12	18	24	30
7	7	14	21	28	35
8	8	16	24	32	40
9	9	18	27	36	45
10	10	20	30	40	50
11	11	22	33	44	55
12	12	24	36	48	60
13	13	26	39	52	65
14	14	28	42	56	70
15	15	30	45	60	75

Πίνακας 11 - Ποσοτική εκτίμηση του βαθμού κινδύνου

Παρατηρείται ότι κάποιες αριθμητικές τιμές της κλίμακας αντιστοιχίζονται σε περισσότερους από έναν ποιοτικούς όρους του Πίνακα 10. Για παράδειγμα μπορεί κάποιος κίνδυνος να βαθμολογηθεί με τέσσερα (4) και να είναι είναι σύμφωνα με τον Πίνακα 11 Χαμηλός (ανοιχτό πράσινο χρώμα) ή Πολύ Χαμηλός (σκούρο πράσινο

χρώμα). Επίσης παρατηρείται, ότι αριθμητική τιμή που αντιστοιχίζεται σε χαμηλό ποιοτικό όρο μπορεί να είναι μεγαλύτερη από τιμή που αντιστοιχίζεται σε ψηλότερο ποιοτικό όρο. Για παράδειγμα υπάρχει Υψηλός βαθμός κινδύνου με αριθμητική τιμή 35 και Μεσαίος βαθμός κινδύνου με αριθμητική τιμή 36.

Για τους παραπάνω λόγους πραγματοποείται τροποποίηση του Πίνακα 11, με κριτήριο τη διεύρυνση των ορίων κάθε φορά του υψηλότερου βαθμού κινδύνου (βλ. Πίνακας 12). Αυτό σημαίνει πως τιμές του Πίνακα 11 που αντιστοιχίζονται σε Πολύ Χαμηλούς κινδύνους (4 έως 9) μεταφέρονται στους Χαμηλούς, τιμές των Χαμηλών κινδύνων μεταφέρονται στους Μεσαίους (16, 18) και τιμές των Μεσαίων κινδύνων μεταφέρονται στου Υψηλούς (36). Οι πολύ υψηλοί κίνδυνοι δεν επηρεάζονται.

Πιθανότητα

Αντίκτυπος	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25
6	6	12	18	24	30
7	7	14	21	28	35
8	8	16	24	32	40
9	9	18	27	36	45
10	10	20	30	40	50
11	11	22	33	44	55
12	12	24	36	48	60
13	13	26	39	52	65
14	14	28	42	56	70
15	15	30	45	60	75

Πίνακας 12 - Τροποποιημένη ποσοτική εκτίμηση του βαθμού κινδύνου

Με αυτόν τον τρόπο καταλήγουμε στα ακόλουθα αποτελέσματα:

- Ο υψηλότερος κίνδυνος βαθμολογείται με την τιμή 75 και ο χαμηλότερος όλων με την τιμή 1.
- Ένας κίνδυνος που λαμβάνει αριθμητική τιμή 1 έως 3 από τον τύπο υπολογισμού του κινδύνου αντιστοιχίζεται ως Πολύ Χαμηλός.
- Ένας κίνδυνος που λαμβάνει αριθμητική τιμή 4 έως 15 από τον τύπο υπολογισμού του κινδύνου αντιστοιχίζεται ως Πολύ Χαμηλός.
- Ένας κίνδυνος που λαμβάνει αριθμητική τιμή 16 έως 33 από τον τύπο υπολογισμού του κινδύνου αντιστοιχίζεται ως Μεσαίος.
- Ένας κίνδυνος που λαμβάνει αριθμητική τιμή 35 έως 48 από τον τύπο υπολογισμού του κινδύνου αντιστοιχίζεται ως Υψηλός.
- Ένας κίνδυνος που λαμβάνει αριθμητική τιμή 50 έως 75 από τον τύπο υπολογισμού του κινδύνου αντιστοιχίζεται ως Πολύ Υψηλός.
- Οι αριθμητικές τιμές που δεν αναφέρονται στα παραπάνω δεν μπορούν να προκύψουν από την πράξη γινομένου του τύπου.

Καθορισμός των κριτηρίων αποδοχής κινδύνου (Criteria of risk acceptance)

Η παρούσα μέθοδος αξιολόγησης έπειτα από την εκτίμηση του βαθμού κάθε κινδύνου τους κατατάσσει σε αποδεκτούς και μη αποδεκτούς. Πιο συγκεκριμένα:

1. Κάθε Χαμηλός ή Πολύ χαμηλός κίνδυνος είναι αποδεκτός από τον οργανισμό και δεν απαιτούνται μέτρα προστασίας του αντίστοιχου πόρου.
2. Μεσαίοι κίνδυνοι έως την αριθμητική τιμή 25 είναι αποδεκτοί από τον οργανισμό και θα επαναξεταστούν σε μελλοντική αξιολόγηση.
3. Μεσαίοι κίνδυνοι με αριθμητική τιμή μεγαλύτερη του 25 είναι μη αποδεκτοί από τον οργανισμό και πρέπει να αντιμετωπιστούν εντός εύλογου χρονικού διαστήματος.
4. Υψηλοί και Πολύ Υψηλοί κίνδυνοι είναι μη αποδεκτοί από τον οργανισμό και πρέπει να αντιμετωπιστούν το συντομότερο δυνατόν.

5.2. Τα πλεονεκτήματα της μεθόδου

Στην παρούσα ενότητα περιγράφονται τα πλεονεκτήματα της συγκεκριμένης μεθοδολογίας αξιολόγησης κινδύνου και οι ωφέλιμες διαφοροποιήσεις της σε σχέση με άλλες μεθοδολογίες. Πιο αναλυτικά:

- ✓ Πρόκειται για μια πολύ απλή και έυχρηστη μεθοδολογία. Η σύνταξη της διαρκεί ένα αρκετά μικρό χρονικό διάστημα και αυτο δίνει τη δυνατότητα στον οργανισμό να την πραγματοποιεί ανά τακτά χρονικά διαστήματα.
- ✓ Συνδυάζει ποιοτικούς και ποσοτικούς όρους, με αποτέλεσμα να δίνει μια ολοκληρωμένη εικόνα γύρω από τους κινδύνους που ανιχνεύονται. Για παράδειγμα έστω ότι ένας Πολύ Υψηλός κίνδυνος αποτιμάται με τιμή 60/75. Η διπλή αυτή περιγραφή του βαθμού προσδίδει μια αρκετά ακριβή όσο και απλή εικόνα του κινδύνου.
- ✓ Μπορεί να εφαρμοστεί σε οποιοδήποτε μικρό ή μεσαίο οργανισμό ή σε αντίστοιχου μεγέθους τμήμα οργανισμού. Δεν έχει χαρακτηριστικά που αποκλείουν οργανισμούς από τη χρήση της. Αντίθετα είναι έτσι διαμορφωμένη ώστε να υλοποιείται σε ποικίλλα περιβάλλοντα.
- ✓ Εξετάζει τον αντίκτυπο του συμβάντος απειλής υπό πέντε διαφορετικούς άξονες δίνοντας με αυτόν τον τρόπο μια πολυδιάστατη ερμηνεία του όρου.
- ✓ Με τη χρήση της επιλογής του πιο υψηλού βαθμού αντικτύπου, ουσιαστικά αποτρέπει την υποτίμηση των λεγόμενων κρυφών κινδύνων. Για παράδειγμα, ένα συμβάν απειλής μπορεί να έχει πολύ χαμηλό αντίκτυπο σε τέσσερις κατηγορίες και έναν πολύ υψηλό. Αθροιστικές μέθοδοι για τον αντίκτυπο ή χρήση του μέσου όρου είναι πολύ πιθανό να κατέτασσαν τον παραγόμενο αντίκτυπο ως χαμηλό, ενώ η πραγματικότητα είναι διαφορετική, μιας και σε ένα συγκεκριμένο τομέα πρόκειται να επιφέρει τεράστιο πλήγμα.
- ✓ Αποτελεί μια ευέλικτη μέθοδο, καθώς δεν υπαγορεύει στον οργανισμό συγκεκριμένους επίσημους τρόπους για το πως θα αναγνωρίσει τα στοιχεία πληροφορίας, τις απειλές και τις ευαλωτότητες. Αντίθετα προτείνει τα αντίστοιχα πεδία και αφήνει τον οργανισμό να επιλέξει τα κριτήρια του.
- ✓ Η γλώσσα και οι όροι που χρησιμοποιούνται είναι στην κατεύθυνση της κατανόησης από όλη την έκταση του οργανισμού. Από τη διοίκηση μέχρι και τους απλούς εργαζομένους.

- ✓ Μπορεί να επεκταθεί καταλλήλως ώστε να είναι συμβατή με το πρότυπο ISO/IEC 27001.
- ✓ Η απλή μορφή της δημιουργεί ένα τεράστιο πεδίο βελτιώσεων, τροποποιήσεων και επεκτάσεων της.

5.3. Εφαρμογή του εργαλείου σε υποθετικά σενάρια

Στην ενότητα αυτή πραγματοποιείται η εφαρμογή της προτεινόμενης μεθοδολογίας αξιολόγησης κινδύνου σε έναν υποθετικό οργανισμό για πέντε διαφορετικά σενάρια, που στοχεύει στην κατανόηση του τρόπου λειτουργίας της μεθόδου και στην ανάδειξη των πλεονεκτημάτων που αναφέρθηκαν. Ο οργανισμός που έχει επιλεχθεί είναι ένα κατάστημα τραπέζης που απασχολεί περί τους 30 υπαλλήλους και πραγματοποιεί καθημερινά διαδικασίες μέσω υπολογιστικών συστημάτων. Η επιλογή αυτή γίνεται λόγω του μεγάλου όγκου πληροφοριών και στοιχείων πληροφορίας που διαθέτει και επεξεργάζεται ένας τέτοιος οργανισμός.

Σενάριο 1: Καταστροφή εκτυπωτή/σκάνερ

Η αξιολόγηση αναγνωρίζει ως στοιχείο πληροφορίας του οργανισμού, στην κατηγορία του υλικού, τον εκτυπωτή/σκάνερ. Εντός της τράπεζας υπάρχουν τέσσερα, σχετικά σύγχρονα, τέτοια στοιχεία. Στη συνέχεια, η μεθοδολογία αναζητά απειλές και ευαλωτότητες σχετικά με αυτό και αναγνωρίζει ως απειλή την καταστροφή του εκτυπωτή που μπορεί να προέλθει από κακή κατασκευή του (ξαφνικό πρόβλημα κατά τη χρήση του και αδυναμία να πραγματοποιήσει τη ζητούμενη εργασία) ή την απροσεξία υπαλλήλων και πελατών (πτώση υγρού στο μηχάνημα ή τα καλώδια). Τον προηγούμενο χρόνο δεν υπήρξε κάποιο τέτοιο συμβάν πραγματοποίησης της συγκεκριμένης απειλής για το λόγο αυτό η αξιολόγηση αποτιμά την πιθανότητα της απειλής με την αριθμητική τιμή 2 (Μικρή πιθανότητα). Ο αντίκτυπος αυτού του συμβάντος στην παροχή υπηρεσιών αποτιμάται με την τιμή 2, καθώς υπάρχουν ακόμα τρεις διαθέσιμοι εκτυπωτές εντός του οργανισμού, που αρκούν για τις λειτουργίες του οργανισμού. Ο αντίκτυπος στο σχεδιασμό αποτιμάται εξίσου με την τιμή 2 για τον ίδιο λόγο. Ο αντίκτυπος σε συμμόρφωση με το νόμο και φήμη του οργανισμού είναι μηδενικός γι αυτό αποτιμάται με τη χαμηλότερη τιμή. Ο αντίκτυπος σε οικονομικές απώλειες αποτιμάται με την τιμή 3, διότι αφενός δεν εμποδίζει

κάποιον οικονομικό στόχο, και αφετέρου η αποκατάσταση του μηχανήματος είναι μικρού κόστους σε σχέση με το μέγεθος του οργανισμού. Συνεπώς, επιλέγεται ως αντίκτυπος ο μεγαλύτερος από τους παραπάνω, δηλαδή ο αντίκτυπος σε οικονομικές απώλειες, με την τιμή 3 (Αμελητέας σημασίας). Ο υπολογισμός του κινδύνου προκύπτει από το γινόμενο 2 x 3 (Πιθανότητα x Αντίκτυπος). Τελικά, ο βαθμός κινδύνου είναι η τιμή 6 (Χαμηλός) και κατατάσσεται σύμφωνα με τα κριτήρια της μεθόδου ως αποδεκτός.

Σενάριο 2: Καταστροφή του φυσικού χώρου του ταμείου από φωτιά

Στη συγκεκριμένη περίπτωση αναγνωρίζεται ως στοιχείο πληροφορίας ο χώρος του ταμείου στην κατηγορία των φυσικών εγκαταστάσεων. Μια απειλή προς αυτό το στοιχείο αποτελεί η εκδήλωση φωτιάς. Το συγκεκριμένο κατάστημα βρίσκεται στο κέντρο της πόλης, όπου συχνά πραγματοποιούνται διαδηλώσεις και επεισόδια και είναι γνωστό πως τα τραπεζικά καταστήματα αποτελούν συχνό στόχο επίθεσης σε τέτοιες καταστάσεις. Πυρκαγιά μπορεί να προκληθεί και ακούσια από κάποιο ατύχημα. Για το λόγο αυτό, ο οργανισμός έχει εγκαταστήσει ένα καλό σύστημα πυρασφάλειας. Στο συγκεκριμένο κατάστημα δεν έχει πραγματοποιηθεί ποτέ τέτοιο συμβάν, ωστόσο τα τελευταία χρόνια έχουν παρατηρηθεί παρόμοια περιστατικά στην περιοχή. Η αξιολόγηση αποτιμά την πιθανότητα του συμβάντος με την τιμή 2 (Μικρή). Ο αντίκτυπος του συμβάντος απειλής στην παροχή υπηρεσιών αποτιμάται με την τιμή 10, διότι έως ότου αποκατασταθεί η ζημιά, δυσχαιρένεται η εξυπηρέτηση των πελατών. Ο αντίκτυπος της απειλής στο σχεδιασμό αποτιμάται με 6, στην περίπτωση που ο υπόλοιπος οργανισμός λειτουργεί κατά τη διάρκεια αποκατάστασης της βλάβης. Ο αντίκτυπος στη φήμη του οργανισμού και στη συμμόρφωση με το νόμο αποτιμάται με 1, καθώς η απειλή δεν επηρέαζει αυτές τις κατηγορίες. Ο αντίκτυπος σε οικονομικές απώλειες αποτιμάται με 2, αφού σε σχέση με το μέγεθος του ευρύτερου οργανισμού της τράπεζας η ζημιά είναι ελάχιστη. Συνεπώς, ως αντίκτυπος για τον υπολογισμό του κινδύνου επιλέγεται ο αντίκτυπος στην παροχή υπηρεσιών με τιμή 10 (Μεγάλης σημασίας). Από τον τύπο υπολογισμού του κινδύνου (2 x 10) προκύπτει ο βαθμός του κινδύνου ίσος με 20 (Μεσαίος κίνδυνος). Σύμφωνα με τα κριτήρια αποδοχής, ο κίνδυνος κατατάσσεται ως αποδεκτός.

Σενάριο 3: Επίθεση από χάκερς σε υπολογιστή υπαλλήλου

Η μεθοδολογία αναγνωρίζει ως στοιχεία πληροφορίας του οργανισμού τους υπολογιστές των υπαλλήλων. Μία από τις βασικές απειλές σε αυτά είναι η κλοπή δεδομένων και πληροφοριών από τα αρχεία του υπολογιστή ύστερα από επίθεση από χάκερς. Κάποιες από αυτές τις πληροφορίες ίσως αφορούν ευαίσθητα προσωπικά στοιχεία πελατών. Ο συγκεκριμένος οργανισμός, διαθέτει αρκετά μη ενημερωμένα λογισμικά και ένα παλαιό, μη επικαιροποιημένο firewall. Ύστερα από παλαιότερη έρευνα, είχε παρατηρηθεί, επίσης, χρήση εύκολων και μη πολυσύνθετων κωδικών από αρκετούς εργαζομένους στις διάφορες τραπεζικές εφαρμογές. Τα παραπάνω αποτελούν πολύ σημαντικές ευαλωτότητες σχετικά με το συγκεκριμένο στοιχείο και τη συγκεκριμένη απειλή. Για το λόγο αυτό, η μεθοδολογία αξιολογεί την πιθανότητα του συμβάντος ως Μεγάλη με αριθμητική τιμή 4. Ο αντίκτυπος του συμβάντος στην παροχή υπηρεσιών, στο σχεδιασμό και οικονομικές απώλειες αποτιμάται με τις τιμές 2, 3 και 1 αντίστοιχα καθώς δεν επιφέρεται κάποιο ιδιαίτερο πλήγμα σε αυτούς τους τομείς. Ωστόσο, ο αντίκτυπος στη φήμη του οργανισμού και στη συμμόρφωση με το νόμο είναι πολύ μεγάλος. Σχετικά με τη φήμη του οργανισμού, η διαρροή προσωπικών πληροφοριών πελατών αποφέρει σοβαρό πλήγμα. Το ίδιο συμβαίνει και στη συμμόρφωση του οργανισμού με τους νόμους προστασίας προσωπικών δεδομένων. Οι δύο αντίκτυποι βαθμολογούνται με 13 και 14 αντίστοιχα. Τελικά, επιλέγεται ο αντίκτυπος στη συμμόρφωση με το νόμο ως παράγοντας υπολογισμού του βαθμού κινδύνου. Ο βαθμός κινδύνου αξιολογείται ύστερα από το γινόμενο υπολογισμού (4 x 14) ως Πολύ Υψηλός με αριθμητική τιμή 56. Η τιμή αυτή τον κατατάσσει ως μη αποδεκτό κίνδυνο σύμφωνα με τα κριτήρια αποδοχής.

Σενάριο 4: Διακοπή σύνδεσης με το κεντρικό δίκτυο

Κάθε υποκατάστημα επικοινωνεί με το κεντρικό δίκτυο της τράπεζας για να πραγματοποιεί τις καθημερινές του λειτουργίες. Το δίκτυο του οργανισμού, συνεπώς, αποτελεί στοιχείο πληροφορίας και αναγνωρίζεται από τη μεθοδολογία αξιολόγησης. Στην περίπτωση του οργανισμού που εξετάζεται, η σύνδεση με το κεντρικό δίκτυο πραγματοποιείται μέσω οπτικών ινών και δεν υπάρχει δευτερογενής σύνδεση (οπτικές ίνες μονής όδευσης). Ενδεχόμενη βλάβη στο δίκτυο οπτικών ινών διακόπτει τη σύνδεση και ο οργανισμός ουσιαστικά δε δύναται να πραγματοποιήσει καμία λειτουργία. Αυτό αποτελεί ένα αρκετά σημαντικό συμβάν απειλής. Η αξιολόγηση

χαρακτηρίζει την πιθανότητα να πραγματοποιηθεί ως Μεσαία με αριθμητική τιμή 3. Ο αντίκτυπος του συμβάντος είναι σχετικά μικρός σε νομικές παραβάσεις και οικονομικές απώλειες καθώς δεν αλλοιώνει κάποια συμφωνία με νομικά πλαίσια και το κόστος αποκατάστασης του δικτύου επιβαρύνει τον πάροχο. Σε αυτές τις δύο κατηγορίες ο αντίκτυπος βαθμολογείται με 1 και 3 αντίστοιχα. Ωστόσο, το γεγονός πως ο οργανισμός υπολειτουργεί ή δε λειτουργεί καθόλου μέχρι την αποκατάσταση της βλάβης, αποφέρει πολύ σοβαρό πλήγμα στη φήμη, το σχεδιασμό και την παροχή υπηρεσιών του. Ο αντίκτυπος σε αυτές τις περιπτώσεις αξιολογείται με τις τιμές 11, 14 και 15 αντίστοιχα. Τελικά για τον υπολογισμό του βαθμού κινδύνου χρησιμοποείται ως παράγοντας ο πιο σοβαρός αντίκτυπος στην παροχή υπηρεσιών με τιμή 15 (Ύψιστης σημασίας αντίκτυπος). Ύστερα από την πράξη του τύπου υπολογισμού του βαθμού κινδύνου (3 x 15) προκύπτει η τιμή 45 (Υψηλός κίνδυνος). Τα κριτήρια αποδοχής κινδύνων κατατάσσουν τον κίνδυνο ως μη αποδεκτό.

Σενάριο 5: Παύση εργασίας με απαραίτητο για τον οργανισμό εργαζόμενο

Στο συγκεκριμένο σενάριο, το κατάστημα της τράπεζας απασχολεί μόνο ένα άτομο στο κομμάτι των επενδύσεων σε ομόλογα. Η μεθοδολογία αξιολόγησης αναγνωρίζει το άτομο αυτό ως στοιχείο πληροφορίας μέσα στον οργανισμό, στην κατηγορία του προσωπικού. Ένα συμβάν απειλής σχετικά με αυτό το στοιχείο, είναι η παύση εργασίας του ατόμου. Η παύση αυτή μπορεί να προέλθει από λόγους υγείας ή άλλους προσωπικούς λόγους και να διαρκέσει λίγες μέρες ή να είναι μόνιμη. Σε αυτή την περίπτωση δεν υπάρχει άλλος εργαζόμενος στον οργανισμό με γνώσεις στο συγκεκριμένο αντικείμενο. Η πιθανότητα πραγματοποίησης της απειλής στον καιρό της πανδημίας αποτιμάται ως μεσαία με αριθμητική τιμή 3. Ο αντίκτυπος του συμβάντος στη φήμη, τη συμμόρφωση με το νόμο και τις οικονομικές απώλειες είναι χαμηλός διότι δεν επηρεάζει σε μεγάλο βαθμό τους συγκεκριμένους τομείς. Για το λόγο αυτό αποτιμάται 4, 1 και 2 αντίστοιχα. Ο αντίκτυπος στο σχεδιασμό μπορεί να είναι μεσαίου βαθμού στην περίπτωση που ορισμένοι βραχυπρόθεσμοι στόχοι του οργανισμού αφορούν την επίτευξη συμφωνιών για την επένδυση σε ομόλογα, γι αυτό και αποτιμάται με την τιμή 7. Ωστόσο, ο αντίκτυπος στην παροχή υπηρεσιών είναι μεγάλος, στην περίπτωση που δε μπορεί να εξυπηρετηθεί κάποιος πελάτης που

επιθυμεί να επενδύσει σε ομόλογα για το διάστημα που δεν εργάζεται ο συγκεκριμένος υπάλληλος. Για το λόγο αυτό βαθμολογείται με 13 (Ύψιστης σημασίας) και αποτελεί τον παράγοντα υπολογισμού του βαθμού κινδύνου. Το γινόμενο του τύπου υπολογισμού (3 x 13) αξιολογεί τον κίνδυνο ως Υψηλό με αριθμητική τιμή 39. Ο συγκεκριμένος κίνδυνος είναι μη αποδεκτός για τον οργανισμό σύμφωνα με τα κριτήρια αποδοχής της μεθοδολογίας.

Σενάριο 6: Λανθασμένη χρήση οδηγιών σχετικά με τον αριθμό ατόμων μέσα στο κατάστημα

Το συγκεκριμένο σενάριο εξετάζει ως στοιχείο πληροφορίας του οργανισμού τις οδηγίες (κατηγορία οργανωτικής δομής) που υπάρχουν στον καιρό τις πανδημίας σε σχέση με τον αριθμό ατόμων που επιτρέπονται να βρίσκονται ταυτόχρονα εντός του καταστήματος. Ο διευθυντής του συγκεκριμένου οργανισμού δεν έχει διαβάσει ενδελεχώς τις οδηγίες του υπουργείου υγείας και για το λόγο αυτό έχει δώσει στον υπεύθυνο υπάλληλο μη σαφείς εντολές σχετικά με το θέμα. Πολύ συχνό φαινόμενο είναι επίσης κατά την είσοδο να εισέρχονται δύο-δύο πελάτες για να αποφύγουν μεγαλύτερη αναμονή, ενώ ο υπάλληλος πολλές φορές ξεχνά να επαληθεύει τον αποδεκτό αριθμό των ατόμων εντός του οργανισμού. Η απειλή να μη χρησιμοποιηθούν σωστά οι οδηγίες πιθανολογείται ως Μεγάλη με αριθμητική τιμή 4. Ο αντίκτυπος της είναι ελάχιστος στο σχεδιασμό και στην παροχή υπηρεσιών γιαυτό και βαθμολογείται με τις τιμές 1 και 3 αντίστοιχα. Ωστόσο, σε νομικό επίπεδο ο οργανισμός παραβιάζει τους κανόνες που θα του επιφέρουν και το ανάλογο οικονομικό κόστος σε πρόστιμο. Ακόμα, ο οργανισμός δυσφημείται, καθώς συζητείται από πολίτες πως τα προβλεπόμενα μέτρα κατά της πανδημίας δεν τηρούνται. Συνεπώς ο αντίκτυπος σε νομικές παραβάσεις, οικονομικές απώλειες και φήμη του οργανισμού βαθμολογείται με 12, 10 και 8 αντίστοιχα. Με βάση τον αντίκτυπο σε νομικές παραβάσεις, προκύπτει από τον τύπο υπολογισμό του κινδύνου (4 x 12) βαθμός ίσος με 48 και κατατάσσεται ως Υψηλός. Ο συγκεκριμένος κίνδυνος είναι μη αποδεκτός από τον οργανισμό.

Σενάριο 7: Κλοπή δεδομένων από το cloud

Οι εργαζόμενοι χρησιμοποιούν συγκεκριμένη υπηρεσία cloud, συνεπώς το τελευταίο αναγνωρίζεται από την αξιολόγηση ως στοιχείο πληροφορίας του οργανισμού. Οι πληροφορίες που αποθηκεύουν οι χρήστες σε υπηρεσίες cloud αυξάνονται ραγδαία, το ίδιο και οι κακόβουλες επιθέσεις σε αυτές. Ένα σημαντικό μέτρο προστασίας από αυτές τις επιθέσεις είναι η κρυπτογράφηση των δεδομένων μέσω συγκεκριμένων εφαρμογών, καθώς ενδεχομένη κακόβουλη επίθεση θα μπορέσει να υποκλέψει τα δεδομένα αλλά όχι να τα χρησιμοποιήσει. Στον οργανισμό που εξετάζεται, δεν πραγματοποιείται η κρυπτογράφηση των δεδομένων πριν την αποθήκευση στο cloud. Επίσης όπως αναφέρθηκε προηγουμένως, οι κωδικοί που χρησιμοποιούν οι εργαζόμενοι είναι αρκετά αδύναμοι και ευάλωτοι σε επιθέσεις. Για τους παραπάνω λόγους, η πιθανότητα υποκλοπής απόρρητων πληροφοριών χαρακτηρίζεται από την αξιολόγηση ως Μεγάλη. Ο αντίκτυπος, όπως ακριβώς και στο σενάριο 3, σε παροχή υπηρεσιών, σχεδιασμό, οικονομικές απώλειες, φήμη και νομικές παραβάσεις είναι 2, 3, 1, 13, 14 αντίστοιχα. Ως αποτέλεσμα, ο κίνδυνος βαθμολογείται με 56 (14 x 4) και χαρακτηρίζεται Πολύ Υψηλός. Σύμφωνα με τα κριτήρια αποδοχής κινδύνων της μεθόδου, ο συγκεκριμένος κίνδυνος δεν είναι αποδεκτός.

Σενάριο 8: Κακόβουλα λογισμικά και ιοί σε υπολογιστές εργαζομένων.

Τα κακόβουλο λογισμικά βρίσκονται ευρέως στο διαδίκτυο και παραμονεύουν να μολύνουν τον υπολογιστή κάποιου χρήστη, προκαλώντας μερική αλλοίωση, τροποποίηση ή διαγραφή δεδομένων, αντιγράφων και άλλων πληροφοριών. Ο πλέον συνήθης τρόπος διάδοσης του ιού είναι μέσω του ηλεκτρονικού ταχυδρομείου (e-mail) και συνδέσμων (links) από πλατφόρμες μέσων κοινωνικής δικτύωσης. Στον οργανισμό, δεν υπάρχει κάποια επίσημη οδηγία από τη διοίκηση για τον τρόπο λειτουργίας των επαγγελματικών υπολογιστών των εργαζομένων, γι αυτό και οι τελευταίοι τους χρησιμοποιούν και σε ώρες διαλείμματος για λειτουργίες εκτός της εργασίας τους (π.χ. προσωπικό e-mail, Facebook, Twitter). Τα λογισμικά antivirus του οργανισμού δεν έχουν επικαιροποιηθεί σχετικά πρόσφατα. Η πιθανότητα να μολυνθεί ένας επαγγελματικός υπολογιστής χαρακτηρίζεται ως Μεσαία (τιμή 3), διότι οι εργαζόμενοι είναι ως ένα βαθμό

τεχνολογικά εκπαιδευμένοι να αναγνωρίζουν τις κοινές πιθανές κακόβουλες ενέργειες αυτής της μορφής (μόλυνση από ιό). Ο αντίκτυπος από την αλλοίωση πληροφοριών εντός του υπολογιστή είναι σημαντικός για το σχεδιασμό και την παροχή υπηρεσιών, καθώς εμποδίζει την εργασία του ατόμου και βαθμολογείται με 9 και 8 αντίστοιχα. Η απειλή του κακόβουλου λογισμικού δεν επηρεάζει σε μεγάλο βαθμό σε οικονομικούς όρους τον οργανισμό, τη φήμη του και τη συμμόρφωση του με το νόμο. Οι προηγούμενοι αντίκτυποι βαθμολογούνται με 2. Συνεπώς, ο παραγόμενος κίνδυνος βαθμολογείται με 27 (9 x 3) και χαρακτηρίζεται Μεσαίος αλλά μη αποδεκτός σύμφωνα με τα κριτήρια της μεθόδου.

Σενάριο 9: Κλοπή προσωπικού φορητού υπολογιστή (laptop)

Ο οργανισμός παρέχει σε κάθε εργαζόμενο έναν προσωπικό υπολογιστή για τις ανάγκες εργασίας (αν είναι αναγκαίο) εκτός του περιβάλλοντος του οργανισμού, για παράδειγμα το σαββατοκύριακο ή σε περίοδο διακοπων. Ο φορητός υπολογιστής αποτελεί στοιχείο πληροφορίας του οργανισμού και προφανώς περιέχει πληθώρα πληροφοριών. Ενδεχόμενη κλοπή του από φυσικό πρόσωπο σημαίνει και κλοπή αυτών των πληροφοριών. Ο οργανισμός δε διαθέτει συγκεκριμένες οδηγίες για την ατομική προστασία του κάθε laptop, συνεπώς, η ασφάλεια του κρίνεται από τις ενέργειες του κάθε εργαζομένου ξεχωριστά. Ακόμα, δεν υπάρχει κάποια πολιτική με το τι πληροφορίες επιτρέπονται να αποθηκεύονται σε αυτό. Η πιθανότητα κλοπής ενός laptop του οργανισμού χαρακτηρίζεται Μικρή με αριθμητική τιμή 2. Ο αντίκτυπος αυτού του συμβάντος από την ενδεχόμενη παραβίαση του υπολογιστή θα επηρεάσει σε μικρό βαθμό τον οργανισμό σε επίπεδο παροχής υπηρεσιών, σχεδιασμό και οικονομικές απώλειες γι αυτό και αποτιμάται με την αριθμητική τιμή 3, 5 και 3 αντίστοιχα. Ωστόσο, όπως αναφέρθηκε και στο Σενάριο 3, οι πληροφορίες που μπορούν να διαρρεύσουν και να αφορούν ακόμα και ευαίσθητα προσωπικά στοιχεία πελατών θα επιφέρουν μεγάλο πλήγμα στη φήμη του οργανισμού και στη συμμόρφωση του με το νόμο. Οι συγκεκριμένοι αντίκτυποι βαθμολογούνται με 11 και 12. Η μικρή διαφοροποίηση στα μεγέθη των δύο τελευταίων αντικτύπων με το Σενάριο 3 προκύπτει από το γεγονός πως οι εργαζόμενοι του οργανισμού αποθηκεύουν απόρρητες πληροφορίες κατά κύριο λόγο στους υπολογιστές εντός του

οργανισμού. Συνεπώς, ο βαθμός κινδύνου (12 x 2) χαρακτηρίζεται ως Μεσαίος με αριθμητική τιμή 24. Η τιμή αυτή τον κατατάσσει στους αποδεκτούς κινδύνους.

Σενάριο 10: Εξαπάτηση πελάτη μέσω του ATM

Ο οργανισμός διαθέτει,όπως όλα σχεδόν τα υποκαταστήματα τραπεζών, ATM για την εξυπηρέτηση διαδικασιών ανάληψης ή κατάθεσης μετρητών και άλλων ενεργειών από τους πελάτες. Το ATM προφανώς αποτελεί στοιχείο πληροφορίας του οργανισμού και μάλιστα κρίσιμης σημασίας. Τους τελευταίους μήνες έχουν καταγραφεί στην πόλη αρκετές περιπτώσεις εξαπάτησης πελατών μέσω ATM με τη μορφή card skimming (υποκλοπή στοιχείων της κάρτας από τη μαγνητική επιφάνεια μέσω ειδικής συσκευής), card trapping (εκούσιο μπλοκάρισμα κάρτας μέσω μηχανισμού και ύστερη εξαπάτηση του πελάτη) και cash trapping (εκούσιο μπλοκάρισμα χρημάτων μέσω μηχανισμού και κλοπή τους ύστερα από τη φυγή του ανυποψίαστου πελάτη). Ο συγκεκριμένος οργανισμός διαθέτει εξωτερικές κάμερες ασφαλείας αλλά όχι ανθρώπινη παρουσία για την προστασία του ATM ούτε τις νυχτερινές ώρες. Η αξιολόγηση βαθμολογεί την πιθανότητα πραγματοποίησης ενός από τα παραπάνω συμβάντα με την τιμή 3 (Μεσαία πιθανότητα). Ο αντίκτυπος της απειλής στο σχεδιασμό, σε οικονομικές απώλειες και σε νομικές παραβάσεις είναι αμελητέας σημασίας και συγκεκριμένα 1, 3 και 1 αντίστοιχα. Ωστόσο, αν κάποιος πελάτης εξαπατηθεί και χάσει κάποιο χρηματικό ποσό με αυτόν τον τρόπο είναι πιθανό να θα θεωρήσει υπεύθυνη για το κακό γεγονός την τράπεζα. Η φήμη του οργανισμού θα πληγεί σε ένα βαθμό (Αντίκτυπος ίσος με 8). Επίσης, αυτή η απειλή ασφαλώς και εμποδίζει τις υπηρεσίες του οργανισμού (Αντίκτυπος ίσος με 10). Συνολικά ο βαθμός κινδύνου προκύπτει από το γινόμενο της πιθανότητας με τον αντίκτυπο στην παροχή υπηρεσιών (3 x 10) και χαρακτηρίζεται ως Μεσαίος με αριθμητική τιμή 30. Ο συγκεκριμένος κίνδυνος δεν είναι αποδεκτός από τον οργανισμό.

Στη συνέχεια παρουσιάζονται τα παραπάνω σενάρια συνοπτικά (βλ. Πίνακας 13).

Asset	Threat	Vulnerability	Likelihood	Category of Max Impact	Max Impact	Risk grade	Risk Acceptance
Σταθερός υπολογιστής/Desktop	Κλοπή πληροφοριών από χάκερς	Αδύναμα passwords Απαρχαιωμένα λογισμικά Μη επικαιροποιημένο firewall	4	Συμμόρφωση με το νόμο	14	56	Μη αποδεκτός
	Αλλοίωση πληροφοριών από κακόβουλα λογισμικά και ιούς	Επίσκεψη ηλεκτρονικού ταχυδρομείου και μέσων κοινωνικής δικτύωσης από τους εργαζόμενος Μη επίκαιρα antivirus	3	Σχεδιασμός	9	27	Μη αποδεκτός
Λογαριασμοί σε υπηρεσίες cloud	Κλοπή δεδομένων	Μη κρυπτογράφηση Αδύναμα passwords	4	Συμμόρφωση με το νόμο	14	56	Μη αποδεκτός
Φορητός υπολογιστής/laptop	Κλοπή υπολογιστή	Μη ύπαρξη οδηγιών από τον οργανισμό Μη ύπαρξη πολιτικής σχετικής με τις πληροφορίες που μπορεί να αποθηκεύει στο laptop	2	Συμμόρφωση με το νόμο	12	24	Αποδεκτός
Οπτικές ίνες σύνδεσης με το κεντρικό δίκτυο	Διακοπή σύνδεσης	Οπτικές ίνες μονής όδευσης	3	Παροχή υπηρεσιών	15	45	Μη αποδεκτός

Πίνακας 13 – Παρουσίαση αποτελεσμάτων αξιολόγησης κινδύνου

Asset	Threat	Vulnerability	Likelihood	Category of Max Impact	Max Impact	Risk grade	Risk Acceptance
ATM	Εξαπάτηση πελατών	Μη ύπαρξη φυσικής προστασίας του μηχανήματος	3	Παροχή υπηρεσιών	10	30	Μη αποδεκτός
Οδηγίες περιορισμού ατόμων λόγω της πανδημίας	Παραβίαση των σχετικών νόμων	Μη σαφείς εντολές από τη διοίκηση Αδυναμία αποτροπής εισόδου σε δύο πελάτες αντί ενός Αδιαφορία ή εφησυχασμός του αρμόδιου εργαζομένου	4	Συμμόρφωση με το νόμο	12	48	Μη αποδεκτός
Ειδικός στις επενδύσεις σε ομόλογα	Αδυναμία εξυπηρέτησης σε ενδεχόμενη απουσία του	Μη ύπαρξη δεύτερου ατόμου στον οργανισμό σχετικού με το αντικείμενο	3	Παροχή υπηρεσιών	13	39	Μη αποδεκτός
Εκτυπωτής/Σκάνερ	Καταστροφή μηχανήματος	Απροσεξία εργαζόμενων Κατασκευαστικό λάθος	2	Οικονομικές απώλειες	3	6	Αποδεκτός
Φυσικός χώρος του ταμείου	Καταστροφή του χώρου από φωτιά	Απροσεξία και ατύχημα από εργαζόμενο Τοποθεσία του οργανισμού	2	Παροχή υπηρεσιών	10	20	Αποδεκτός

Πίνακας 13 συνέχεια – Παρουσίαση αποτελεσμάτων αξιολόγησης κινδύνου

5.4. Προτάσεις για το μέλλον

Όπως αναφέρθηκε ήδη στα πλεονεκτήματα της προτεινόμενης μεθοδολογίας, η απλή μορφή της δημιουργεί ένα τεράστιο πεδίο βελτιώσεων και επεκτάσεων της. Αρχικά, είναι απόλυτα επιθυμητή η συμπλήρωση της παρούσας μεθοδολογίας με κριτήριο που θα αξιολογεί τους κινδύνους με πολύ χαμηλή πιθανότητα και πολύ σοβαρό αντίκτυπο (οικονομική κρίση, πανδημία, πολύ ισχυρό φυσικό φαινόμενο), κάτι που όπως αναφέρθηκε δεν πραγματοποιεί ξεχωριστά αυτή η μέθοδος. Ακόμα, έχει τονιστεί και αναδειχθεί ο ρόλος του αντίκτυπου στη συγκεκριμένη μέθοδο αξιολόγησης μέσα από τη διευρεύνηση πέντε διαφορετικών κατηγοριών αντικτύπων και την επιλογή του σπουδαιότερου από αυτούς. Σε αυτό το πλαίσιο προτείνεται διεύρυνση των κατηγοριών σε περισσότερες από πέντε και η επιλογή περισσότερων από έναν αντίκτυπο για τον μετ' έπειτα υπολογισμό του βαθμού κινδύνου. Για παράδειγμα, μπορεί να χρησιμοποιηθεί το άθροισμα των δύο ή τριών σπουδαιότερων αντικτύπων από ένα εύρος οκτώ κατηγοριών (με την ανάλογη τροποποίηση της κλίμακας κινδύνου). Επίσης, προτείνεται μεταβολή της κλίμακας πιθανότητας από το σχήμα 1-2-3-4-5 στο σχήμα 0.1-0.3-0.5-0.7-0.9 που αποτελούν και πραγματικές, πιθανές, μαθηματικές τιμές πιθανοτήτων για την καλύτερη κατανόηση του μεγέθους από το σύνολο του οργανισμού. Τέλος, η αντιστοίχιση των βαθμών κινδύνου σε ποιοτικούς όρους βασίστηκε στον Πίνακα 10, μια υποκειμενική άποψη του ατόμου, που δημιούργησε τη μέθοδο, πάνω στους συνδυασμούς ποιοτικών όρων της πιθανότητας και του αντικτύπου. Ο πίνακας αυτός μπορεί να τροποποιηθεί σύμφωνα με μια πιο αυστηρή ή πιο χαλαρή στρατηγική.

Βιβλιογραφία

(n.d.). The ISO story. Retrieved 29 January, 2020, from iso: https://www.iso.org/the-iso-story.html

Information Security Management System ISO 27001:2005. (2015). Retrieved August 21, 2020, from tuv-nord: http://www.tuv-nord.com/cps/rde/xbcr/tng_in/Product_Information_27001.pdf

Accerboni, F., & Sartor, M. (2019). ISO/IEC 27001. In *Quality Management: Tools, Methods, and Standards* (pp. 245-264).

Al-Dhahri, S., Al-Sarti, M., & Aziz, A. A. (2017). Information Security Management System. *International Journal of Computer Applications, 158*(7).

Alfantookh, A. (2019). An Approach of the Assessment of ISO 27001. *Essential Information Security Controls*.

Aljazzaf, Z., Capretz, M., & Perry, M. (2016). Trust-based Service-Oriented Architecture. *Journal of King Saud University-Computer and Information Sciences, 28*(4).

Ashenden, D. (2008). Information Security management: A human challenge? *Information security technical report*, pp. 195-201.

Asosheh, A., Khodkari, H., & Hajinazari, P. (2013). A Practical Implementation of ISMS. *7th International Conference on e-commerce in developing countries with focus on e-security.*

Beckers, K., Heisel, M., Solhaug, B., & Stolen, K. (2014). ISMS-CORAS: A Structured Method for Establishing an ISO 27001 Compliant Information Security Management System. *Lecture Notes in Computer Science*, 315-344.

Brykczynski, B., & Small, B. (2003). Securing your organization's information assets. *The Journal of Defense Software Engineering*.

Calder, A., & Watkins, G. (2010). *Information Security Risk Management for ISO27001/ISO27002.* IT Governance publishing.

Chandrashekar, A., Kumarhs, S., & Huded, Y. (2015). Advances in information security risk practices. *International Journal of advanced research in data mining and cloud computing, 3*(2).

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management . *Journal of Information Security*, 92-100.

Ghazouani, M., Faris, S., Medromi H., & Sayouti, A. (2014). Information Security Risk Assessment-A Practical Approach with a Mathematical Formulation of Risk. *International Journal of Computer Applications, 103*(8).

Giesler, A. (2019). *What do the ISO 27001 requirements and structure look like? The ISO 27001 & ISO 22301 Blog*. Retrieved June https://advisera.com/27001academy/blog2019/06/03/iso-27001-requirements-and-structure/, 2020, from advisera.

Hayne, C., & Free, C. (2014). Hybridized professional groups and institutional work: COSO and the rise of enterprise risk management. *Accounting, Organizations and Society, 39*(5).

Hong, K., Chi, Y., Chao, L., & Tang, J. (2003). An integrated system theory of information security management. *Information Management & Computer Security*, 243-248.

Humphreys, E. (2011). Information Security Management System Standards. *Datenschutz und Datensicherheit*.

Kiran, K., Reddy, L., & Haritha , N. (2013). A comparative analysis on risk assessment information security models. *International Journal of Computer Applications, 82*(9).

Kosutic, D. (2013). *List of mandatory documents required by ISO 27001 (2013 revision)*. Retrieved April 2, 2020, from advisera: https://advisera.com/27001academy/knowledgebase/list-of-mandatory-documents-required-by-iso-27001-2013-revision/

KPMG/IMPACT. (1994). *Information as an asset: The board agenda.* London: KPMG/IMPACT.

Pinheiro, F., & Ribeiro, W. (2015). Information security and ISO 27001. *Revista de Gestao & Tecnologia*, 20-28.

Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2015). Taxonomy of information security risk assessment (ISRA). *computers & security, 57*, 14-30.

Susanto, H., Almunawar, M., & Tuan, Y. (2011). Information Security Management System Standards: A Comparative Study of the Big Five. *International Journal of Electrical & Computer Science, 11*(5).

Tajammul, M., & Parveen, R. (2017). Comparative Analysis of Big Ten ISMS Standards and their Effect on Cloud Computing. *International Conference on Computing and Communication Technologies for Smart Nations.*

Vasudevan, V., Mangla , A., Ummer, F., Shetty, S., Pakala, S., & Anbalahan, S. (2015). *Application Security in the ISO27001:2013 Environment.* United Kingdom: IT Governance Publishing.

Wallshein, C., & Loerch, A. (2015). Software cost estimating for CMMI Level 5 developers. *The Journal of Systems & Software*, 105.

Wei, Y., Wu, W., & Chu, Y. (2017). Performance evaluation of the recommendation mechanism of information security risk identification. *Neurocomputing, 279*, 48-53.

Yazar, Z. (2002). A qualitative risk analysis and management tool - CRAMM. *As part of the Information Security Reading Room*.

Young, C. (2016). Information Security Threats and Risk. *Information Security Science*, 3-27.

Zwass , V. (2017, December 28). *Information system.* Retrieved August 20, 2020, from Britannica: https://www.britannica.com/topic/information-system