ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΠΜΣ «Τεχνοοικονομική Διοίκηση Ψηφιακών Συστημάτων»

Διπλωματική εργασία

‘ Προσδιορισμός Κινδύνων Έργων Πληροφοριακών Συστημάτων ’

Μαρία Ι. Δημητρακάκη

Επιβλέπων Καθηγήτρια : Φλώρα Μαλαματένιου

Αθήνα, Νοέμβριος 2012

Περίληψη

Αντικείμενο της παρούσας διπλωματικής εργασίας είναι η ανάλυση της μεθοδολογίας Διαχείρισης Κινδύνων για Πληροφοριακά Έργα και η εφαρμογή της μεθοδολογίας αυτής στην υλοποίηση ενός πραγματικού πληροφοριακού συστήματος. Το επιλεχθέν έργο είναι το «*Ολοκληρωμένο Πληροφοριακό Σύστημα του Δήμου Αθηναίων*».

Ειδικότερα, στο πρώτο κεφάλαιο, πραγματοποιείται μια συνοπτική αναφορά στην έννοια των Πληροφοριακών Συστημάτων, στα είδη που υπάρχουν και τα διάφορα χαρακτηριστικά τους, στον σκοπό, στον κύκλο ζωής των Π.Σ και τους παράγοντες που μπορούν να οδηγήσουν σε επιτυχία ή αποτυχία ένα Π.Σ.

Στο δεύτερο κεφάλαιο εισάγεται η έννοια του έργου, ποια είναι τα βασικά χαρακτηριστικά του, οι στόχοι του και ο κύκλος ζωής ενός έργου.

Στο τρίτο κεφάλαιο, αναλύεται η έννοια της διαχείρισης κινδύνων για έργα Πληροφοριακών Συστημάτων. Αρχικά, αναφέρεται τι είναι κίνδυνος, οι διάφοροι τύποι κινδύνων, η δομή και τα χαρακτηριστικά των κινδύνων. Στη συνέχεια, εισάγεται η έννοια της Διαχείρισης των Κινδύνων και αναφέρονται τα βήματα που ακολουθούνται για τη διαδικασία διαχείρισης κινδύνων. Επίσης, αναφέρεται πως ενσωματώνεται η διαδικασία Διαχείρισης Κινδύνων στον Κύκλο Ζωής ενός έργου Πληροφοριακού Συστήματος, και πως πραγματοποιείται η διαδικασία διαχείρισης κινδύνων σε περίπτωση που το έργο ανατεθεί σε εξωτερική ομάδα. Τέλος, παρουσιάζεται το διάγραμμα ροής της μεθοδολογίας διαχείρισης κινδύνων.

Στο τέταρτο κεφάλαιο, αναλύεται η έννοια του εντοπισμού των κινδύνων και τα βήματα από τη μεθοδολογία διαχείρισης κινδύνων που ακολουθούνται. Επίσης, αναφέρονται οι διάφοροι μέθοδοι εντοπισμού των κινδύνων και αναφέρονται τα πλεονεκτήματα και τα μειονεκτήματα των μεθόδων αυτών. Τέλος, αναφέρονται οι πιθανοί κίνδυνοι που μπορεί να επηρεάσουν την υλοποίηση του έργου και αναλύονται οι σημαντικότεροι κίνδυνοι για ένα έργο Π.Σ (Top IT Project Risks).

Στο πέμπτο κεφάλαιο, αναλύεται η έννοια της ανάλυσης των κινδύνων, πραγματοποιείται ο διαχωρισμός της ποιοτικής και της ποσοτικής ανάλυσης κινδύνων και αναφέρονται οι μέθοδοι που χρησιμοποιούνται στην κάθε ανάλυση.

Στο έκτο κεφάλαιο, αναλύεται η έννοια της αντιμετώπισης των κινδύνων, οι διάφοροι μέθοδοι που χρησιμοποιούνται και τα βήματα της μεθοδολογίας αντιμετώπισης των κίνδυνων. Τέλος, παρουσιάζονται οι διάφορες κατηγορίες ελέγχων αντιμετώπισης κινδύνων.

Στο έβδομο κεφάλαιο, αναλύεται η έννοια της παρακολούθησης των κινδύνων και οι βασικές λειτουργίες που χρησιμοποιούνται. Επίσης, αναφέρονται χρήσιμα στοιχεία για την επόπτευση των κινδύνων, οι διάφοροι μέθοδοι για την παρακολούθηση τους και αποτελέσματα που προκύπτουν από την παρακολούθηση αυτή.

Στο όγδοο κεφάλαιο, αναλύεται η μεθοδολογία διαχείρισης κινδύνων για το έργο «Ολοκληρωμένο Πληροφοριακό Σύστημα (ΟΠΣ) Δήμου Αθηναίων». Ουσιαστικά, παρουσιάζεται ο σκοπός και ο στόχος του πληροφοριακού έργου, ο προϋπολογισμός, ο χρόνος υλοποίησής, η εγγύηση καλής λειτουργίας και τα ενδιαφερόμενα μέρη. Επίσης, παρουσιάζονται τα δύο Υποέργα του κυρίως έργου. Πραγματοποιείται εκτεταμένη ανάλυση για το Υποέργο 1 που αφορά την δημιουργία του ΟΠΣ και αναλύονται τα υποσυστήματα του και οι απαιτήσεις του υποέργου. Τέλος, αναλύονται οι πιθανοί κίνδυνοι που το απειλούν, πραγματοποιείται αξιολόγηση της πιθανότητας εμφάνισης και των επιπτώσεων αυτών των κινδύνων και προτείνονται μέθοδοι αντιμετώπισης αυτών ανάλογα με την αξία του μετριασμού τους για την πορεία υλοποίησης του.

Τέλος, στο ένατο κεφάλαιο παρουσιάζονται τα συμπεράσματα και οι προτάσεις της παρούσας διπλωματικής εργασίας.

Ευχαριστίες

Στο σημείο αυτό θα ήθελα να ευχαριστήσω τον καθηγήτριά μου κ. Φ. Μαλαματένιου, που μου έδωσε την ευκαιρία να ασχοληθώ με το συγκεκριμένο θέμα και για την πολύτιμη βοήθειά της καθ' όλη τη διάρκεια εκπόνησης της διπλωματικής εργασίας, αλλά και την οικογένειά μου για τη στήριξη που μου παρείχε όλο αυτό το διάστημα.

Νοέμβριος 2012

Μαρία Ι. Δημητρακάκη

Περιεχόμενα

Κεφάλαιο 1: Πληροφοριακά Συστήματα Επιχειρήσεων

1.1 Εισαγωγή

Πληροφοριακό Σύστημα είναι ένα σύνολο αλληλοσυνδεόμενων μερών που συνεργάζονται μεταξύ τους για τη συλλογή, επεξεργασία, αποθήκευση και διάχυση πληροφοριών, με σκοπό την υποστήριξη της λήψης αποφάσεων, του συντονισμού, του ελέγχου και της ανάλυσης δεδομένων μέσα σε μια επιχείρηση ή έναν οργανισμό. Από επιχειρηματική σκοπιά, θα μπορούσαμε να ορίσουμε ένα Πληροφοριακό Σύστημα (Π.Σ) ως μια διοικητική λύση, βασισμένη στην τεχνολογία της Πληροφορικής και των Τηλεπικοινωνιών, που απαντά σε διάφορα προβλήματα της επιχείρησης και του περιβάλλοντός της [1]. Στις ακόλουθες ενότητες αναφέρονται κάποια είδη πληροφοριακών συστημάτων που υπάρχουν στην αγορά, ποιοι είναι οι βασικοί σκοποί των Π.Σ και τα ιδιαίτερα χαρακτηριστικά τους. Τέλος, γίνεται αναφορά στον κύκλο ζωής των Π.Σ και των παραγόντων που μπορούν να οδηγήσουν σε επιτυχία και αποτυχία ένα Π.Σ.

1.2 Είδη Πληροφοριακών Συστημάτων

Υπάρχουν πολλά είδη πληροφοριακών συστημάτων που μπορούν να χρησιμοποιηθούν ανάλογα με τις ανάγκες και τις οικονομικές δυνατότητες της επιχείρησης. Τα σημαντικότερα Π.Σ είναι τα εξής [2]:

- SCMS (Supplier and Contract Management System / Συστήματα Διαχείρισης Αλυσίδας Εφοδιασμού)
- KMS (Knowledge Management Systems / Συστήματα Διαχείρισης Γνώσης)
- OAS (Office Automation Systems / Συστήματα Αυτοματοποίησης Γραφείου)
- TPS (Transaction Processing Systems / Συστήματα Επεξεργασίας Συναλλαγών)
- ERP (Enterprise resource planning / Συστήματα Ενδοεπιχειρησιακού Σχεδιασμού)

- ESS (Executive Support Systems / Συστήματα Υποστήριξης Διοίκησης)
- DSS (Decision Support Systems / Συστήματα Υποστήριξης Απόφασης)
- MIS (Management Information Systems / Διοικητικά Συστήματα Πληροφόρησης)

1.3 Σκοποί Πληροφοριακού Συστήματος

Οι βασικοί σκοποί ενός πληροφοριακού συστήματος αναφέρονται ακολούθως [3]:

1. Η παροχή λειτουργικής πληροφόρησης στους εργαζομένους για να επιτελούν κατά τον καλύτερο δυνατό τρόπο τις δραστηριότητες της επιχείρησης.

2. Η συλλογή και αποθήκευση δεδομένων, τα οποία με κατάλληλη επεξεργασία μετασχηματίζονται σε χρήσιμη πληροφόρηση.

3. Η παροχή στρατηγικής πληροφόρησης σε κατάλληλη μορφή στα διευθυντικά στελέχη για να παίρνουν τις καλύτερες δυνατές αποφάσεις, που σχετίζονται με τη μελλοντική πορεία του οργανισμού.

4. Η επέκταση της αλυσίδας αξίας της επιχείρησης. Για την επίτευξη αυτού του σκοπού είναι αναγκαίο το πληροφοριακό σύστημα της επιχείρησης να συνδέεται με εξωτερικά πληροφοριακά συστήματα και ιδιαίτερα με εκείνα των προμηθευτών, των ενδιάμεσων και των αγοραστών, προκειμένου να δημιουργηθούν οφέλη από την απόκτηση επιπρόσθετης πληροφόρησης.

1.4 Χαρακτηριστικά Πληροφοριακών Συστημάτων

Τα πληροφοριακά συστήματα παρουσιάζουν τα εξής ιδιαίτερα χαρακτηριστικά [4]:

- Μεγάλος όγκος δεδομένων που απαιτεί ειδικούς μηχανισμούς αποθήκευσης και συχνά καθορίζει την αρχιτεκτονική του συστήματος.
- Ταυτόχρονη πρόσβαση στο σύστημα από πολλούς χρήστες
- Αυξημένες απαιτήσεις επικοινωνίας με το χρήστη
- Επικοινωνία με άλλα πληροφοριακά συστήματα

- Νοητική δυσαρμονία στα δεδομένα
- Παράλογη Λογική
- Ταυτοποίηση και αυθεντικοποίηση για πρόσβαση των χρηστών στους πόρους του συστήματος
- Ασφάλεια και έλεγχος

1.5 Κύκλος Ζωής Πληροφοριακών Συστημάτων

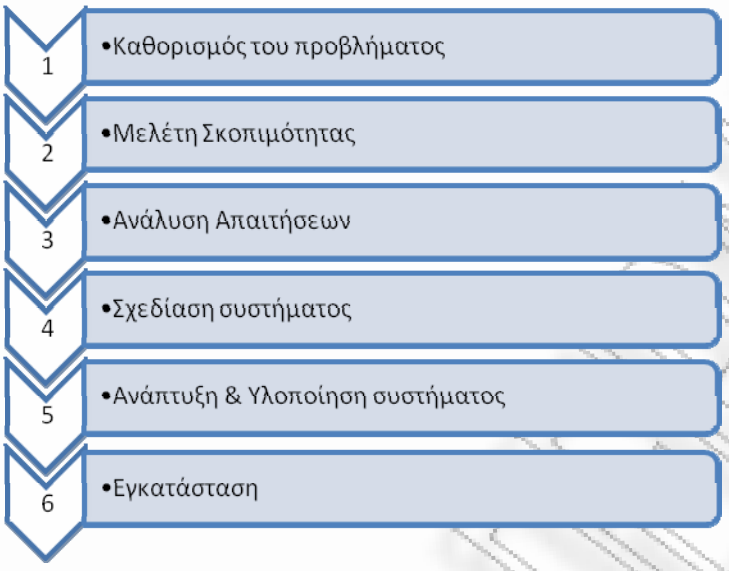
Κατά το πρώτο βήμα εξετάζεται ποιο είναι το πραγματικό πρόβλημα που θέλει να επιλύσει ο οργανισμός με τη χρήση του Πληροφοριακού Συστήματος. Επίσης, πραγματοποιείται μια προκαταρκτική έρευνα για τις πιθανές επιλογές Π.Σ που υπάρχουν στην αγορά και αξιολογούνται οι εφικτές επιλογές βάση των αναγκών και των απαιτήσεων που θέλει να καλύψει ο οργανισμός από το Π.Σ.

Κατά το στάδιο της Μελέτης Σκοπιμότητας εξετάζεται αν είναι εφικτή η υλοποίηση της λύσης και προσδιορίζεται το κόστος και το όφελος του Πληροφοριακού Συστήματος.

Κατά το στάδιο της ανάλυσης απαιτήσεων απαντώνται ερωτήματα σχετικά με την απόδοση του συστήματος και τις λειτουργίες που θα παρέχονται.

Κατά το στάδιο του σχεδιασμού το Πληροφοριακό Σύστημα αρχίζει να παίρνει μορφή. Υλοποιείται ο φυσικός και λογικός σχεδιασμός, παρέχεται δομή στο σύστημα και επιλέγεται ο κατάλληλος εξοπλισμός για την εγκατάσταση του. Πρόκειται για το σημαντικότερο κομμάτι του όλου συνόλου και αναπτύσσεται ανάλογα με τις ανάγκες που έχουν καθοριστεί από τον οργανισμό.

Κατά το στάδιο της Υλοποίησης γίνεται η ανάπτυξη και ο έλεγχος του Πληροφοριακού Συστήματος. Τέλος, ακολουθεί η φάση της εγκατάστασης και συντήρησης του Π.Σ. Αν ωστόσο σε οποιοδήποτε βήμα εμφανιστεί η ανάγκη βελτίωσης του συστήματος, πραγματοποιούνται οι κατάλληλες αλλαγές και τροποποιήσεις. Επίσης, είναι σημαντικό να αναφερθεί ότι οι φάσεις του Κύκλου Ζωής των Π.Σ μπορεί να ενσωματώνονται και να υλοποιούνται ταυτόχρονα.



Σχήμα 1: Φάσεις Κύκλου Ζωής Πληροφοριακών Συστημάτων

1.6 Παράγοντες επιτυχίας Πληροφοριακών Συστημάτων

Ένα από τα πιο αποτελεσματικά και περισσότερο εφαρμοζόμενα και δοκιμασμένα εργαλεία μέτρησης της ποιότητας ενός Πληροφοριακού Συστήματος αποτελεί το μοντέλο επιτυχίας Π.Σ των DeLone & McLean [5]. Μέσα από το συγκεκριμένο μοντέλο εξετάζονται ουσιαστικοί παράγοντες, οι οποίοι αλληλεξαρτώνται και αλληλεπιδρώνται. Οι παράγοντες αυτοί διερευνούν έννοιες, όπως η ποιότητα του συστήματος, η ποιότητα της πληροφορίας, η ικανοποίηση του χρήστη, καθώς και η επίδραση της ποιότητας, τόσο στο άτομο, όσο και στον οργανισμό. Σύμφωνα με το συγκεκριμένο μοντέλο, τα Π.Σ αξιολογούνται με βάση τους εξής παράγοντες:

- Η ***Ποιότητα του Συστήματος*** (System Quality) περιγράφει το πόσο «καλό» είναι το Π.Σ, όσον αφορά τα λειτουργικά του χαρακτηριστικά.
- Η ***Ποιότητα της Πληροφορίας*** (Information Quality) ορίζει το πόσο «καλό» είναι το Π.Σ, όσον αφορά τις εκροές του. Ορισμένοι παράγοντες οι οποίοι έχουν σχέση με την ποιότητα της πληροφορίας ενδεικτικά είναι:
  - η σημαντικότητα
  - η σχετικότητα
  - η χρησιμότητα
  - η ακρίβεια

- η πληρότητα
- το περιεχόμενο της πληροφορίας

- Η ***Χρήση του Συστήματος*** (System Use) αναφέρεται στην χρησιμοποίηση και αξιοποίηση των εκροών από το ίδιο το Π.Σ.
- Η ***Ικανοποίηση του Χρήστη*** (User Satisfaction) μετρά το πώς αντιλαμβάνονται οι χρήστες το ίδιο το σύστημα κατά τη χρησιμοποίησή του, και θεωρείται ως μία σημαντική παράμετρος για τη μέτρηση της επιτυχίας ενός Π.Σ. Το αποτέλεσμα του συνόλου της χρήσης είναι ισοδύναμο και σημαντικό, ανεξάρτητα από την αποτελεσματικότητα του καθαυτού συστήματος.
- Η ***Επίδραση στο Άτομο*** (Individual Impact) αφορά το πώς επιδρά η χρήση ενός Π.Σ στην εκτέλεση των καθηκόντων του ατόμου μέσα στον χώρο της εργασίας του. Σύμφωνα με τους DeLone & McLean, η επίδραση θα μπορούσε να αποτελεί μία ισχυρή ένδειξη ότι το πληροφοριακό σύστημα προσφέρει στον χρήστη καλύτερη κατανόηση του περιεχομένου των αποφάσεων του, βελτίωση σχετικά με τις αποφάσεις του για την παραγωγικότητα, αλλαγή στις δραστηριότητές του, καθώς και αλλαγή στην κατανόηση της σημαντικότητας και παράλληλα της χρησιμότητας του συστήματος του οργανισμού.
- Τέλος, η ***Επίδραση στον Οργανισμό*** (Organizational Impact) εξετάζει κατά πόσο τα αποτελέσματα της επίδρασης του ατόμου επηρεάζουν την λειτουργία του οργανισμού, και επιπροσθέτως μετράει την αποτελεσματικότητα του οργανισμού ως ένα ολόκληρο σύνολο, ως μία πλήρη οντότητα.

1.7 Παράγοντες αποτυχίας Πληροφοριακών Συστημάτων

Η αποτελεσματική εφαρμογή ενός πληροφοριακού συστήματος εξαρτάται από ένα σύνολο παραγόντων και όχι μεμονωμένα από έναν. Υπάρχουν περιπτώσεις άριστα σχεδιασμένα συστήματα να αποτυγχάνουν. Για παράδειγμα ένα Π.Σ μπορεί να εξυπηρετεί άριστα μια εταιρεία και να αποτύχει σε μια άλλη. Οι λόγοι αποτυχίας ενός Π.Σ είναι οι εξής [6]:

- ***Εστίαση στα τεχνικά χαρακτηριστικά του συστήματος***

Οι επιχειρήσεις και οι οργανισμοί είναι ένα σύνολο κρίκων που ενώνονται και εργάζονται ώστε να δημιουργήσουν ένα αποτέλεσμα, είτε αυτό είναι προϊόν, είτε αυτό είναι υπηρεσία. Το σύνολο αυτό αποτελείται από τους ανθρώπους, την τεχνολογία, την δομή και τις διαδικασίες. Όταν κάτι επηρεάζει αυτό το σύνολο δημιουργεί επιπτώσεις που σχετίζονται άμεσα ή έμμεσα με τα υπόλοιπα. Τα συστήματα αυτά έχουν τεχνικές και κοινωνικές επιπτώσεις σε μια επιχείρηση, όταν δίνεται μεγαλύτερη έμφαση στην τεχνική του μεριά, τότε έχουμε αρνητικές επιπτώσεις στην κοινωνική του, άρα στους ανθρώπους.

- ***Ο ανθρώπινος παράγοντας***

Όπως προαναφέραμε ένα Π.Σ μπορεί από τεχνικής άποψης να είναι πετυχημένο και ταυτόχρονα αποτυχημένο σε επίπεδο χρήστη. Και αυτό γιατί οι δημιουργοί του συστήματος σκέφτονται μόνο να αναπτύξουν μια πολύ καλή μηχανή και ξεχνάνε ότι αυτή η μηχανή θα χρησιμοποιηθεί από ανθρώπους. Όταν δημιουργείται το σύστημα οι σχεδιαστές εμπλέκουν τον ανθρώπινο παράγοντα χωρίς όμως επιτυχία. Όταν δημιουργείται ένα Π.Σ θα πρέπει και τα στελέχη της επιχείρησης να λαμβάνουν μέρος σε αυτή την διαδικασία διότι αυτοί και οι υπάλληλοι τους θα χρησιμοποιήσουν αυτό το σύστημα. Επιπλέον μπορεί να έχει πραγματοποιηθεί λανθασμένη εκτίμηση τον αναγκών και των αλλαγών που πρέπει να πραγματοποιηθούν, άρα θα προκύψουν και προβλήματα κατά την χρήση του. Υπάρχουν στελέχη που θεωρούν ότι η εισαγωγή ενός Π.Σ θα επηρεάσει ένα μικρό ποσοστό της επιχείρησης και όχι ολόκληρη, με αποτέλεσμα με την εγκατάσταση του Π.Σ να προκαλείται αναστάτωση σε αρκετά τμήματα της επιχείρησης. Επιπλέον ένα δύσχρηστο Π.Σ δεν θα μπορέσει να ικανοποιήσει τους χρήστες, άρα θα υπάρχει μεγάλο πρόβλημα από άποψη χρηστικότητας και ικανοποίησης των χρηστών. Από την στιγμή που το Π.Σ θα αποτύχει να ικανοποιήσει τους χρήστες, θα αποτύχει και το ίδιο σαν σύστημα.

- ***Έλλειψη εκπαίδευσης και διαθέσιμου χρόνου***

Όταν εγκατασταθεί ένα Π.Σ θα πρέπει να γίνει ή να έχει γίνει εκπαίδευση των υπαλλήλων για την προσαρμογή τους στις νέες συνθήκες. Άρα αν δεν γίνει η εκπαίδευση δεν θα μπορέσει να λειτουργήσει σωστά το σύστημα. Επιπλέον, δεν μπορεί η εκπαίδευση να πραγματοποιηθεί τελευταία στιγμή, πρέπει η επιχείρηση να έχει φροντίσει για την έγκαιρη εκπαίδευση του προσωπικού, ώστε η προσαρμογή του να γίνει με ομαλούς ρυθμούς.

- ***Ο παράγοντας κόστος***

Ένα Π.Σ μπορεί να αποτύχει πριν ακόμα δημιουργηθεί και αυτό γιατί μπορεί να αποτύχει σαν πρόταση υλοποίησης, διότι το κόστος του να μην μπορέσει να καλυφτεί από την επιχείρηση και να ανατρέξει σε πιο οικονομικές λύσεις. Επιπλέον ένα Π.Σ να έχει υλοποιηθεί και να μην καταφέρει ποτέ να αποσβέσει τα χρήματα του και αυτό γιατί δεν θα είχε πραγματοποιηθεί σωστή έρευνα και δεν αξιολογήθηκαν σωστά τα αναμενόμενα οφέλη.

- ***Ο παράγοντας χρόνος***

Η ομάδα υλοποίησης του έργου θα πρέπει να ακολουθήσει αυστηρά το χρόνο παράδοσης και υλοποίησης του Π.Σ και αυτό γιατί οποιαδήποτε πιθανή καθυστέρηση μπορεί να δυσαρεστήσει ή ακόμα και να αποβεί μοιραία τόσο για την επιχείρηση όσο και για την ομάδα υλοποίησης του έργου.

Κεφάλαιο 2: Διαχείριση Έργων Π.Σ

2.1 Εισαγωγή

Στον παρόν κεφάλαιο κρίνεται σκόπιμο να πραγματοποιηθεί μια συνοπτική αναφορά στα έργα και στη διαχείριση έργων για έργα Π.Σ. Αναλύεται ο ορισμός του έργου, οι περιορισμοί και οι στόχοι του, τα βασικά χαρακτηριστικά του και ο Κύκλος Ζωής ενός έργου. Επίσης, πραγματοποιείται συνοπτική αναφορά στη διαχείριση κινδύνων έργων Πληροφοριακών Συστημάτων που αφορά την ανάλυση της συγκεκριμένης διπλωματικής εργασίας. Η εισαγωγή αυτή παρουσιάζει τις ενέργειες και διεργασίες που απαιτούνται καθ ' όλη τη διάρκεια κατασκευής ενός έργου.

2.2 Ορισμός Έργου

Ως έργο χαρακτηρίζεται μια προσωρινή προσπάθεια δημιουργίας ενός μοναδικού προϊόντος ή υπηρεσίας. Η απόφαση έναρξης ενός έργου έρχεται να καλύψει μια διαγνωσμένη ανάγκη - έλλειψη στον τομέα που θα καλύψει με την ολοκλήρωση του. Ένα έργο περιλαμβάνει ένα μοναδικό στόχο, τελικό προϊόν ή αποτέλεσμα και αποτελεί μια συγκεκριμένη χρονική δραστηριότητα που δεν επαναλαμβάνεται ποτέ με τον ίδιο τρόπο.

Έργο, είναι ένα *προσωρινό* εγχείρημα που στοχεύει στη δημιουργία ενός *μοναδικού* προϊόντος ή υπηρεσίας [7, 10]:

Προσωρινό σημαίνει ότι κάθε έργο έχει συγκεκριμένη αρχή και καθορισμένο τέλος. Το τέλος έρχεται όταν οι στόχοι του έργου επιτευχθούν, ή όταν καταστεί σαφές ότι οι στόχοι του έργου δεν θα επιτευχθούν ή δεν μπορούν να επιτευχθούν, ή η ανάγκη για το έργο δεν υφίσταται πλέον και τερματίζεται. Προσωρινό δε σημαίνει απαραίτητα και σύντομο χρονικά. Πολλά έργα διαρκούν πολλά χρόνια. Σε κάθε περίπτωση, πάντως, το τέλος του είναι συγκεκριμένο και δεν μπορεί να συνεχίζεται σε μόνιμη βάση.

Η προσωρινή φύση ενός έργου δεν αναφέρεται μόνο στο χρόνο παράδοσης του, αλλά και στην ομάδα έργου η οποία σπάνια έχει μεγαλύτερη διάρκεια από το έργο.

Τα περισσότερα έργα εκτελούνται από μια ομάδα που δημιουργήθηκε για το σκοπό και μόνο εκτέλεσης του έργου και με το πέρας του χρόνου η ομάδα διαλύεται.

Μοναδικό σημαίνει ότι το προϊόν ή η υπηρεσία διαφέρει κατά ξεχωριστό τρόπο απ ' όλα τα παρόμοια προϊόντα ή υπηρεσίες. Ένα προϊόν ή μια υπηρεσία μπορεί να είναι μοναδικά ακόμα και αν η κατηγορία στην οποία ανήκουν είναι πλούσια σε παρόμοια προϊόντα ή υπηρεσίες.

Οι ιδιότητες αυτές των έργων, να είναι προσωρινά αλλά και μοναδικά εγχειρήματα, έρχονται σε αντίθεση με τη δομή που έχουν οι περισσότερες επιχειρήσεις που λειτουργούν βάση διαδικασιών που έχουν σταθερό και μόνιμο χαρακτήρα. Η διαχείριση αυτών των ιδιοτήτων είναι συχνά δύσκολη διότι απαιτεί ιδιαίτερες ικανότητες από διαφορετικά γνωστικά πεδία.

Το ζητούμενο λοιπόν στη διαχείριση έργων είναι να εξασφαλίσουμε ότι το έργο εκτελείται και παραδίδεται λαμβάνοντας υπόψη καθορισμένους περιορισμούς. Περιορισμοί που μπορεί να είναι ανεπαρκής διαθέσιμος χρόνος, περιορισμένος προϋπολογισμός κ.α. Η δεύτερη πρόκληση που είναι και πιο φιλόδοξη, είναι η βελτιστοποίηση που απαιτείται να γίνει σε όλους τους παράγοντες που επηρεάζουν την εκτέλεση ενός έργου. Επομένως, ένα έργο είναι ένα προσεκτικά επιλεγμένο σύνολο δραστηριοτήτων που επιλέγονται για τη βέλτιστη χρήση των πόρων (χρόνος, χρήματα, άνθρωποι, υλικά, μηχανήματα, ενέργεια, χώρος κ.α.) με απώτερο σκοπό την επίτευξη των προκαθορισμένων στόχων του έργου.

Έτσι καταλήγουμε σε ένα δεύτερο ορισμό για το έργο:

Έργο είναι μια ακολουθία μοναδικών, σύνθετων και αλληλοσχετιζόμενων δραστηριοτήτων που αποσκοπούν στην επίτευξη κάποιου συγκεκριμένου σκοπού. Όλες οι δραστηριότητες ενός έργου θα πρέπει να ολοκληρωθούν μέσα σε περιορισμένο χρόνο και με περιορισμένο κόστος, ικανοποιώντας ταυτόχρονα τις απαιτούμενες προδιαγραφές ποιότητας.

2.3 Βασικά χαρακτηριστικά ενός έργου

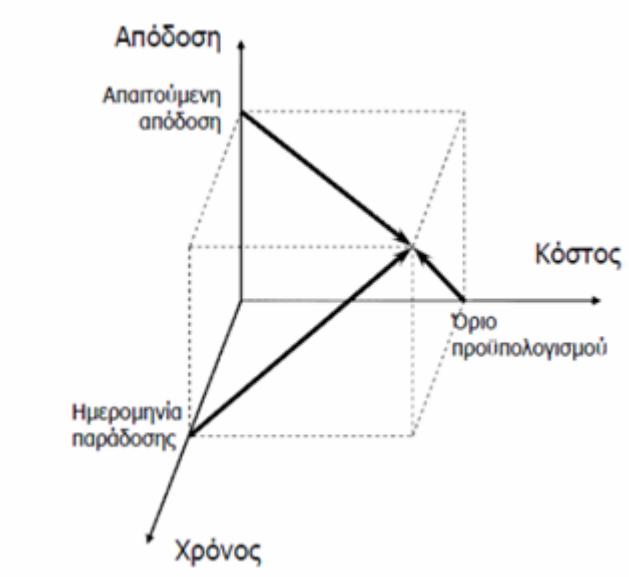
Τα βασικά χαρακτηριστικά ενός έργου αναφέρονται παρακάτω [7]:

- Αποτελείται από μη επαναλαμβανόμενες δραστηριότητες οι οποίες στη γενική περίπτωση μπορούν να περιγραφούν από τον κύκλο ζωής του έργου.
- Απαιτείται σχεδιασμός ώστε να επιτευχθεί το τελικό αποτέλεσμα
- Το τελικό αποτέλεσμα είναι μοναδικό
- Η εκτέλεση του έργου απαιτεί την ύπαρξη ομάδας
- Έχει έναρξη και λήξη
- Υπόκειται σε περιορισμούς διαφόρων ειδών (χρόνου, κόστους ποιότητας κ.α.)
- Οι διαθέσιμοι πόροι είναι περιορισμένοι
- Είναι μεγάλο και πολύπλοκο

2.4 Περιορισμοί – Στόχοι του Έργου

Το παραδοτέο του έργου υπόκεινται σε τρεις κύριους περιορισμούς, τον χρόνο, το κόστος και την ποιότητα [8]. Το καθήκον του διαχειριστή του έργου είναι να εξισορροπήσει αυτές τις μεταβλητές ώστε να φθάσει σε βέλτιστη ισορροπία κόστους – χρονοδιαγράμματος – ποιότητας. Η τριάδα των περιορισμών αυτών αναφέρεται συχνά ως τρίγωνο διαχείρισης έργου, όπου κάθε πλευρά αντιπροσωπεύει έναν περιορισμό. Αλλαγή στην μια πλευρά του τριγώνου που μεταφράζεται σε αλλαγή των περιορισμών προκαλεί αλλαγή στους περιορισμούς που σχετίζονται με τους άλλους παράγοντες. Έτσι, η μείωση του χρόνου μπορεί να απαιτεί αύξηση του κόστους ή μείωση των ποιοτικών χαρακτηριστικών κοκ . Ένα έργο είναι ένα προσεκτικά επιλεγμένο σύνολο δραστηριοτήτων που επιλέγονται για τη βέλτιστη χρήση των πόρων (χρόνος, χρήμα, άνθρωποι, υλικά, χώρος κ. α) με απώτερο σκοπό την επίτευξη των προκαθορισμένων στόχων του έργου.

Εικονικά κάθε έργο έχει έναν τρισδιάστατο στόχο όπως φαίνεται στο Σχήμα 2, να ολοκληρώσει την εργασία σύμφωνα με τον προϋπολογισμό, με το χρονοδιάγραμμα, και τις απαιτήσεις απόδοσης



Σχήμα 2: Το τρίγωνο της διαχείρισης έργων

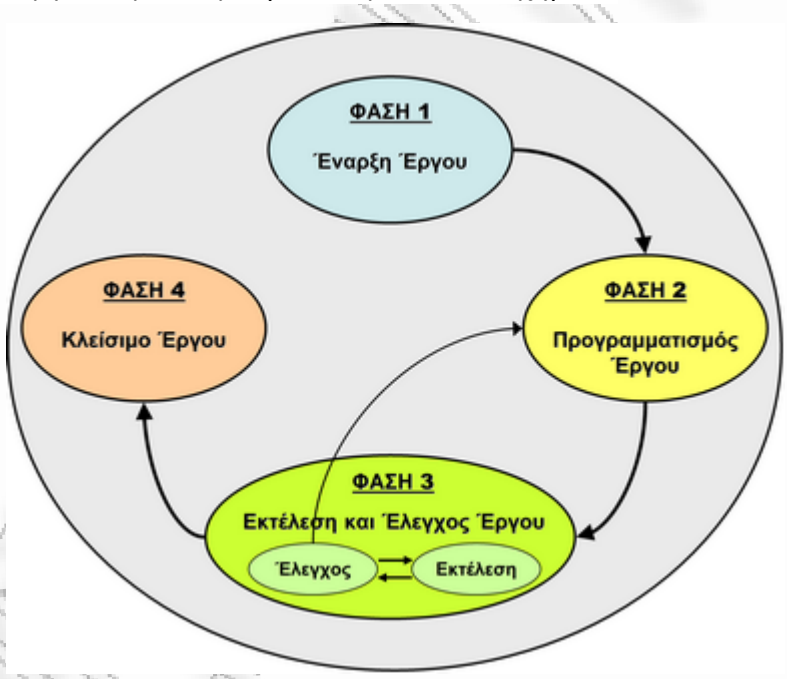
Αναλύοντας τους τρεις περιορισμούς – στόχους του έργου:

1. **Ποιότητα**: Ένα σύστημα ποιότητας για την παρακολούθηση των διεργασιών σ' ένα έργο είναι μια καλή επένδυση. Όχι μόνο συνεισφέρει στην ικανοποίηση του πελάτη αλλά επίσης βοηθάει τον οργανισμό να χρησιμοποιεί αποτελεσματικότερα τους πόρους του μειώνοντας τις σπατάλες.
2. **Κόστος**: Το κόστος του έργου είναι το ύψος της χρηματοδότησης που έχει προϋπολογιστεί από την εκκίνηση έως την ολοκλήρωσή του. Αποτελεί μια από τις κύριες συνιστώσες επιτυχίας του έργου και η αυξομείωσή του είναι συνάρτηση του μεγέθους και της πολυπλοκότητας του έργου. Σε αρκετές περιπτώσεις το κόστος εκτιμάται κατά την εκκίνηση του έργου και αποτελεί κριτήριο για τη συνέχιση ή όχι του έργου. Η διάσταση του προϋπολογισμού του έργου λοιπόν, δηλώνει το προσδιορισμένο ή επιτρεπόμενο κόστος για το έργο.
3. **Χρόνος**: Συνήθως ο πελάτης ορίζει ένα χρονοδιάγραμμα ή μια καταληκτική ημερομηνία ολοκλήρωσης του έργου. Ο χρόνος είναι αρκετά ενδιαφέρον πόρος. Καταναλώνεται ακόμα και αν δε χρησιμοποιείται, δεν αποθηκεύεται και η σχέση του με το κόστος είναι

αντιστρόφως ανάλογη. Ο στόχος της ομάδας έργου είναι να διαχειριστεί το χρόνο με τον πιο αποτελεσματικό και αποδοτικό τρόπο. Η διάσταση του χρονοδιαγράμματος του έργου, περιλαμβάνει την χρονική περίοδο στην οποία θα γίνει η εργασία και την ημερομηνία - στόχο στην οποία θα ολοκληρωθεί το έργο.

2.5 Κύκλος ζωής Έργου

Ο Κύκλος Ζωής Έργου αναφέρεται σε μία λογική ακολουθία δραστηριοτήτων για την επίτευξη των σκοπών ή στόχων του έργου [9]. Ανεξάρτητα από το αντικείμενο ή την πολυπλοκότητά του, κάθε έργο διέρχεται από μία σειρά φάσεων κατά τη διάρκεια της ζωής του. Τυπικά ο Κύκλος Ζωής Έργου αποτελείται από τέσσερις βασικές φάσεις, όπως παρουσιάζονται στο Σχήμα 3:



Σχήμα 3: Κύκλος Ζωής Έργου

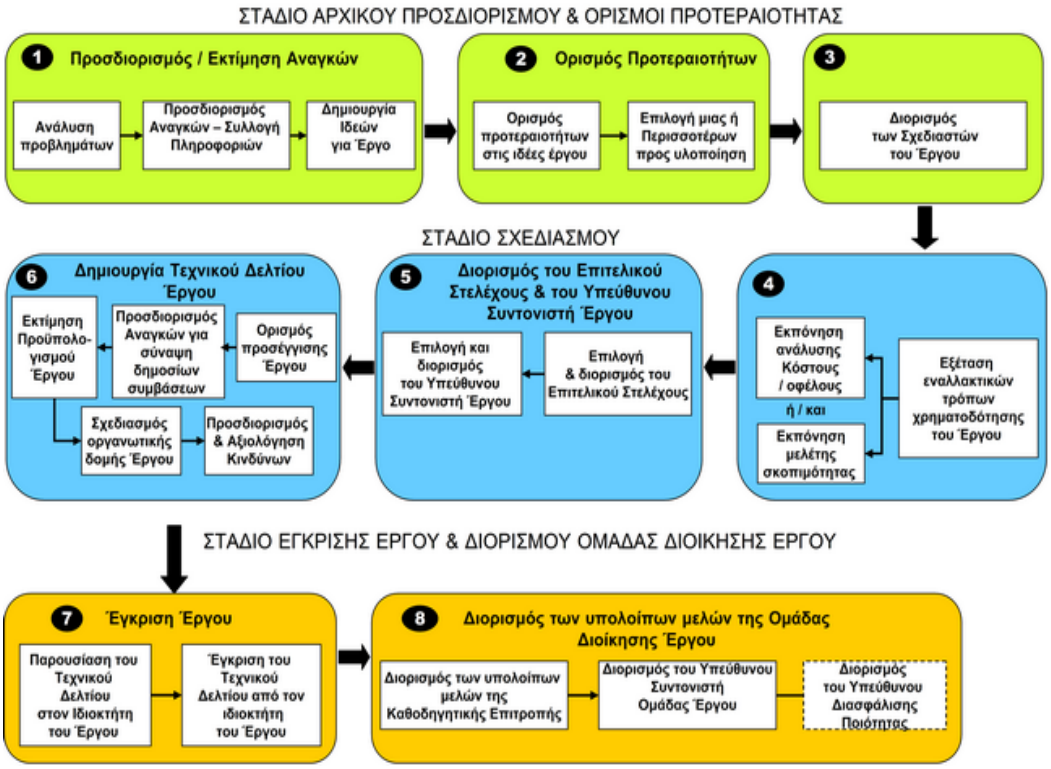
- ***Φάση 1: Έναρξη έργου***

Κατά τη φάση αυτή εντοπίζεται ένα επιχειρησιακό πρόβλημα ή μία ευκαιρία και παράγεται η Έκθεση Επιχειρησιακής Σκοπιμότητας Έργου. Είτε πριν είτε κατά τη διάρκεια είτε μετά την εκπόνηση της Έκθεσης Επιχειρησιακής Σκοπιμότητας Έργου

εκπονούνται συνήθως η Ανάλυση Κόστους - Οφέλους και η Μελέτη Σκοπιμότητας για τον προσδιορισμό της εναλλακτικής λύσης με το μέγιστο καθαρό όφελος και για τη διερεύνηση του βαθμού στον οποίο κάθε εναλλακτική λύση αντιμετωπίζει το επιχειρησιακό πρόβλημα. Ως αποτέλεσμα της Έκθεσης Επιχειρησιακής Σκοπιμότητας Έργου, προτείνεται μία τελική συνιστώμενη λύση. Όταν η συνιστώμενη λύση εγκριθεί, διορίζονται το Επιτελικό Στέλεχος και ο Υπεύθυνος Συντονιστής για να συμμετάσχουν στην εκπόνηση του «Τεχνικού Δελτίου Έργου», το οποίο περιγράφει συνοπτικά το αντικείμενο, τους στόχους, τις δραστηριότητες, τη δομή, τον προϋπολογισμό, το χρονοδιάγραμμα υλοποίησης, τους κινδύνους, τους περιορισμούς και τις υποθέσεις εργασίας για το έργο. Όταν το Τεχνικό Δελτίο Έργου εγκριθεί, διορίζονται τα υπόλοιπα μέλη της Ομάδας Διαχείρισης Έργου.

Συνοπτικά, οι διαδικασίες έναρξης του έργου περιλαμβάνουν τρία στάδια και παρουσιάζονται αναλυτικά στο Σχήμα 4:

1. **Στάδιο Αρχικού Εντοπισμού Αναγκών και Ορισμού Προτεραιοτήτων**
2. **Στάδιο Σχεδιασμού**: Πρόκειται για εκτενής περιγραφή του έργου που τυπικά εγκρίνεται από τον ιδιοκτήτη του έργου.
3. **Στάδιο Έγκρισης Έργου και Διορισμού Ομάδας Διαχείρισης Έργου:** Πρόκειται για το τελικό στάδιο, όπου πλέον το έργο εγκρίνεται επίσημα, δεσμεύονται τα αναγκαία κονδύλια και διορίζεται η ομάδα διαχείρισης έργου (εκτός από το επιτελικό στέλεχος και τον υπεύθυνο συντονιστή που έχουν διοριστεί στο στάδιο σχεδιασμού).



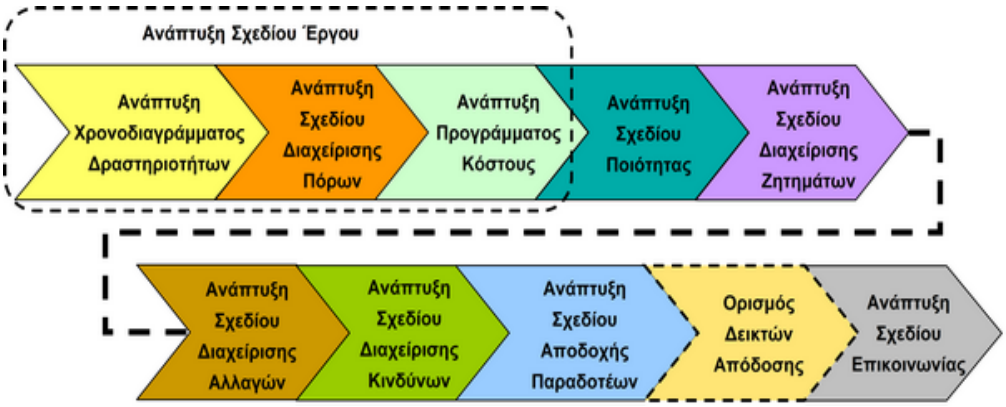
Σχήμα 4: Διάγραμμα ροής βημάτων/δραστηριοτήτων που λαμβάνουν χώρα στα τρία στάδια της Έναρξης Έργου

- ***Φάση 2: Προγραμματισμός έργου***

Η φάση αυτή περιλαμβάνει τον προγραμματισμό / σχεδιασμό όλων των στοιχείων/ παραμέτρων του έργου, έτσι ώστε να είναι έτοιμο προς υλοποίηση. Με αυτή την προοπτική, πρέπει να εκπονούνται τα εξής σχέδια: ***Χρονοδιάγραμμα Δραστηριοτήτων*** (καθορισμός της ακολουθίας δραστηριοτήτων και εργασιών, χρονικός προγραμματισμός), ***Σχέδιο Διαχείρισης Πόρων*** (προσδιορισμός της εργασίας, του εξοπλισμού, των υλικών που απαιτούνται σε κάθε εργασία/στάδιο), ***Πρόγραμμα Κόστους*** (προσδιορισμός εσωτερικών και εξωτερικών μεγεθών κόστους και του χρόνου εμφάνισής τους), ***Σχέδιο Διαχείρισης Κινδύνων*** (επισήμανση πιθανών κινδύνων και των ενεργειών για τον μετριασμό τους), ***Σχέδιο Ποιότητας*** (ορισμός στόχων ποιότητας για τα παραδοτέα του Έργου και καθορισμός των διεργασιών διασφάλισης και ελέγχου ποιότητας), ***Σχέδιο Διαχείρισης Ζητημάτων*** (καθορισμός διεργασίας για τον προσδιορισμό, εκτίμηση και επίλυση ζητημάτων σχετικών με το έργο), ***Σχέδιο Διαχείρισης Αλλαγών*** (καθορισμός διεργασίας για τη διαχείριση αλλαγών που έχουν άμεση επίπτωση στο έργο), ***Σχέδιο Αποδοχής***

Παραδοτέων (ορισμός κριτηρίων αποδοχής για τα παραδοτέα του έργου και καθορισμός των διεργασιών για την εκτέλεση των δοκιμών αποδοχής), ***Σχέδιο Επικοινωνίας*** (καθορισμός πληροφοριών προς διανομή στους ενδιαφερομένους και επιλογή των κατάλληλων μεθόδων για τη διανομή τους). Επιπλέον, κατά τη φάση αυτή καθορίζονται συνήθως οι Δείκτες Απόδοσης που θα χρησιμοποιηθούν σε μεταγενέστερο στάδιο για την παρακολούθηση της προόδου υλοποίησης του έργου και την αξιολόγηση της απόδοσής του σε σύγκριση με διατυπωμένους σκοπούς και στόχους.

Ο προγραμματισμός είναι επαναλαμβανόμενη και επαναληπτική διεργασία. Κάθε φορά που παρουσιάζονται νέες πληροφορίες ή πραγματοποιούνται τροποποιήσεις στις υφιστάμενες όλα τα παραπάνω σχέδια οφείλουν να ενημερώνονται. Οι διεργασίες προγραμματισμού εφαρμόζονται κατά τη δεύτερη φάση του κύκλου ζωής του έργου και παρουσιάζονται στο Σχήμα 5:



Σχήμα 5: Οι Διεργασίες Προγραμματισμού

- ***Φάση 3: Εκτέλεση και Έλεγχος του Έργου***

Η φάση αυτή περιλαμβάνει την εκτέλεση κάθε δραστηριότητας και εργασίας που ορίζεται στο Χρονοδιάγραμμα του Έργου. Κατά την υλοποίηση των δραστηριοτήτων και των εργασιών εκτελείται επίσης μία σειρά από διαχειριστικές διαδικασίες για την παρακολούθηση και τον έλεγχο των εξής: χρόνου, πόρων, κόστους, κινδύνων, ποιότητας, ζητημάτων, αλλαγών, διαδικασίας αποδοχής παραδοτέων, επικοινωνίας, κλπ. Ο Φορέας Υλοποίησης φέρει την πλήρη ευθύνη για την επίτευξη όλων των αποτελεσμάτων του έργου. Ωστόσο, σε περίπτωση που ένας

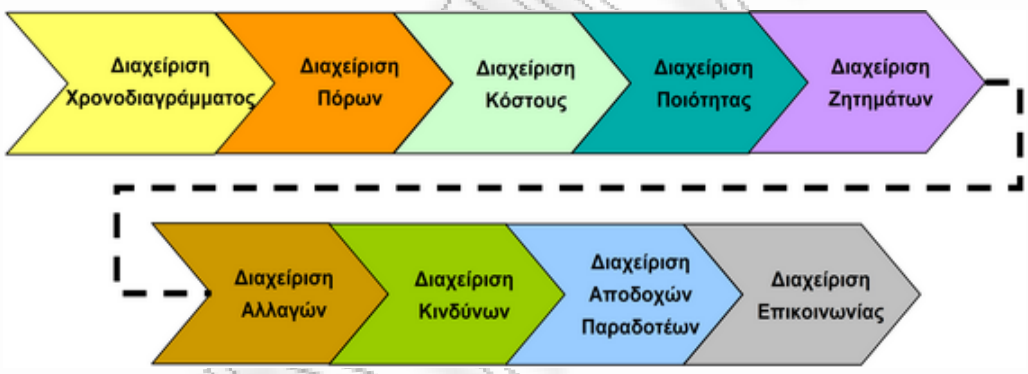
Φορέας Υλοποίησης αποφασίζει να αναθέσει με υπεργολαβία την εκτέλεση τμημάτων ή του συνόλου του έργου, αναλαμβάνει την ευθύνη παρακολούθησης και ελέγχου των αναδόχων. Από την άποψη αυτή, εφαρμόζονται οι ακόλουθες διεργασίες διαχείρισης:

1. ***Διαχείριση Χρονοδιαγράμματος***: Είναι η διεργασία μέσω της οποίας παρακολουθείται η πραγματική πρόοδος των δραστηριοτήτων και εργασιών και, εφόσον τούτο είναι αναγκαίο, υλοποιούνται διορθωτικές ενέργειες για να επαναφέρουν τις εργασίες, τις δραστηριότητες ή και το συνολικό έργο εντός του χρονοδιαγράμματος.
2. ***Διαχείριση Πόρων:*** Είναι η διεργασία μέσω της οποίας παρακολουθείται η πραγματική πρόοδος της απασχόλησης των πόρων και, εφόσον τούτο είναι αναγκαίο, υλοποιούνται διορθωτικές ενέργειες για την επίλυση προβλημάτων κατανομής πόρων.
3. ***Διαχείριση Κόστους:*** Είναι η διεργασία μέσω της οποίας παρακολουθείται το πραγματικό κόστος έναντι του εκτιμηθέντος και, εφόσον τούτο είναι αναγκαίο, υλοποιούνται διορθωτικές ενέργειες για τη διατήρηση του κόστους εντός του προϋπολογισμού.
4. ***Διαχείριση Ποιότητας:*** Είναι η διεργασία μέσω της οποίας διασφαλίζεται και ελέγχεται η ποιότητα των παραδοτέων, με χρήση των σχετικών τεχνικών και εφαρμογή του Σχεδίου Ποιότητας που εκπονήθηκε κατά την προηγούμενη φάση.
5. ***Διαχείριση Ζητημάτων:*** Είναι η διεργασία μέσω της οποίας προσδιορίζονται, εκτιμώνται και επιλύονται, με τυποποιημένο τρόπο, ζητήματα σχετικά με το έργο.
6. ***Διαχείριση Αλλαγών:*** Είναι η διεργασία μέσω της οποίας προσδιορίζονται, αξιολογούνται και εγκρίνονται πριν από την υλοποίηση, με τυποποιημένο τρόπο, αλλαγές στο αντικείμενο, τα παραδοτέα, τις χρονικές κλίμακες ή τους πόρους του έργου.
7. ***Διαχείριση Κινδύνων:*** Είναι η διεργασία μέσω της οποίας ελέγχονται οι κίνδυνοι που εντοπίσθηκαν κατά τις Φάσεις έναρξης και προγραμματισμού, παρακολουθούνται οι υπολειμματικοί κίνδυνοι και εντοπίζονται νέοι, εξασφαλίζεται η εκτέλεση των Σχεδίων Διαχείρισης

Κινδύνων (προληπτικές ενέργειες και ενέργειες αντιμετώπισης) και αξιολογείται η αποτελεσματικότητά τους στο μετριασμό των κινδύνων.

8. ***Διαχείριση Αποδοχών Παραδοτέων:*** Είναι η διεργασία μέσω της οποίας τα παραγόμενα παραδοτέα επισκοπούνται και γίνονται αποδεκτά από την Αναθέτουσα Αρχή σύμφωνα με το Σχέδιο Αποδοχής Παραδοτέων.

9. ***Διαχείριση Επικοινωνίας:*** Είναι η διεργασία μέσω της οποίας διανέμονται πληροφορίες στα ενδιαφερόμενα μέρη του έργου σύμφωνα με το Σχέδιο Επικοινωνίας, και μέσω της οποίας αναφέρεται η πρόοδος του έργου.



Σχήμα 6: Οι διεργασίες Εκτέλεσης & Ελέγχου

- ***Φάση 4: Κλείσιμο Έργου***

Η φάση αυτή περιλαμβάνει όλες τις δραστηριότητες και τις εργασίες που διασφαλίζουν την πλήρη αποπεράτωση του έργου και το σωστό «κλείσιμο» της σύμβασης. Επίσης, περιλαμβάνει την αξιολόγηση των διαδικασιών που χρησιμοποιήθηκαν στο έργο και των αποτελεσμάτων που επιτεύχθηκαν. Με την έννοια αυτή, πρέπει να εφαρμόζονται οι εξής διεργασίες:

1. ***Διοικητικό Κλείσιμο:*** Είναι η διεργασία μέσω της οποίας συλλέγονται και αρχειοθετούνται όλα τα αρχεία του Έργου και αποδεσμεύονται όλοι οι παρεχόμενοι στο Έργο πόροι.

2. ***Επισκόπηση Αξιολόγησης του Έργο:*** Είναι η διεργασία μέσω της οποίας γίνεται αξιολόγηση του Έργου (Επιτεύχθηκαν οι στόχοι του Έργου; Τι πήγε καλά και τι όχι; Ήταν καλή η ποιότητα της διαχείρισης Έργου; κλπ.).

3. ***Επισκόπηση Έργου σε Κανονική Λειτουργία:*** Είναι η διεργασία μέσω της οποίας γίνονται εκτιμήσεις για τα οφέλη του Έργου μετά από μία περίοδο χρήσης/λειτουργίας.

Σχήμα 7: Οι Διεργασίες Κλεισίματος

Κεφάλαιο 3: Διαχείριση Κινδύνων έργων Π.Σ

3.1 Εισαγωγή

Στο παρόν κεφάλαιο προτείνεται μια διαδικασία διαχείρισης κινδύνων που αποτελεί τη βέλτιστη πρακτική για τη διεθνή πραγματικότητα, καθώς υιοθετεί στοιχεία από τα οποία προκύπτει το βέλτιστο δυνατό αποτέλεσμα, το οποίο θα μπορεί να εφαρμοστεί σε διάφορα επίπεδα ολοκλήρωσης, αντικατοπτρίζοντας τις ανάγκες μιας μικρής, μέσης και μεγάλης επιχείρησης. Ουσιαστικά αναλύεται τι είναι κίνδυνος, ποια είναι η δομή και τα χαρακτηριστικά του, καθώς επίσης και ποιοι είναι οι διάφοροι τύποι κινδύνων που υπάρχουν. Τέλος, αναλύεται η προτεινόμενη διαδικασία διαχείρισης κινδύνων και πως αυτή σχετίζεται με τη διοίκηση έργων.

3.2 Ορισμός Κινδύνου

Κίνδυνος είναι ένα αβέβαιο γεγονός ή κατάσταση που, σε περίπτωση που προκύψει, έχει θετική ή αρνητική συνέπεια σε κάποιο στόχο του έργου, όπως είναι ο χρόνος, το κόστος και η ποιότητα [10]. Επομένως, ο κίνδυνος είναι ένας παράγοντας που δεν είναι εφικτό να είναι γνωστό αν θα εμφανιστεί ή όχι. Ο κίνδυνος μπορεί να έχει μία οι περισσότερες αιτίες και εφόσον προκύψει μπορεί να οδηγήσει σε μια οι περισσότερες συνέπειες. Προκειμένου να μεγιστοποιούνται οι πιθανότητες και οι συνέπειες των θετικών για τους στόχους του έργου συμβάντων και να ελαχιστοποιούνται οι πιθανότητες και οι συνέπειες των δυσμενών συμβάντων, πρέπει σε κάθε έργο να σχεδιάζονται και να εγκαθίστανται διαδικασίες διαχείρισης κινδύνου.

3.3 Τύποι Κινδύνων

Οι κίνδυνοι μπορούν να διαχωριστούν τόσο στο επίπεδο της ***φύσης*** τους όσο και στο επίπεδο της ***προσέλευσης*** τους [11]. Όσον αφορά τη φύση τους χωρίζονται σε ευκαιρίες και απειλές και όσον αφορά τη προσέλευση τους σε εσωτερικούς και εξωτερικούς.

Ο διαχωρισμός του κινδύνου σε εσωτερικό και εξωτερικό πραγματοποιείται με τη δυνατότητα του οργανισμού να αναλογιστεί αν το έργο που εκτελείται, είναι σε θέση να επηρεάσει, μέσω συγκεκριμένων ενεργειών, την πιθανότητα εμφάνισης του κινδύνου. Εάν ναι, τότε πρόκειται για εσωτερικό κίνδυνο, εάν όχι ο κίνδυνος είναι εξωτερικός.

Ενδιαφέρον μάλιστα παρουσιάζει ο συνδυασμός των δύο καταστάσεων, καθώς δημιουργεί μια εικόνα του οργανισμού για κάθε κίνδυνο. Έτσι, η εικόνα του οργανισμού είναι ιδιαίτερα θετική για τις εσωτερικές ευκαιρίες από τη στιγμή που μπορεί να τις επηρεάσει και να αυξήσει την θετική επιρροή τους. Στην αντίθετη πλευρά, βρίσκονται οι εξωτερικές απειλές, στην κατάσταση στην οποία ο οργανισμός δεν επεμβαίνει ώστε να μετριάσει τη πιθανότητα εκδήλωσης αρνητικών συνεπειών. Ενδιάμεση κατάσταση αποτελούν οι εξωτερικές ευκαιρίες και οι εσωτερικές απειλές. Από την μια πλευρά οι εξωτερικές ευκαιρίες έχουν πολύ μικρή πιθανότητα να συμβούν, από την άλλη πλευρά οι εσωτερικές απειλές πρέπει να εξαλειφθούν.

Σχήμα 8: Διαχωρισμός κινδύνων κατά φύση και προέλευση

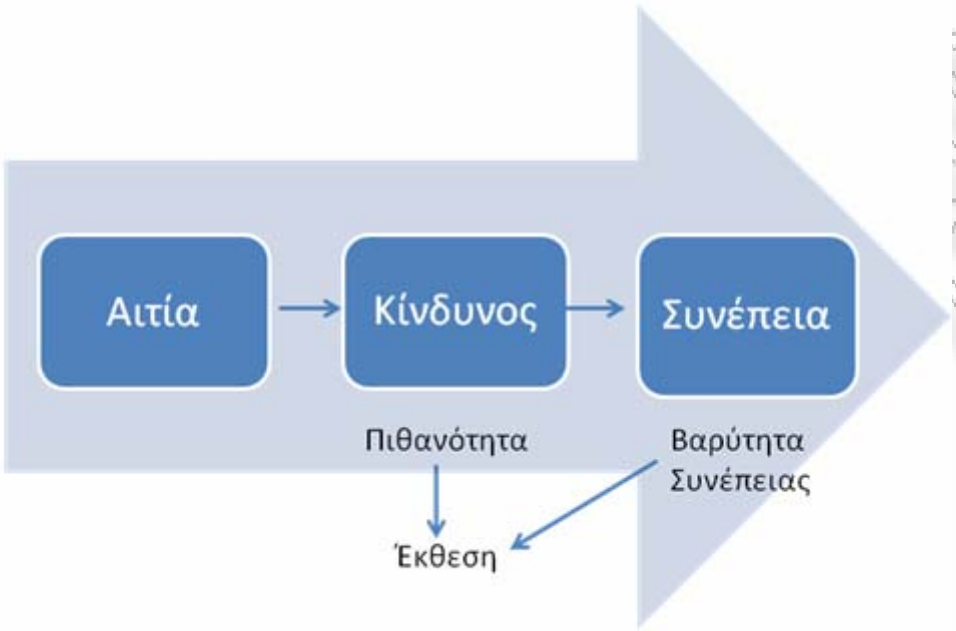
Εκτός από τις βασικές κατηγορίες κινδύνων υπάρχουν και άλλες κατηγορίες όπως για παράδειγμα: ο κίνδυνος μπορεί να αποφευχθεί ή όχι (υποκειμενικό κριτήριο), πρόκειται για κίνδυνο που έχει άμεση επίπτωση ή όχι, πρόκειται για κίνδυνο που επαναλαμβάνεται κατά τη διάρκεια εκτέλεσης του έργου [12].

Τέλος, πέρα από τη γενική κατηγοριοποίηση των κινδύνων σύμφωνα με τις γενικότερες ιδιότητές τους, οι κίνδυνοι διαχωρίζονται και κατά τομείς επίδρασης (διοικητικοί, τεχνικοί, οικονομικοί κλπ).

3.4 Δομή και χαρακτηριστικά του κινδύνου

Κάθε κίνδυνος, ανεξάρτητα από τη φύση ή την προέλευσή του και ανεξάρτητα από τον τομέα επίδρασης στον οποίο αναφέρεται, έχει συγκεκριμένη δομή. Ο κίνδυνος δημιουργείται επειδή υφίστανται κάποιες αιτίες και σε περίπτωση που επέλθει, επιφέρει κάποιες συνέπειες στους στόχους του έργου. Κάθε ένα στοιχείο της δομής του κινδύνου (αιτία, κίνδυνος, συνέπεια) διαθέτει συγκεκριμένα χαρακτηριστικά (πιθανότητα, βαρύτητα, έκθεση) [11].

Πιο συγκεκριμένα οι αιτίες θεωρούνται δεδομένα στοιχεία του έργου και για να χαρακτηριστεί ένα στοιχείο ως *αιτία* θα πρέπει να μην υπάρχει αμφιβολία σχετικά με τη βεβαιότητά του. Δηλαδή, η αιτία είναι ένα γεγονός το οποίο ενδεχομένως να οδηγήσει στην εμφάνιση *κινδύνου*. Ωστόσο, ο κίνδυνος, μπορεί να έχει περισσότερες από μια αιτίες και μια αιτία μπορεί να αναφέρεται σε περισσότερους από ένα κινδύνους. Επίσης, ο κίνδυνος, φέρει συγκεκριμένη *πιθανότητα* εμφάνισης, η οποία καθορίζεται από τις ήδη υπάρχουσες αιτίες. Απλοϊκά, όσες περισσότερες αιτίες υπάρχουν , τόσο μεγαλύτερη είναι η πιθανότητα εμφάνισης του κινδύνου. Το δεύτερο χαρακτηριστικό του κινδύνου είναι η *έκθεση*, δηλαδή το πόσο σημαντικός είναι ο κίνδυνος για το έργο. Η έκθεση προκύπτει από το γινόμενο της πιθανότητας εμφάνισης του κινδύνου και της βαρύτητας της συνέπειας. Το τελευταίο στοιχείο της δομής του κινδύνου είναι η *συνέπεια* η οποία υποδεικνύει πόσο σημαντική είναι η συνέπεια ενός κινδύνου σε περίπτωση εμφάνισής του, σε σχέση με τους στόχους του έργου. Ένας κίνδυνος μπορεί να έχει μια ή περισσότερες συνέπειες και μια συνέπεια μπορεί να προκαλείται από περισσότερους από έναν κινδύνους.



Σχήμα 9: Δομή και χαρακτηριστικά του κινδύνου

3.5 Διαχείριση Κινδύνων

Η διαχείριση των κινδύνων κατά PMBOK (Project Management Book Of Knowledge) είναι η συστηματική διαδικασία εντοπισμού, ανάλυσης, αντιμετώπισης και παρακολούθησης των κινδύνων και αφορά τη λήψη μέτρων για το μετριασμό των κινδύνων [13]. Ουσιαστικά μεγιστοποιεί την πιθανότητα και τις συνέπειες των θετικών γεγονότων και ελαχιστοποιεί την πιθανότητα των δυσμενών γεγονότων με σκοπό την επίτευξη των στόχων του έργου. Ουσιαστικά, η διαχείριση κινδύνων είναι η διαδικασία που βοηθάει την ομάδα διαχείρισης κινδύνων να μην αποκλίνουν από την αποστολή του οργανισμού, να λαμβάνουν κατάλληλα μέτρα προστασίας των Πληροφοριακών Συστημάτων και να προσπαθούν να επιλύσουν τυχόν προβλήματα κινδύνων πριν αυτά συμβούν.

Το γενικότερο πλαίσιο της διαδικασίας διαχείρισης κινδύνων περιγράφεται από το λεγόμενο σχέδιο διαχείρισης κινδύνων (Project Risk Management), στο οποίο περιγράφονται οι τρόποι που θα εφαρμοστεί η διαδικασία, οι μέθοδοι και οι τεχνικές που θα ακολουθηθούν, ο ρυθμός των συναντήσεων, ο τρόπος και ο χρονισμός των αναφορών και γενικότερα οτιδήποτε μπορεί να προδιαγραφεί πριν ξεκινήσει η διαδικασία. Ο βασικός σκοπός του σχεδίου διαχείρισης κινδύνων σε

έργα πληροφορικής είναι να βοηθήσει τους οργανισμούς να προστατεύουν και να παρέχουν ασφάλεια στις διάφορες πληροφορίες που μπορεί κάποιος να αντλήσει από ένα Πληροφοριακό Σύστημα.

Όπως φαίνεται και στο Σχήμα 10, το σχέδιο διαχείρισης των κινδύνων είναι το σημείο αναφοράς το οποίο επιτρέπει στην ομάδα του έργου να κινηθεί εντός του «Γαλαξία των Κινδύνων», μεθοδικά και με αυξημένη αποτελεσματικότητα. Η συσχέτιση του σχεδίου διαχείρισης κινδύνων μ' έναν Γαλαξία, πραγματοποιείται για να τονιστεί η αβεβαιότητα και η πολυπλοκότητα που υπάρχει σ΄ ένα έργο, και τους πιθανούς κινδύνους που μπορούν να το επηρεάσουν.

Σχήμα 10: Διαδικασία Διαχείρισης Κινδύνων

3.6 Εφαρμογή Διαδικασίας Διαχείρισης Κινδύνων

Η εφαρμογή της διαδικασίας διαχείρισης κινδύνων κατά PMBOK περιλαμβάνει 6 βήματα όπως ακολουθεί [13]:

1. Δημιουργία Σχεδίου Διαχείρισης Κινδύνων
2. Εντοπισμός Κινδύνων

3. Ανάλυση Κινδύνων
4. Αντιμετώπιση Κινδύνων
5. Παρακολούθηση Κινδύνων
6. Αξιολόγηση & Αναφορά Κινδύνων

Το πρώτο βήμα της διαδικασίας διαχείρισης κινδύνων περιλαμβάνει τη ***δημιουργία σχεδίου διαχείρισης κινδύνων***, το οποίο είναι ο βασικός οδηγός εκτέλεσης της διαδικασίας διαχείρισης κινδύνων. Ο ποιοτικός σχεδιασμός του και η πληρότητά του είναι σημαντικά στοιχεία για την επιτυχία ή την αποτυχία της διαδικασίας διαχείρισης κινδύνων. Ουσιαστικά το σχέδιο διαχείρισης κινδύνων περιγράφει τον τρόπο με τον οποίο θα εκτελούνται τα βήματα της διαδικασίας διαχείρισης κινδύνων (εντοπισμός, ανάλυση, αντιμετώπιση και παρακολούθηση). Η έκταση του σχεδίου είναι ανάλογη με το μέγεθος του έργου και είναι απαραίτητη διαδικασία όσο μικρό και να είναι το έργο.

Σύμφωνα με τους περισσότερους επιστήμονες και καταξιωμένα στελέχη που ασχολούνται με τη διαχείριση κινδύνων, τα περιεχόμενα ενός σχεδίου διαχείρισης κινδύνων πρέπει να περιλαμβάνουν τουλάχιστον τα εξής [14]:

- **Μέθοδος:** Το σχέδιο διαχείρισης κινδύνων θα πρέπει να περιλαμβάνει με σαφήνεια τα βήματα της διαδικασίας διαχείρισης κινδύνων που θα ακολουθηθούν. Η καταγραφή της μεθόδου γίνεται για να καθοριστεί ο τρόπος προσέγγισης της διαχείρισης κινδύνων και προσδιορίζει τα εργαλεία που θα χρησιμοποιηθούν και τις πηγές αναζήτησης στοιχείων. Για παράδειγμα, στη μέθοδο μπορεί να προσδιοριστεί ότι ο εντοπισμός των κινδύνων θα γίνει από τον πελάτη ή από την ίδια εταιρία που καλείται να υλοποιήσει το έργο.
- **Ρόλοι και αρμοδιότητες:** Μετά την επιλογή της κατάλληλης μεθόδου ακολουθεί η συγκρότηση της ομάδας διαχείρισης κινδύνου και η κατανομή αρμοδιοτήτων. Αποφασίζεται ποιος θα είναι ο υπεύθυνος της διαδικασίας και κατά πόσο η ομάδα θα είναι εσωτερική, ή εξωτερική. Για παράδειγμα, όταν η επιλογή της ομάδας είναι εξωτερική, θα πρέπει να γίνει σωστή τοποθέτηση της ομάδας στο οργανόγραμμα του έργου και να υπάρχει άριστη επικοινωνία μεταξύ της ομάδας και της διοίκησης για να επιτευχθεί το επιθυμητό αποτέλεσμα. Επιπλέον, είναι πολύ πιθανό να δημιουργηθούν

εντάσεις οι οποίες θα ζημιώσουν το έργο αν η εταιρία που υλοποιεί το έργο αντιμετωπίζει ανταγωνιστικά την εξωτερική ομάδα διαχείρισης κινδύνων. Ωστόσο, η επιλογή εσωτερικής ομάδας παρουσιάζει πλεονέκτημα διότι δεν αντιμετωπίζει προβλήματα εξουσίας καθώς τα στελέχη που την απαρτίζουν έχουν γνώση των δεδομένων της επιχείρησης. Σημαντική απόφαση για την επιλογή εσωτερικής ή εξωτερικής ομάδας είναι η διαθεσιμότητα έμπειρων στελεχών στην εταιρία που θα υλοποιήσει το έργο καθώς επίσης και το περιθώριο ανάληψης περισσότερων ευθυνών και ο διαθέσιμος χρόνος που διαθέτουν.

- **Εκπαίδευση:** Είναι σημαντικό να οργανώνονται σύντομα προγράμματα εκπαίδευσης της ομάδας διαχείρισης έργων, είτε από στελέχη της επιχείρησης που έχουν κατάλληλη εμπειρία, είτε από εξειδικευμένους εξωτερικούς συμβούλους. Στις εκπαιδεύσεις αυτές εκτός από τη γενική ιδέα της διαχείρισης των κινδύνων, θα πρέπει επίσης ο εκπαιδευτής να προβάλει τις τεχνικές ή τα εργαλεία εκείνα που είναι περισσότερο πιθανό να χρησιμοποιηθούν ανάλογα με το είδος του υπό εξέταση έργου.
- **Προϋπολογισμός:** Υπάρχουν διάφοροι τρόποι για να καθοριστεί ο προϋπολογισμός της διαχείρισης των κινδύνων ενός έργου.
- Συνήθως, ορίζεται ένα ***ποσοστό του κόστους του έργου***, ως απόθεμα για την αντιμετώπιση των κινδύνων. Αυτό το απόθεμα, μπορεί να χρησιμοποιηθεί από την ομάδα για την υλοποίηση ενεργειών αντιμετώπισης. Το αρνητικό σε αυτό τον τρόπο προσδιορισμού του προϋπολογισμού είναι ότι οι κίνδυνοι δεν είναι εκ των προτέρων γνωστοί άρα και το ποσό που υπολογίζεται ως απόθεμα είναι σχετικό και μπορεί να οδηγήσει σε λάθος αποτέλεσμα.
- Ένας άλλος τρόπος είναι η προκαταρκτική ***ανάλυση των κινδύνων και ο υπολογισμός μιας συνολικής έκθεσης.*** Ένα σημαντικό μειονέκτημα είναι ότι είναι ότι ο προϋπολογισμός θα εκτιμηθεί σε μεταγενέστερο χρόνο, καθώς θα πρέπει να καθοριστεί όσο το δυνατό καλύτερα το έργο για να γίνει ο εντοπισμός και η ανάλυση των κινδύνων. Αυτό πρακτικά σημαίνει

ότι το αναμενόμενο κόστος θα είναι γνωστό πιθανόν μετά την ολοκλήρωση των διαπραγματεύσεων για την ανάθεση του έργου.

- Ένας ενδιάμεσος συλλογισμός, είναι ***η επιλογή και των δύο τρόπων***. Κάποιος από αυτούς τους τρόπους καθορίζεται ότι θα χρησιμοποιηθεί, στο σχέδιο διαχείρισης των κινδύνων, έτσι ώστε να γίνεται γνωστό αφ ΄ ενός το ποσό που θα έχει στη διάθεσή της η ομάδα διαχείρισης κινδύνων και αφ ΄ ετέρου το κόστος που θα πρέπει να προστεθεί στο συνολικό κόστος του έργου και θα αφορά τη διαχείριση κινδύνων.
- **Χρονισμός:** Σε τακτά χρονικά διαστήματα θα πρέπει να γίνονται συναντήσεις με θέμα την παρακολούθηση των κινδύνων. Οι συναντήσεις αυτές θα πρέπει να καθορίζονται από πριν, και θα έχουν ως θέμα την ανάλυση των τακτικών αναφορών σχετικά με την εξέλιξη των κινδύνων, τον εντοπισμό νέων κινδύνων και τις ενέργειες αντιμετώπισης.
- **Μέθοδοι μέτρησης και κλίμακες:** Ουσιαστικά, καθορίζονται οι μέθοδοι που θα χρησιμοποιηθούν (π. χ ποιοτικές ή ποσοτικές) και οι κλίμακες που ορίζουν τα χαρακτηριστικά των κινδύνων (πιθανότητα, συνέπεια). Ανάλογα με το μέγεθος, το είδος και τη σημαντικότητα του έργου, θα πρέπει η ομάδα διαχείρισης κινδύνων να επιλέξει αν η ανάλυση θα είναι ποιοτική ή ποσοτική. Όσον αφορά τις κλίμακες, χρειάζεται ιδιαίτερη προσοχή, για παράδειγμα η ερμηνεία μιας λεκτικής κλίμακας (π. χ αρκετά, λίγο κ. α) θα πρέπει να είναι αντικειμενική γιατί κάθε άνθρωπος την αντιλαμβάνεται με εντελώς διαφορετικό τρόπο ανάλογα με τα βιώματά του και την ιδιοσυγκρασία του.
- **Όρια:** Καθορίζονται τα όρια που είναι αποδεκτά για τους κινδύνους. Γενικά εμφανίζονται τρία επίπεδα κινδύνων: οι ***αμελητέοι,*** οι ***μέσοι*** και οι ***σημαντικοί***. Τα όρια ουσιαστικά καθορίζουν σε ποια από αυτές τις κατηγορίες ανήκει ο κάθε κίνδυνος και είναι ως επί τω πλείστον διαφορετικά για κάθε επιχείρηση και για κάθε έργο. Επιβάλλεται λοιπόν, να προσδιοριστούν σαφώς τα όρια αυτά πριν από την εκτέλεση του έργου. Ωστόσο, σ' ένα μεγάλο έργο με πολλούς κινδύνους, θα πρέπει να υπάρχουν φίλτρα τα οποία θα συγκρατούν κάποιους κινδύνους καθώς θα ανεβαίνουν

τα επίπεδα της ιεραρχίας, ώστε στην ανώτερη διοίκηση να φθάνουν μόνο οι πολύ σημαντικοί κίνδυνοι.

- **Επικοινωνία:** Καθορίζεται ο τρόπος με τον οποίο καταγράφονται, αναλύονται και κοινοποιούνται τα αποτελέσματα της διαχείρισης κινδύνων στους ενδιαφερόμενους του έργου. Επισημαίνεται ότι δεν είναι απαραίτητο να ενημερώνονται όλοι οι ενδιαφερόμενοι του έργου για όλους τους κινδύνους, αλλά ούτε να ενημερώνονται και όλοι με τον ίδιο τρόπο (π. χ συναντήσεις, ηλεκτρονικό ταχυδρομείο, πρότυπη αναφορά κ. α).
- **Καταγραφή – Ιχνηλασία:** Καθορίζεται ο τρόπος με τον οποίο θα καταγράφονται όλες οι δραστηριότητες της διαχείρισης κινδύνων, έτσι ώστε να ωφεληθεί το έργο και να εμπλουτιστεί η εταιρική γνώση και η μελλοντική χρήση. Σε εταιρίες που δεν έχουν συστήματα διαχείρισης γνώσεων για δέσμευση της γνώσης και αποθήκευσής της θα πρέπει τουλάχιστον να αποθηκεύονται τα φύλλα διαχείρισης κινδύνων ανά κατηγορία έργου.

Το δεύτερο και πιο κρίσιμο στάδιο της διαδικασίας διαχείρισης κινδύνων αφορά τον ***εντοπισμό των κινδύνων,*** ο οποίος αποτελεί τον εντοπισμό και την καταγραφή όλων των κινδύνων που είναι πιθανό να επηρεάσουν τους στόχους ενός έργου. Ο εντοπισμός των κινδύνων είναι μια συνεχής διαδικασία για την καταγραφή τόσο των υπαρχόντων όσο και των μελλοντικών κινδύνων και λαμβάνει μέρος σε όλες τις φάσεις του κύκλου ζωής του έργου. Ουσιαστικά, σε αυτό το βήμα αναγνωρίζεται η αιτία εμφάνισής των κινδύνων, η συνέπεια τους (ποιότητα του έργου, κόστος, χρονοδιάγραμμα) και η προέλευση (κίνδυνος τεχνολογίας, επιχειρησιακός κ. α) τους.

Στο επόμενο στάδιο πραγματοποιείται ***ανάλυση των κινδύνων*** που έχουν εντοπιστεί κατά το δεύτερο στάδιο. Η διαδικασία της ανάλυσης, χρησιμοποιείται αφ’ ενός για να καθοριστεί το μέγεθος της συνέπειας του κινδύνου και η πιθανότητα εμφάνισης του, και αφ ΄ ετέρου για να ταξινομηθούν οι κίνδυνοι με βάση τη σοβαρότητά τους. Μόλις ολοκληρωθεί λοιπόν η ανάλυση, οι κίνδυνοι

ιεραρχούνται με βάση την έκθεσή τους και καταγράφονται σε κατάλογο με σειρά προτεραιότητας.

Ουσιαστικά σε αυτό το στάδιο πρέπει να ορίζονται προτεραιότητες για τους κινδύνους, οι κίνδυνοι που μπορεί να είναι πιο επιβλαβείς για το έργο πρέπει να αντιμετωπιστούν είτε με σχέδια μετριασμού, είτε με σχέδια έκτακτης ανάγκης. Περίπου δέκα κίνδυνοι υψηλής έκθεσης (Top Risk List) μπορούν να αντιμετωπιστούν από την ομάδα έργου αποτελεσματικά. Αν η ομάδα διαπιστώσει ότι πάνω από δέκα κίνδυνοι έχουν υψηλή έκθεση, θα πρέπει να επανεξεταστεί το σύνολο της διαδικασίας διαχείρισης κινδύνων, και θα πρέπει να ενημερωθούν ο χορηγός του έργου και τα ενδιαφερόμενα μέρη, γιατί το έργο ενδεχομένως να έχει υψηλό κίνδυνο αποτυχίας.

Με βάση τον κατάλογο προτεραιότητας που έχει προκύψει από το προηγούμενο στάδιο, ακολουθεί το στάδιο ***αντιμετώπισης των κινδύνων*** στο οποίο καθορίζονται σχέδια αντιμετώπισης των κινδύνων, τα οποία θα περιλαμβάνουν προληπτικές και διορθωτικές κινήσεις σύμφωνα με συγκεκριμένες στρατηγικές. Για τους κινδύνους που απαιτούν αντιμετώπιση υπάρχουν δύο στρατηγικές που προτείνονται και αναλύονται στο κεφάλαιο 6, ο μετριασμός των κινδύνων και ο σχεδιασμός σχεδίων έκτακτης ανάγκης.

Με τη λήξη του προηγούμενου σταδίου ακολουθεί το στάδιο της ***παρακολούθησης των κινδύνων***. Σ΄ αυτό το στάδιο, ελέγχεται η υλοποίηση των ενεργειών αντιμετώπισης των κινδύνων καθώς και η αποτελεσματικότητά τους. Επιπλέον, καθορίζονται διορθωτικές κινήσεις και επανεκτιμώνται τα χαρακτηριστικά των κινδύνων. Ο Project Manager σε αυτό το στάδιο θα πρέπει να οργανώνει να κατευθύνει και να παρακολουθεί τις δράσεις μετριασμού των κινδύνων. Επίσης, θα πρέπει να αξιολογεί την αποτελεσματικότητα των μεθόδων μετριασμού των κινδύνων και να επαναξιολογεί σε τακτική βάση το επίπεδο έκθεσης των κινδύνων.

Τέλος, ακολουθεί το στάδιο ***αξιολόγησης και αναφοράς των κινδύνων***. Σε αυτό το στάδιο, οι καινούργιοι κίνδυνοι που έχουν εντοπιστεί και οι παλαιοί κίνδυνοι που έχουν αλλάξει θα πρέπει να κοινοποιούνται στις συνεδριάσεις της ομάδας διαχείρισης του έργου. Παραδείγματα αλλαγών των κινδύνων είναι ο επιτυχής μετριασμός συγκεκριμένου κίνδυνου με αποτέλεσμα να αποσυρθεί ο κίνδυνος, η

εμφάνιση νέου γεγονότος που μπορεί να επηρεάσει σημαντικά συγκεκριμένο κίνδυνο, η ενεργοποίηση ή απενεργοποίηση του σχεδίου έκτακτης ανάγκης και τέλος, η επαναξιολόγηση της "Top Risk List" και η ιεράρχηση των κινδύνων.

Ολόκληρη η διαδικασία λοιπόν, επαναλαμβάνεται σε τακτά χρονικά διαστήματα ώστε να εντοπιστούν νέοι κίνδυνοι και να ενημερωθούν τα φύλλα κινδύνων.

3.7 Ενσωμάτωση Διαδικασίας Διαχείρισης Κινδύνων στον Κύκλο Ζωής των Π.Σ

Η διαδικασία διαχείρισης κινδύνων πρέπει να ενσωματωθεί αποτελεσματικά στο κύκλο ζωής ενός έργου Πληροφοριακού Συστήματος. Ο κύκλος ζωής των Πληροφοριακών Συστημάτων περιλαμβάνει 5 στάδια, την έναρξη, την ανάπτυξη ή απόκτηση, την υλοποίηση, την λειτουργία ή συντήρηση και την διάθεση του Π.Σ στον οργανισμό. Σε ορισμένες περιπτώσεις μπορεί να ενσωματώνονται αυτές οι φάσεις και να υλοποιούνται ταυτόχρονα. Ωστόσο, η διαδικασία διαχείρισης κινδύνων είναι η ίδια σε κάθε φάση του Κύκλου Ζωής και αφορά μια επαναληπτική διαδικασία [15].

Φάση του Κύκλου Ζωής Π.Σ	Χαρακτηριστικά της κάθε Φάσης	Υποστήριξη από τις Δραστηριότητες Διαχείρισης Κινδύνου
1η Φάση Έναρξη	Εκφράζεται η ανάγκη υλοποίησης ενός έργου πληροφορικής και καθορίζεται πλήρως το πεδίο και ο σκοπός του	Οι αναγνωρισμένοι κίνδυνοι χρησιμοποιούνται κατά την αναζήτηση των απαιτήσεων του έργου και ειδικότερα των απαιτήσεων ασφαλείας αλλά και τον καθορισμό των διαδικασιών
2η Φάση Ανάπτυξη ή απόκτηση	Το πληροφοριακό σύστημα σχεδιάζεται, αγοράζεται, προγραμματίζεται, αναπτύσσεται ή κατασκευάζεται	Οι κίνδυνοι που προσδιορίζονται κατά τη διάρκεια αυτής της φάσης μπορούν να χρησιμοποιηθούν για να υποστηρίξουν τις αναλύσεις ασφάλειας του συστήματος, που μπορεί να οδηγήσουν σε αλλαγές αρχιτεκτονικής και σχεδίου κατά τη διάρκεια της ανάπτυξης των συστημάτων

3η Φάση **Υλοποίηση**	Τα χαρακτηριστικά των συστημάτων ασφαλείας διαμορφώνονται, ενεργοποιούνται, εξετάζονται και ελέγχονται	Η διαδικασία διαχείρισης κινδύνου αξιολογεί την εφαρμογή των συστημάτων έναντι των απαιτήσεων τους σε ένα μοντελοποιημένο λειτουργικό περιβάλλον. Οι αποφάσεις σχετικά με τους προσδιορισμένους κινδύνους πρέπει να ληφθούν προτού τα συστήματα τεθούν σε λειτουργία
4η Φάση **Λειτουργία/Συντήρηση**	Το σύστημα εκτελεί τις λειτουργίες του. Ουσιαστικά το σύστημα τροποποιείται σε μια τρέχουσα βάση μέσω της προσθήκης hardware και software και από αλλαγές στις διαδικασίες και πολιτικές του οργανισμού	Οι δραστηριότητες της διαχείρισης κινδύνων πραγματοποιούνται για την περιοδική εξουσιοδότηση των συστημάτων ή όποτε γίνονται σημαντικές αλλαγές στο λειτουργικό ή το περιβάλλον παραγωγής του λειτουργικού
5η Φάση **Διάθεση**	Η φάση αυτή μπορεί να περιλάβει τις δραστηριότητες διάθεσης των πληροφοριών, του hardware και του software. Οι δραστηριότητες αυτές μπορεί να περιλαμβάνουν τη μετακίνηση, την αρχειοθέτηση, την απόρριψη ή την καταστροφή των πληροφοριών και την αποστείρωση του hardware και του software	Οι δραστηριότητες διαχείρισης κινδύνων εκτελούνται για τα τμήματα των συστημάτων που θα διατεθούν ή θα αντικατασταθούν για να εξασφαλίσουν ότι το hardware και το software διατίθεται κατάλληλα, ότι τα υπόλοιπα δεδομένα χρησιμοποιούνται ορθά και ότι η μετακίνηση των συστημάτων διευθύνεται με ασφαλή και συστηματικό τρόπο

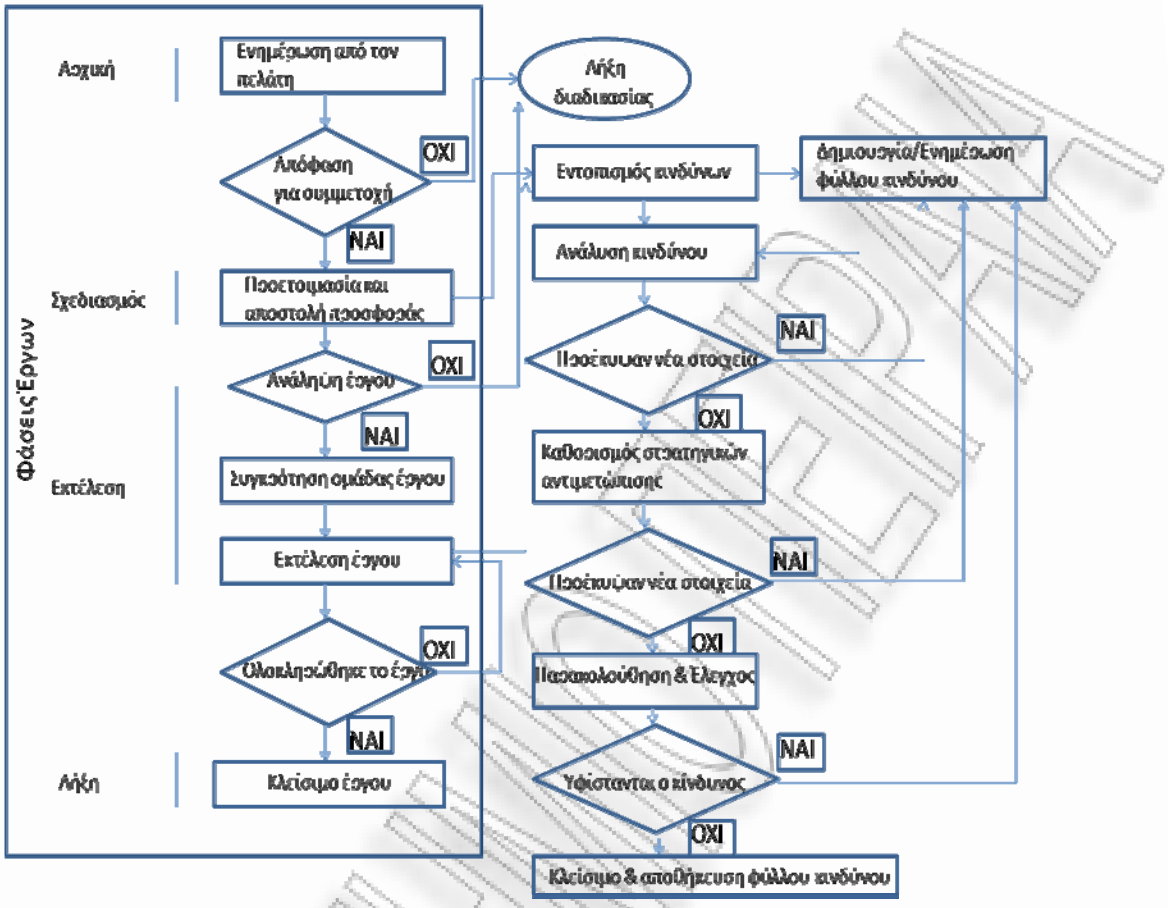
Σχήμα 11: Ενσωμάτωση διαδικασίας διαχείρισης κινδύνων στο κύκλο ζωής των Π.Σ

3.8 Εξωτερική Ανάθεση Διαδικασίας Διαχείρισης Κινδύνων

Σε περίπτωση που η ανάθεση του έργου υλοποιείται από εξωτερική ομάδα έργου, η αρχική φάση πραγματοποιείται συνήθως από τον πελάτη, ενώ το στάδιο του σχεδιασμού από τους ανάδοχους. Σε περίπτωση θετικής για τον ανάδοχο εξέλιξης του έργου, ξεκινά η φάση της εκτέλεσης του έργου, η οποία είναι και η μεγαλύτερη σε διάρκεια. Απ ΄ την άλλη πλευρά, αν η επιλογή της διαχείρισης

κινδύνου αποφασιστεί να γίνει εσωτερικά, η όλη διαδικασία πραγματοποιείται από την ομάδα έργου της ίδιας της εταιρίας. Στο Σχήμα 12 παρουσιάζεται η ενσωμάτωση της διαχείρισης κινδύνων στη διαδικασία διοίκησης έργων στη περίπτωση που ανατεθεί το έργο σε εξωτερική ομάδα.

Η διαχείριση των κινδύνων, ως διαδικασία, ξεκινάει με τον εντοπισμό των κινδύνων. Εντοπισμός των κινδύνων πραγματοποιείται όχι μόνο κατά τη διάρκεια εκτέλεσης του έργου, αλλά και στην πολύ σημαντική φάση της προσφοράς για την ανάληψη του έργου. Όπως φαίνεται και στο Σχήμα 12 η διαδικασία της διαχείρισης κινδύνων περιλαμβάνει τρεις επαναλήψεις της διαδικασίας (εντοπισμός, ανάλυση, αντιμετώπιση και παρακολούθηση). Ο πρώτος κύκλος πραγματοποιείται κατά τη διάρκεια της προσφοράς, ο δεύτερος κατά το χρόνο ανάληψης του έργου και ο τρίτος κατά τη διάρκεια της εκτέλεσης του έργου σε τακτά χρονικά διαστήματα, τα οποία καθορίζονται από το σχέδιο διαχείρισης των κινδύνων. Ωστόσο, το κύριο εργαλείο συνένωσης των σταδίων μεταξύ τους είναι το «φύλλο κινδύνου» το οποίο περιλαμβάνει όλα τα στοιχεία που αφορούν κάθε στάδιο ενός συγκεκριμένου κινδύνου. Κάθε φορά που ολοκληρώνεται ένα στάδιο ελέγχεται αν έχουν προκύψει αλλαγές ή νέα στοιχεία, σε σχέση με τα αναγραφόμενα στο φύλλο κινδύνου, και αν υπάρχουν ενημερώσεις το φύλλο ενημερώνεται. Τέλος, όταν ο κίνδυνος πάψει να υφίστανται, το φύλλο κινδύνου που πρακτικά περιέχει την όλη πορεία και εξέλιξή του στο έργο, αποθηκεύεται, έτσι ώστε να είναι διαθέσιμο για μελλοντική χρήση. Στο παρακάτω σχήμα παρουσιάζεται ένα τυπικό παράδειγμα ενσωμάτωσης της διαχείρισης κινδύνων στη διαδικασία διοίκησης έργων [11].



Σχήμα 12: Ενσωμάτωση της διαχείρισης κινδύνων στη διαδικασία διοίκησης έργων

3.9 Βασικοί ρόλοι στελεχών στη Διαδικασία Διαχείρισης Κινδύνων

Στη συγκεκριμένη ενότητα περιγράφονται οι βασικοί ρόλοι των στελεχών του οργανισμού που πρέπει να υποστηρίξουν και να συμμετάσχουν στη διαδικασία διαχείρισης κινδύνου [15]:

- ***Ανώτερη διοίκηση (Senior Management)***: Η ανώτερη διοίκηση φέρει τη μεγαλύτερη ευθύνη για τη διεκπεραίωση του έργου και πρέπει να εξασφαλίσει ότι οι απαραίτητοι πόροι διατίθενται αποτελεσματικά, για την ικανοποίηση των αναγκών που απαιτούνται για την ολοκλήρωση του έργου. Πρέπει να αξιολογήσει και να ενσωματώσει τα αποτελέσματα της εκτίμησης κινδύνου στη διαδικασία λήψης απόφασης. Η κατάρτιση ενός αποτελεσματικού προγράμματος διαχείρισης κινδύνων που να αξιολογεί και να μετριάζει τους σχετικούς με το πληροφοριακό έργο κινδύνους, απαιτεί την υποστήριξη και τη συμμετοχή της ανώτερης διοίκησης.

- ***Κύριο ανώτερο στέλεχος πληροφοριών (Chief Information Officer - CIO):*** Το στέλεχος αυτό είναι αρμόδιο για το σχεδιασμό του πληροφοριακού έργου, τη σύνταξη του προϋπολογισμού και την απόδοσή του συμπεριλαμβανομένων και των τμημάτων που αφορούν την ασφάλεια των πληροφοριών. Οι αποφάσεις που λαμβάνονται για αυτά τα θέματα πρέπει να βασιστούν σε ένα αποτελεσματικό πρόγραμμα διαχείρισης κινδύνου.
- ***Κάτοχοι συστημάτων και πληροφοριών (System and Information Owners):*** Οι κάτοχοι συστημάτων και πληροφοριών είναι αρμόδιοι να εξασφαλίσουν ότι οι κατάλληλοι έλεγχοι θα πραγματοποιηθούν για να εξετάσουν την ακεραιότητα, την εμπιστευτικότητα και τη διαθεσιμότητα των συστημάτων και των στοιχείων του έργου λογισμικού του οποίου έχουν την κυριότητα. Ουσιαστικά είναι υπεύθυνοι για τις αλλαγές στα πληροφοριακά τους συστήματα, είναι δηλαδή αυτοί που θα εγκρίνουν τις όποιες αλλαγές, όπως για παράδειγμα προσθήκη νέων συστημάτων ή αλλαγές στο software και το hardware. Επιβάλλεται λοιπόν αυτοί να καταλάβουν το ρόλο τους στη διαδικασία διαχείρισης κινδύνων και να την υποστηρίξουν πλήρως.
- ***Επιχειρησιακοί και λειτουργικοί διευθυντές (Business and Functional Managers):*** Οι αρμόδιοι διευθυντές για τις επιχειρησιακές διαδικασίες και τη διαδικασία προμήθειας πληροφοριακών συστημάτων πρέπει να πάρουν ενεργό ρόλο στη διαδικασία διαχείρισης κινδύνου. Οι διευθυντές αυτοί είναι τα πρόσωπα που φέρουν την ευθύνη για αποφάσεις αλλαγών, ουσιαστικών για την ολοκλήρωση του εκάστοτε έργου. Η συμμετοχή τους στη διαχείριση κινδύνων παρέχει την κατάλληλη ασφάλεια των πληροφοριακών συστημάτων, η οποία εάν χρησιμοποιηθεί σωστά, θα προσφέρει την αποτελεσματική ολοκλήρωση της αποστολής με τις ελάχιστες δυνατές δαπάνες πόρων.
- ***Διευθυντές Προγράμματος Ασφαλείας (Information System Security Officer):*** Οι διευθυντές προγράμματος ασφαλείας πληροφοριακών συστημάτων και τα ανώτερα στελέχη ασφάλειας υπολογιστών είναι

αρμόδιοι για τα προγράμματα ασφαλείας του οργανισμού, συμπεριλαμβανομένης και της διαχείρισης κινδύνου. Επομένως διαδραματίζουν κύριο ρόλο στην εισαγωγή μιας κατάλληλης, δομημένης μεθοδολογίας για να βοηθήσουν στον προσδιορισμό, την αξιολόγηση και την ελαχιστοποίηση των κινδύνων των πληροφοριακών συστημάτων που υποστηρίζουν τις λειτουργίες του οργανισμού. Ενεργούν επίσης και ως σύμβουλοι της ανώτερης διοίκησης και εξασφαλίζουν ότι αυτή η δραστηριότητα πραγματοποιείται σε διαρκή βάση.

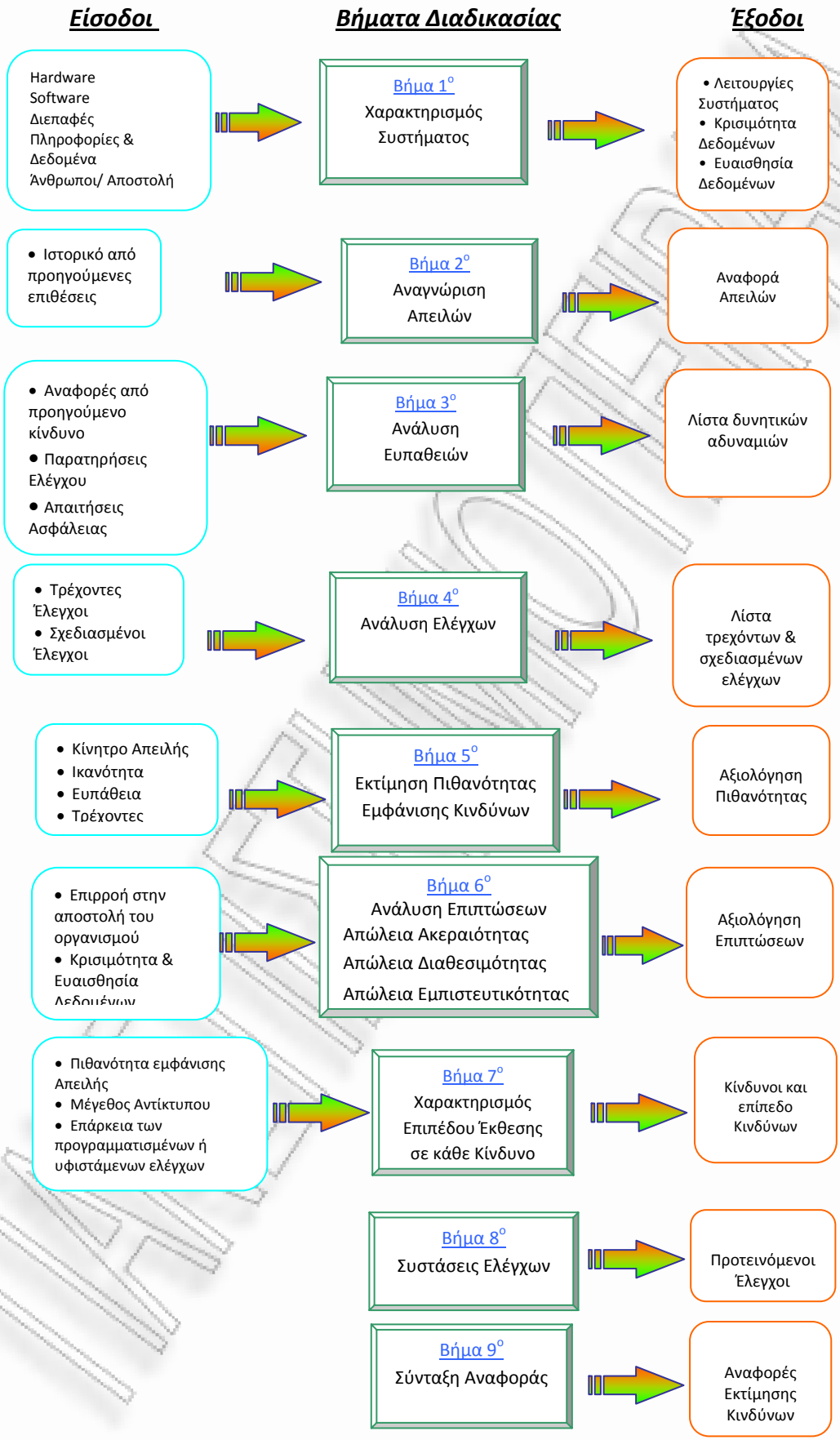
- ***Χειριστές συστημάτων ασφαλείας πληροφοριακών έργων (Information Technology Security Practitioners):*** Τα στελέχη αυτά (για παράδειγμα διοικητές βάσεων δεδομένων, ειδικοί υπολογιστών, αναλυτές ασφαλείας, σύμβουλοι ασφαλείας) είναι αρμόδια για τη σωστή εφαρμογή των απαιτήσεων ασφαλείας των πληροφοριακών συστημάτων. Καθώς οι αλλαγές εμφανίζονται στο υπάρχον λογισμικό περιβάλλον (π.χ. επέκταση στη συνδεσιμότητα δικτύων, αλλαγές στην υπάρχουσα υποδομή και την πολιτική του οργανισμού, εισαγωγή νέων τεχνολογιών) οφείλουν να υποστηρίξουν ή να χρησιμοποιήσουν τη διαχείριση κινδύνων για να προσδιορίσουν και να αξιολογήσουν τους νέους πιθανούς κινδύνους και να εφαρμόσουν τους νέους ελέγχους ασφαλείας όπως απαιτούνται για την προστασία των συστημάτων.
- ***Εκπαιδευτές χρήσης συστημάτων ασφαλείας (Security Awareness Trainers):*** Η χρήση των συστημάτων και των στοιχείων πληροφορικής σύμφωνα με την πολιτική, τις οδηγίες και τους κανόνες συμπεριφοράς του οργανισμού είναι κρίσιμη για τον μετριασμό του κινδύνου και την προστασία των πληροφοριακών συστημάτων. Είναι ουσιαστικό λοιπόν οι χρήστες να έχουν συνείδηση της αξίας των συστημάτων και μηχανισμών ασφαλείας τους. Επομένως οι εκπαιδευτές ασφαλείας πρέπει να κατανοήσουν τη διαδικασία διαχείρισης κινδύνου έτσι ώστε να μπορούν να αναπτύξουν τα κατάλληλα μέσα κατάρτισης του προσωπικού και να ενσωματώσουν την αξιολόγηση κινδύνου στα επιμορφωτικά προγράμματα εκπαίδευσης των τελικών χρηστών.

3.10 Διάγραμμα ροής μεθοδολογίας διαχείρισης κινδύνων

Ο κίνδυνος είναι μια λειτουργία που περιλαμβάνει την πιθανότητα εμφάνισης μιας απειλής που μπορεί να πλήξει τη διαδικασία υλοποίησης ενός έργου και τον επικείμενο αντίκτυπο αυτής της δυσμενούς εκδήλωσης στην πορεία του έργου.

Για να καθοριστεί η πιθανότητα εμφάνισης ενός μελλοντικού δυσμενούς γεγονότος πρέπει οι απειλές σε ένα έργο πληροφοριακού συστήματος να αναλυθούν από κοινού με τις πιθανές ευπάθειες και τους ισχύοντες ελέγχους του έργου. Ο αντίκτυπος αναφέρεται στο μέγεθος της ζημίας που θα μπορούσε να προκληθεί από την εμφάνιση ενός κινδύνου σε έναν ευπαθή τομέα του έργου. Η διαδικασία εκτίμησης κινδύνων περιλαμβάνει τα εννέα βήματα [15] που αναφέρονται στο Σχήμα 13:

1. Χαρακτηρισμός Συστήματος
2. Αναγνώριση Απειλών
3. Ανάλυση Ευπαθειών
4. Ανάλυση Ελέγχων
5. Εκτίμηση Πιθανότητας Εμφάνισης Κινδύνων
6. Ανάλυση Επιπτώσεων
7. Χαρακτηρισμός Επιπέδου Έκθεσης σε κάθε Κίνδυνο
8. Συστάσεις Ελέγχων
9. Σύνταξη Αναφοράς



Σχήμα 13: Διάγραμμα ροής μεθοδολογίας διαχείρισης κινδύνων

Στα επόμενα κεφάλαια θα παρουσιαστούν τα εννέα βήματα της διαδικασίας διαχείρισης κινδύνων. Αρχικά, τα τέσσερα πρώτα βήματα συγκροτούν τη βάση δεδομένων για τα επόμενα βήματα της διαδικασίας και αφορούν τη συλλογή πληροφοριών για το έργο και τον οργανισμό, την αναγνώριση των κινδύνων που μπορούν να προσβάλουν το έργο και την καταγραφή των υπαρχόντων μηχανισμών καταστολής κινδύνων. Ακολουθεί η επεξεργασία αυτών των δεδομένων, για την εξαγωγή συμπερασμάτων σχετικά με την πιθανότητα έκθεσης σε κάθε κίνδυνο, τη σοβαρότητα των επιπτώσεων από την εμφάνισή τους, τη συνολική εικόνα του κάθε κινδύνου, τις προτεινόμενες συστάσεις ελέγχων και τη σύνταξη αναφοράς που θα περιλαμβάνει όλες τις παραπάνω πληροφορίες και που θα αποτελέσει θετικό εργαλείο στη διαμόρφωση του σχεδίου αντιμετώπισης των απειλών.

Κεφάλαιο 4: Εντοπισμός κινδύνων

4.1 Εισαγωγή

Ο εντοπισμός των κινδύνων αποτελεί το δεύτερο στάδιο της διαδικασίας διαχείρισης κινδύνων, μετά από τη δημιουργία σχεδίου διαχείρισης κινδύνων. Οι οργανισμοί χρησιμοποιούν τον εντοπισμό κινδύνων για να καθορίσουν την έκταση της πιθανής απειλής και των κινδύνων που συνδέονται με ένα πληροφοριακό σύστημα σε όλη τη διάρκεια εγκατάστασης αυτού. Τα πορίσματα της διαδικασίας αυτής βοηθούν στον προσδιορισμό των κατάλληλων ελέγχων για τη μείωση ή την εξάλειψη των κινδύνων κατά τη διαδικασία μετριασμού κινδύνων. Τα βήματα που ακολουθούνται σύμφωνα με τη μεθοδολογία διαχείρισης κινδύνων αναλύονται παρακάτω και αφορούν διάφορες πληροφορίες σχετικά με το χαρακτηρισμό του συστήματος, διαδικασίες συλλογής πληροφοριών, αναγνώριση των απειλών και ανάλυση των ευπαθειών του συστήματος.

4.2 Χαρακτηρισμός Συστήματος

Το πρώτο βήμα της διαδικασίας διαχείρισης κινδύνων είναι η συλλογή πληροφοριών σχετικά με τον οργανισμό για τον οποίο προορίζεται το πληροφοριακό σύστημα, τις ανάγκες που καλείται να καλύψει το σύστημα αυτό, αλλά και πληροφορίες για τυχόν παρόμοια έργα που έχουν υλοποιηθεί στο παρελθόν. Η συλλογή αυτών των πληροφοριών θα βοηθήσει στην αναζήτηση των κινδύνων στους οποίους είναι δυνατόν να εκτεθεί το έργο αλλά και στην αναζήτηση τρόπων μετριασμού της πιθανότητας εμφάνισης αυτών ή των επιπτώσεών τους.

Η διαδικασία διαχείρισης κινδύνων απαιτεί λοιπόν την πλήρη κατανόηση του περιβάλλοντος του πληροφοριακού έργου. Οι πληροφορίες που πρέπει να συλλεχθούν μπορούν να ταξινομηθούν στις εξής κατηγορίες [15]:

- Hardware: Πληροφορίες για τον ήδη υπάρχον εξοπλισμό, αλλά και για τον εξοπλισμό που πρόκειται να χρησιμοποιηθεί για το νέο έργο πληροφορικής.
- Software: Πληροφορίες για παλαιό και νέο λογισμικό.

- Διεπαφές συστημάτων: Θα πρέπει να αναγνωριστούν οι εσωτερικές και εξωτερικές διασυνδέσεις του συστήματος που θα εγκατασταθεί.
- Βάσεις δεδομένων: Το είδος, η ποιότητα και η ποσότητα των πληροφοριών και δεδομένων που θα κλιθεί να διαχειριστεί το νέο λογισμικό.
- Στελέχη που θα υποστηρίξουν και θα χρησιμοποιήσουν το νέο σύστημα: Αν διαθέτουν τις κατάλληλες γνώσεις για να χειριστούν το νέο λογισμικό και τι απαιτήσεις για επιπλέον εκπαίδευση υπάρχουν, αν κατανοούν την αξία, τη χρησιμότητα και την ευαισθησία του νέου συστήματος.
- Αποστολή του νέου συστήματος: Ποιες λειτουργίες καλείται να επιτελέσει το νέο πληροφοριακό σύστημα.
- Αξία του νέου συστήματος: Πόσο σημαντική είναι η εγκατάσταση του νέου συστήματος για τη λειτουργία του οργανισμού.
- Ευαισθησία του συστήματος: Το επίπεδο προστασίας που απαιτείται για τη διατήρηση της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των συστημάτων και πληροφοριών.

Επιπλέον πληροφορίες, που σχετίζονται με το λειτουργικό περιβάλλον του συστήματος και είναι εξίσου σημαντικές για τη διαδικασία διαχείρισης κινδύνων, είναι οι εξής:

- Λειτουργικές απαιτήσεις του συστήματος
- Πολιτικές ασφαλείας συστημάτων: Πολιτική του οργανισμού και νομοθετικά πλαίσια.
- Αρχιτεκτονική των συστημάτων ασφαλείας
- Τρέχουσα δικτυακή τοπολογία
- Προστασία αποθηκευμένων πληροφοριών
- Ροή πληροφοριών σχετικών με το σύστημα: Διεπαφές συστήματος, διάγραμμα ροής εισόδων εξόδων του συστήματος.
- Τεχνικοί έλεγχοι που χρησιμοποιούνται για το πληροφοριακό έργο: Ενσωματωμένο ή πρόσθετο υλικό ασφαλείας που υποστηρίζει την αναγνώριση και την επικύρωση πρόσβασης και πληροφοριών,

διακριτικοί ή αυστηροί έλεγχοι πρόσβασης, υπόλοιπη προστασία πληροφοριών, μέθοδοι κρυπτογράφησης.

- Διοικητικοί έλεγχοι για την προστασία του συστήματος: Κανόνες συμπεριφοράς, σχεδιασμός ασφάλειας.
- Λειτουργικοί έλεγχοι: Ασφάλεια προσωπικού, διαδικασίες αποκατάστασης και συντήρησης συστημάτων, έλεγχος χρήσης συστημάτων, προσθήκης και διαγραφής δεδομένων, έλεγχος πρόσβασης χρηστών και ιδιαιτέρως αυτών που έχουν πρόσβαση σε αρχεία και λειτουργίες πέραν των τυποποιημένων.
- Ασφάλεια των εγκαταστάσεων του οργανισμού
- Ασφάλεια σε σχέση με το φυσικό περιβάλλον του έργου: Έλεγχοι για υγρασία, θερμοκρασία, μόλυνση, διαχείριση ενέργειας, βαθμός έκθεσης σε φυσικές καταστροφές.

4.3 Διαδικασίες συλλογής πληροφοριών

Για ένα σύστημα που είναι στη φάση της έναρξης ή του σχεδιασμού, οι πληροφορίες μπορούν να προέλθουν από το ίδιο το σχέδιο ή την κατάσταση με τις απαιτήσεις του έργου. Όταν το έργο είναι υπό ανάπτυξη χρήσιμες πληροφορίες μπορούν να προέλθουν από τον καθορισμό των βασικών κανόνων και των στοιχείων ασφαλείας που προγραμματίζονται για το σύστημα. Για ένα έργο πληροφοριακού συστήματος, οι πληροφορίες συλλέγονται από το περιβάλλον παραγωγής του έργου, συμπεριλαμβανομένων στοιχείων που αφορούν τη διαμόρφωση των συστημάτων, τη συνδεσιμότητα τους και τις προκαθορισμένες ή ακαθόριστες διαδικασίες και πρακτικές. Επομένως, η περιγραφή των συστημάτων μπορεί να βασιστεί στην ασφάλεια που παρέχεται από την υπάρχουσα υποδομή ή τα μελλοντικά σχέδια ασφαλείας.

Φυσικά η συλλογή όλων αυτών των πληροφοριών δεν είναι μια απλή διαδικασία, αλλά απαιτεί προσεκτική, επιστημονική και αυστηρά καθορισμένη ενασχόληση από τα άτομα που θα κληθούν να συλλέξουν αυτές τις πληροφορίες, ούτως ώστε τα αποτελέσματα της έρευνας να έχουν ουσιαστική αξία, να είναι αξιόπιστα και τεκμηριωμένα και να μπορούν να προσφέρουν στη διαδικασία εκτίμησης κινδύνων και όχι να οδηγήσουν σε λάθος συμπεράσματα. Παρακάτω

παρατίθενται διάφοροι μέθοδοι εντοπισμού κινδύνων πληροφοριακών συστημάτων [11, 15].

1. Ερωτηματολόγια

Για να συλλογή σχετικών πληροφοριών, το προσωπικό αξιολόγησης των κινδύνων μπορεί να αναπτύξει ένα ή περισσότερα ερωτηματολόγια σχετικά με τη διαχείριση και τους λειτουργικούς ελέγχους που προγραμματίζονται για το νέο πληροφοριακό σύστημα ή που ήδη χρησιμοποιούνται για τα υπάρχοντα συστήματα. Τα ερωτηματολόγια αυτά πρέπει να διανεμηθούν στο προσωπικό που σχεδιάζει ή υποστηρίζει το σύστημα.

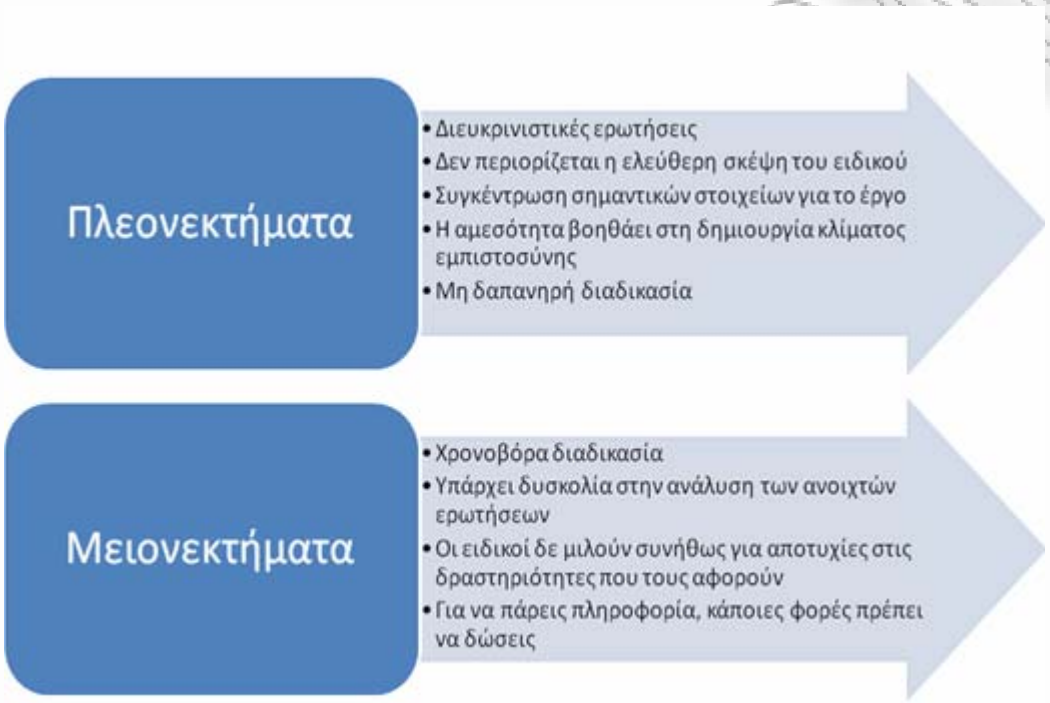
2. Συνεντεύξεις

Οι συνεντεύξεις του προσωπικού υποστήριξης του συστήματος και του διοικητικού προσωπικού του οργανισμού μπορούν να παράσχουν στα άτομα που πραγματοποιούν την αξιολόγηση των κινδύνων χρήσιμες πληροφορίες για την αξία και την αποστολή του νέου συστήματος, καθώς και τις αντιδράσεις των στελεχών στην εισαγωγή νέων τεχνολογιών [16]. Οι συνεντεύξεις αυτές θα βοηθήσουν επίσης στην κατανόηση των λειτουργικών χαρακτηριστικών του οργανισμού και στην αξιολόγηση του φυσικού περιβάλλοντος όπου θα εγκατασταθεί το νέο πληροφοριακό σύστημα.

Οι συνεντεύξεις αν και θεωρούνται ο πιο εύκολος τρόπος εντοπισμού κινδύνων ο ειδικός που αναλαμβάνει αυτές τις συνεντεύξεις θα πρέπει να διαθέτει ειδικές δεξιότητες. Οι πιθανοί υποψήφιοι για συνέντευξη είναι τα μέλη της ομάδας έργου, ανώτερα στελέχη με εμπειρία σε αντίστοιχα έργα και συγκεκριμένοι ενδιαφερόμενοι του έργου που θα μπορούσαν να αποκαλύψουν ειδικούς κινδύνους του έργου. Οι συνεντεύξεις μπορεί να είναι δομημένες ή όχι. Κατά τη διάρκεια μιας δομημένης συνέντευξης υπάρχουν συγκεκριμένες ερωτήσεις τις οποίες καλούνται να απαντήσουν οι ειδικοί. Στην αντίθετη περίπτωση της μη δομημένης συνέντευξης, διενεργείται μια ανοιχτή συζήτηση για το υπό υλοποίηση έργο. Φυσικά υπάρχει η δυνατότητα οι συνεντεύξεις να έχουν χαρακτηριστικά και από τους δύο τύπους καθώς αυτό βοηθάει περισσότερο στον εντοπισμό των

κινδύνων. Αφού ολοκληρωθούν οι συνεντεύξεις, αναλύονται από την ομάδα διαχείρισης κινδύνων, και προκύπτουν οι κίνδυνοι που αφορούν το έργο.

Η μέθοδος των συνεντεύξεων παρουσιάζει βασικά πλεονεκτήματα και μειονεκτήματα τα οποία αναλύονται στο Σχήμα 14:

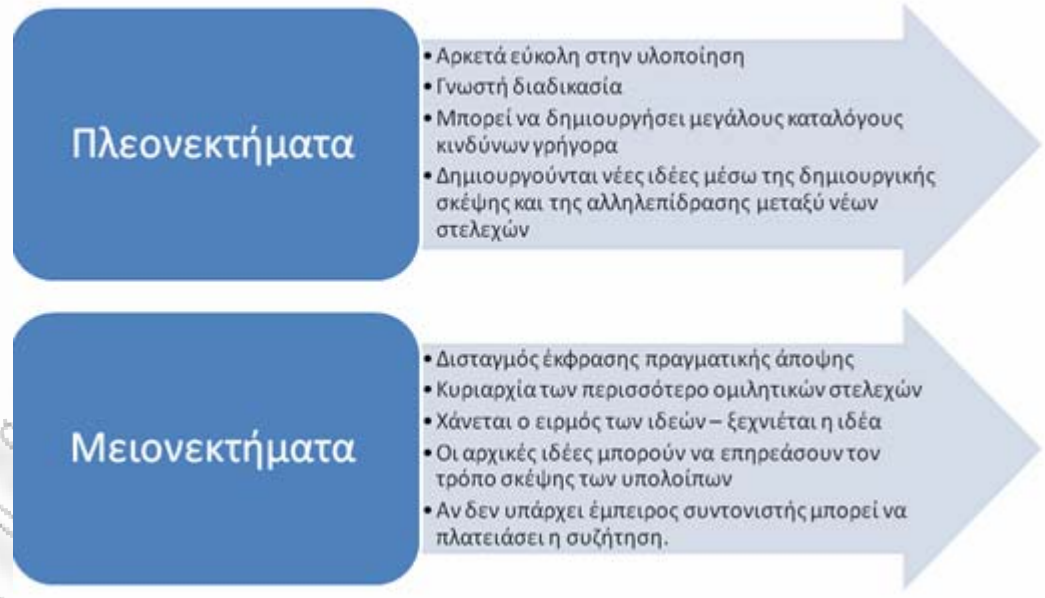


Σχήμα 14: Πλεονεκτήματα και μειονεκτήματα συνεντεύξεων

Υπάρχουν όμως προτεινόμενοι τρόποι για αντιμετώπιση των μειονεκτημάτων των συνεντεύξεων. Για παράδειγμα, μπορεί να αποφευχθούν τα μεγάλα χρονικά διαστήματα μεταξύ διαδοχικών συνεντεύξεων για να μην θεωρείτε τόσο χρονοβόρα διαδικασία. Επίσης, οι ανοιχτές ερωτήσεις θα πρέπει να είναι περιορισμένες και ουσιαστικές και όσο λιγότερο γενικές γίνεται. Επιπλέον, προτιμότερο είναι από τη στιγμή που οι ειδικοί δε μιλούν για αποτυχίες στις δραστηριότητες που τους αφορούν να προσπαθήσει ο ειδικός να μάθει από τους συνεντευξιαζόμενους για τις αποτυχίες των άλλων χωρίς φυσικά να κλονιστεί η εμπιστοσύνη του ειδικού στους άλλους. Τέλος, επειδή για να πάρεις πληροφορία κάποια στιγμή πρέπει να δώσεις, χρειάζεται ακεραιότητα στο χαρακτήρα του ειδικού για να μη μεταφερθούν εμπιστευτικές πληροφορίες, επειδή η αγορά είναι μικρή και αυτό θα μαθευτεί.

3. Ομαδική παραγωγή ιδεών

Η διεξαγωγή της μεθόδου βασίζεται στη δημιουργία ιδεών, την αναζήτηση πιθανών λύσεων για τα προβλήματα ή πιθανών ενισχύσεων για τις ευκαιρίες και την αποτίμηση της αποτελεσματικότητας των προτεινόμενων ενεργειών [17]. Πρόκειται για μια ελαφρώς δομημένη διαδικασία η οποία περιλαμβάνει την ανοιχτή συζήτηση μεταξύ μιας ομάδας στελεχών της επιχείρησης στην οποία εφαρμόζεται. Τα στελέχη που συμμετέχουν στην ομαδική παραγωγή ιδεών επιλέγονται σε βάση τη σχέση τους με το υπό εξέταση έργο και τις θεωρητικές αλλά και τις πρακτικές γνώσεις που διαθέτουν για το αντικείμενο. Το αποτέλεσμα της διαδικασίας είναι η δημιουργία ενός αναλυτικού καταλόγου κινδύνων που ενδεχομένως θα συμβούν και θα επηρεάσουν το έργο. Η αποτελεσματικότητα της μεθόδου οφείλεται κυρίως στο ότι η ομαδική σκέψη, είναι συνήθως πιο παραγωγική από την ατομική και επιπλέον η ιδέα ενός μέλους της ομάδας μπορεί να διεγείρει την ανάπτυξη περισσότερων σχετικών ιδεών από άλλα μέλη της ομάδας. Τέλος, η ομαδική παραγωγή ιδεών είναι η πλέον χρησιμοποιούμενη μέθοδος εντοπισμού κινδύνων, μετά τις συνεντεύξεις, καθώς μια δημιουργική και ελαφρώς δομημένη διαδικασία είναι κατάλληλη για να αντιμετωπίσει την ασταθή φύση των κινδύνων.



Σχήμα 15: Πλεονεκτήματα και μειονεκτήματα ομαδικής παραγωγής ιδεών

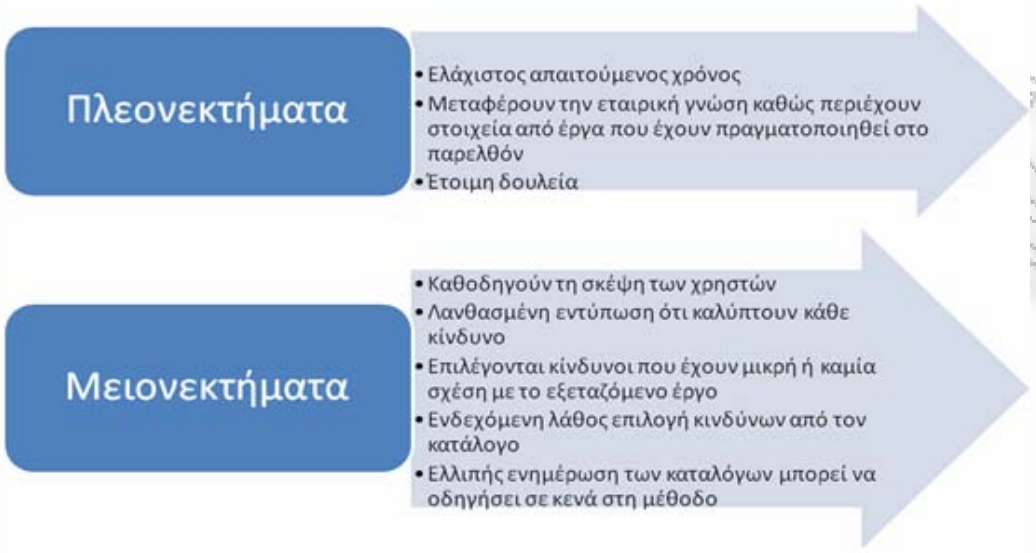
Ωστόσο, υπάρχουν και προτεινόμενοι τρόποι αντιμετώπισης των μειονεκτημάτων της μεθόδου ομαδικής παραγωγής ιδεών. Για παράδειγμα, η

ομάδα που θα δημιουργηθεί μπορεί να περιλαμβάνει στελέχη του ίδιου ιεραρχικού επιπέδου. Επίσης, ο συντονιστής θα πρέπει να ενθαρρύνει τους συμμετέχοντες που δεν είναι τόσο δυνητικοί να εκφράσουν και να υποστηρίξουν τη γνώμη τους. Επιπλέον, για να μη ξεχνιέται η ιδέα και οι αρχικές ιδέες να μην επηρεάζουν τον τρόπο σκέψης των υπολοίπων, μπορεί να γίνει χρήση ηλεκτρονικής ομαδικής παραγωγής ιδεών. Τέλος, αν δεν υπάρχει έμπειρος συντονιστής προτείνεται να μην ακολουθείται η συγκεκριμένη μέθοδος εντοπισμού κινδύνων.

4. Κατάλογοι κινδύνων

Οι κατάλογοι των κινδύνων, περιέχουν κινδύνους που έχουν εμφανιστεί στο παρελθόν ή ενδέχεται να εμφανιστούν στο μέλλον. Μέσω αυτών των πληροφοριών μπορεί να χρησιμοποιηθεί η πρότερη πείρα σε παρόμοια έργα, ώστε να αποφευχθούν λάθη και παραλήψεις του παρελθόντος και να σχηματιστεί μια πιο ρεαλιστική εικόνα των τρόπων αντιμετώπισης των επιπτώσεων.

Ωστόσο, οι κίνδυνοι και οι ενέργειες αντιμετώπισης δεν είναι σταθεροί, διότι αφ ‘ ενός κάθε έργο είναι μοναδικό και αφ ‘ ετέρου το περιβάλλον στο οποίο εκτελούνται τα έργα είναι δυναμικό, επομένως, σε κάθε νέο έργο μπορούν να εμφανιστούν νέοι κίνδυνοι ή να χρησιμοποιηθούν εναλλακτικές ενέργειες αντιμετώπισης για γνωστούς κινδύνους. Η αξιοπιστία των αποτελεσμάτων της μεθόδου εξαρτάται άμεσα από την τακτική ενημέρωση των καταλόγων με τους νέους κινδύνους και τις ενέργειες αντιμετώπισης. Η αξία αυτού του πορίσματος είναι πολύ μεγάλη καθώς δεν περιλαμβάνει την προσωπική άποψη των στελεχών του οργανισμού, που μπορεί να μην είναι απόλυτα αντικειμενική, αλλά μόνο την καταγραφή γεγονότων με βάση την αμεροληψία και τη διορατικότητα των εμπειρογνωμόνων.



Σχήμα 16: Πλεονεκτήματα και μειονεκτήματα κατάλογων κινδύνων

Ενδεχόμενοι τρόποι αντιμετώπισης των μειονεκτημάτων της μεθόδου καταλόγου κινδύνων είναι η παράλληλη εφαρμογή της μεθόδου με κάποια άλλη μέθοδο ούτως ώστε να μη καθοδηγείται η σκέψη των χρηστών και να μη δίνεται λανθασμένη εντύπωση ότι καλύπτει κάθε πιθανό κίνδυνο. Επίσης, για να επιλέγονται κίνδυνοι οι οποίοι έχουν σχέση με το εξεταζόμενο έργο, πρέπει να αναθεωρείτε συχνά ο κατάλογος των κινδύνων με το στάδιο της ανάλυσης και να διατηρείται στην επιχείρηση ένα σύστημα διαχείρισης γνώσεων κινδύνων έργων. Τέλος, όταν είναι γνωστό ότι η ομάδα δεν είναι έμπειρη και δε μπορεί να χρησιμοποιηθεί εξωτερικός σύμβουλος, προτείνεται η χρησιμοποίηση πάνω από μιας μεθόδου εντοπισμού κινδύνων.

5. Δομή ανάλυσης κινδύνων

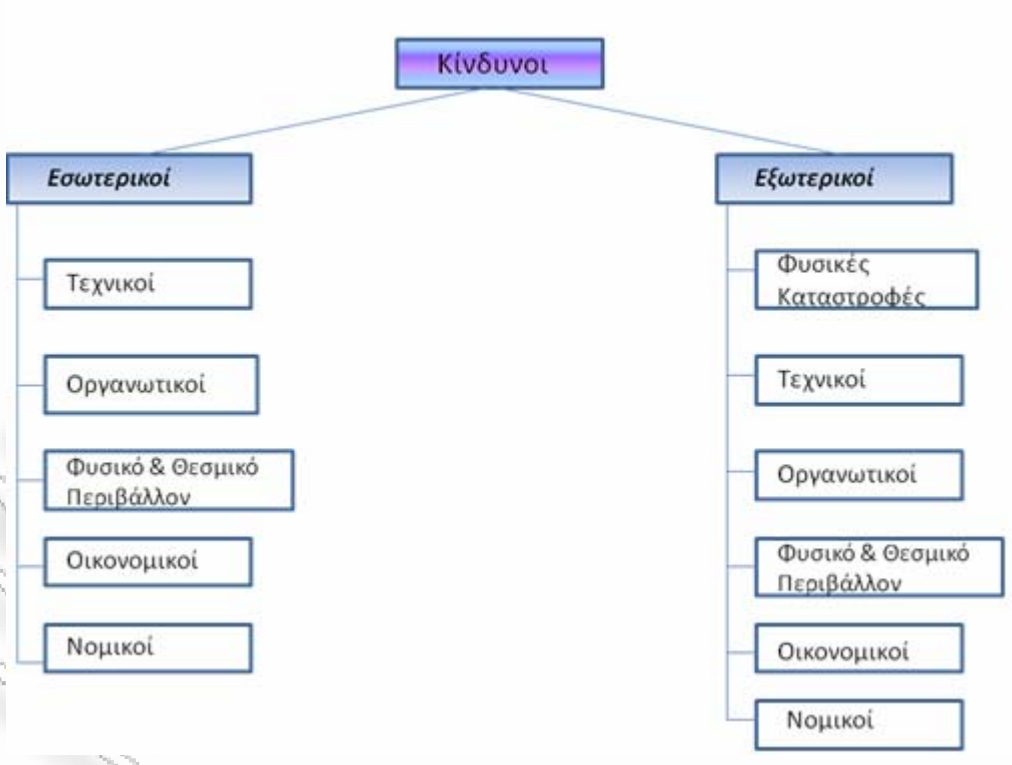
Το αποτέλεσμα των μεθόδων εντοπισμού κινδύνων είναι συνήθως κάποιοι μη δομημένοι κατάλογοι κινδύνων σχετικά με το έργο. Σε αυτούς τους καταλόγους, οι κίνδυνοι παρουσιάζονται μεμονωμένοι, δεν προσδιορίζονται πιθανά πλαίσια εμφάνισης τους και δε δίνεται η γενική εικόνα των κινδύνων που απειλούν το έργο. Γι αυτό το λόγο, είναι χρήσιμη η δημιουργία μιας δομημένης μορφής, έτσι ώστε ο πιθανός συσχετισμός των κινδύνων να διακρίνεται ευκολότερα και η ομάδα που

προσπαθεί να εντοπίσει τους κινδύνους να μην περιορίζεται σε συγκεκριμένους κινδύνους αλλά δε ομάδες κινδύνων.

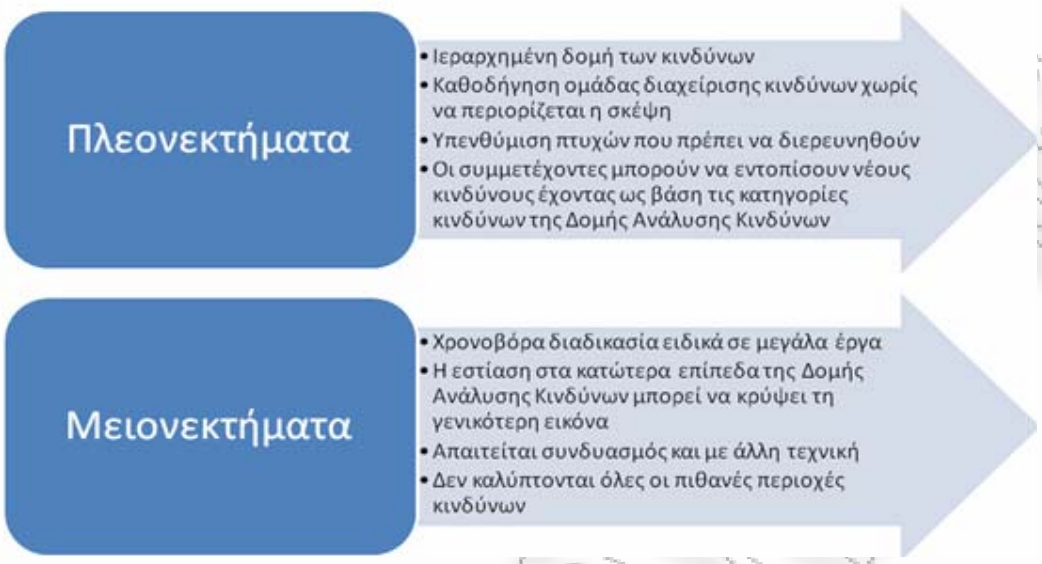
Χαρακτηριστικό παράδειγμα δομημένης μορφής στη διαχείριση έργων είναι η Δομή Ανάλυσης Εργασιών (Work Breakdown Structure – WBS). Οι περιοχές κινδύνων ενός έργου μπορούν να δομηθούν με όμοιο τρόπο και να σχηματίσουν τη Δομή Ανάλυσης Κινδύνων (Risk Breakdown Structure - RBS).

Ουσιαστικά, η δομή ανάλυσης κινδύνων αποτελεί τη βάση για τον εντοπισμό των κινδύνων, μέσω της εστίασης σε συγκεκριμένες πηγές κινδύνων και έχει σαν αποτέλεσμα το σχηματισμό ενός δομημένου κατά κατηγορία καταλόγου κινδύνων. Η Δομή Ανάλυσης Κινδύνων ορίζεται ως μια ιεραρχική οργάνωση των πηγών κινδύνου ενός έργου, κάθε χαμηλότερο επίπεδο της οποίας περιγράφει και μια ειδική ομάδα κινδύνων [18].

Η Δομή ανάλυσης κινδύνων μπορεί να έχει πολλά επίπεδα μέχρι να καταλήξει στο τελικό – κατώτερο επίπεδο. Αν σε αυτό το επίπεδο εισαχθούν οι κίνδυνοι που έχουν εντοπιστεί από άλλες μεθόδους, μπορούμε να ελέγξουμε αν έχουν ληφθεί υπόψη όλες οι περιοχές κινδύνων ή αν υπάρχουν κενά και παραλείψεις.



Σχήμα 17: Τυπική Δομή Ανάλυσης Κινδύνων (Risk Breakdown Structure)



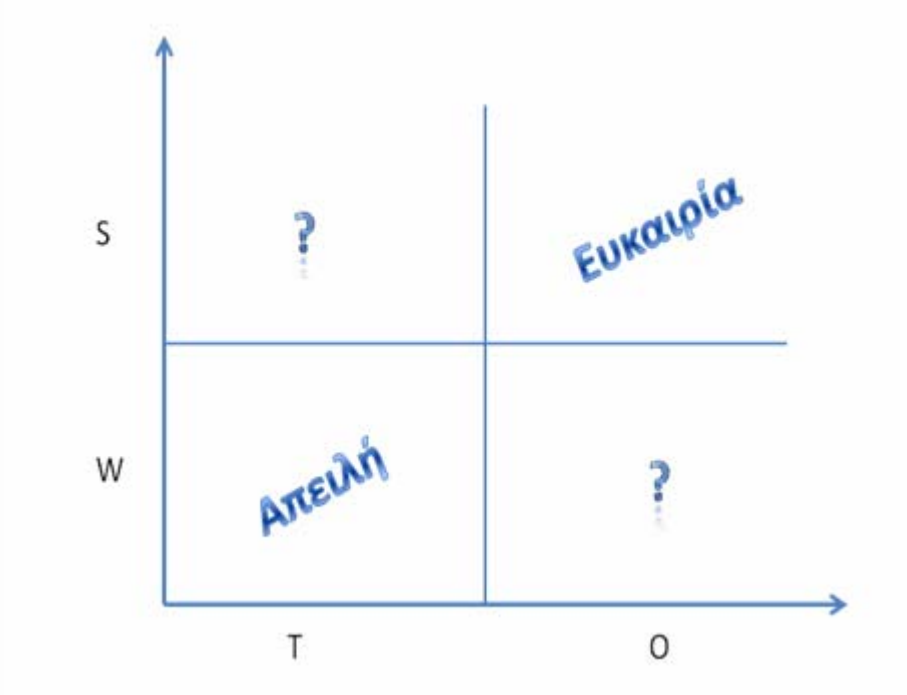
Σχήμα 18: Πλεονεκτήματα και μειονεκτήματα δομής ανάλυσης κινδύνων

Ενδεικτικοί τρόποι αντιμετώπισης των μειονεκτημάτων της μεθόδου Δομής Ανάλυσης Κινδύνων είναι αρχικά η χρησιμοποίηση διαφορετικών στελεχών για κάθε κατηγορία κινδύνων για την αποφυγή της χρονοβόρας διαδικασίας. Επίσης, για να μη κρύβεται η γενικότερη εικόνα του έργου μπορεί να χρησιμοποιηθεί ο πίνακας Δομής Ανάλυσης Έργου με τη Δομή Ανάλυσης Κινδύνων για να εξεταστεί αν έχει παραληφθεί κάποια από τις φάσεις ή κύριες δραστηριότητες του έργου. Τέλος, επειδή σαν μέθοδος δε μπορεί να καλύψει όλες τις πιθανές περιοχές κινδύνων προτείνεται η χρησιμοποίηση επιπλέον μεθόδου εντοπισμού κινδύνων.

6. Ανάλυση SWOT

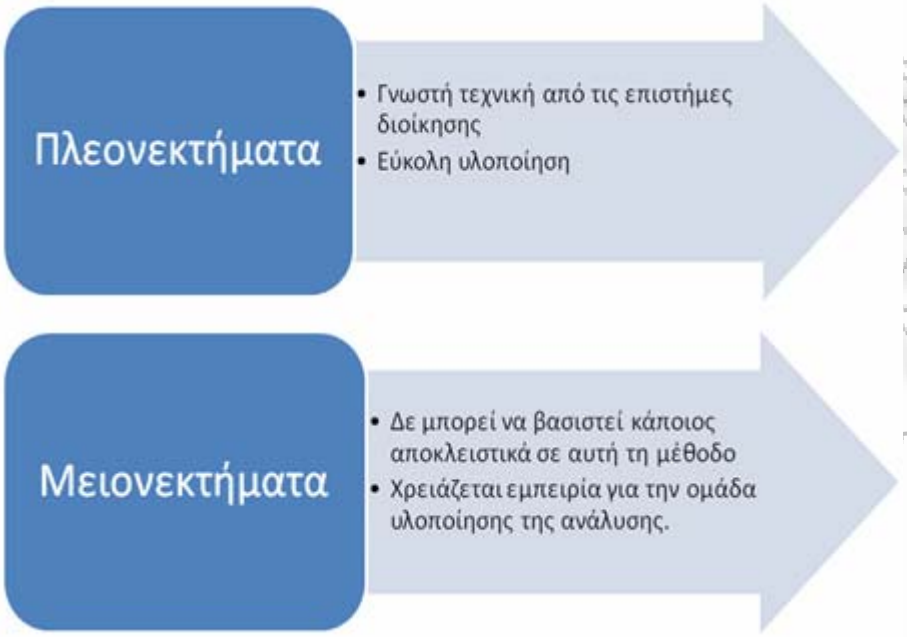
Η SWOT (**S**trengths, **W**eaknesses, **O**pportunities, **T**hreats) [19] εστιάζει στις Δυνάμεις, Αδυναμίες, Ευκαιρίες και Απειλές για το υπό εξέταση έργο. Πρόκειται για μια αρκετά γνωστή τεχνική στο χώρο της διοίκησης επιχειρήσεων η οποία μπορεί να φέρει αρκετά καλά αποτελέσματα όταν χρησιμοποιηθεί για τον εντοπισμό των κινδύνων. Οι δυνατότητες και οι αδυναμίες λοιπόν μιας επιχείρησης, αποτελούν συνήθως αιτίες για κινδύνους, οι οποίες προκύπτουν μέσα από την ανάλυση ευκαιριών και απειλών. Πρόκειται για μια συστηματοποιημένη διαδικασία, η οποία μπορεί να υλοποιηθεί είτε από ένα άτομο είτε από μια ομάδα ατόμων. Η εκτέλεση σε ομάδες συνίσταται γιατί δίνει καλύτερα αποτελέσματα και με μεγαλύτερη

ακρίβεια. Ταυτόχρονα, ελαττώνει την επίδραση της πολιτικής βούλησης, ή των προσωπικών προκαταλήψεων στα αποτελέσματα της ανάλυσης. Η ομάδα που εκτελεί την ανάλυση εντοπίζει αρχικά τα δυνατά και αδύνατα σημεία (αιτίες) της επιχείρησης και με βάση αυτά προσπαθεί να εντοπίσει απειλές και ευκαιρίες (κινδύνους). Η σύνδεση των κινδύνων που προκύπτουν με τους στόχους του έργου (συνέπειες) οδηγούν στο σχηματισμό ολοκληρωμένης αλυσίδας (αιτία – κίνδυνος – συνέπεια).



Σχήμα 19: Απειλές και ευκαιρίες από την ανάλυση SWOT

Επειδή το περιβάλλον στο οποίο εκτελούνται τα έργα είναι δυναμικό, ένα γεγονός που αντιμετωπίζεται ως απειλή σήμερα, μπορεί να είναι ευκαιρία στο μέλλον, ενώ ταυτόχρονα μπορούν να εμφανιστούν νέοι κίνδυνοι ή να εξαλειφθούν υπάρχοντες. Οπότε, η ανάλυση πρέπει να επαναλαμβάνεται τακτικά, διαφορετικά τα αποτελέσματα ενδέχεται να είναι αναξιόπιστα και επικίνδυνα.



Σχήμα 20: Πλεονεκτήματα και μειονεκτήματα της ανάλυσης SWOT

Τέλος, μια πρόταση για το μετριασμό των μειονεκτημάτων της μεθόδου, είναι η επιλογή εναλλακτικής μεθόδου εντοπισμού κινδύνων για διασταύρωση των αποτελεσμάτων ακόμα και αν η ομάδα διαχείρισης κινδύνων θεωρείτε εξαιρετικά έμπειρη.

7. Ανασκόπηση Εγγράφων

Η ανασκόπηση εγγράφων, θεωρείται καταχρηστικά μέθοδος εντοπισμού κινδύνων. Δε χρειάζεται κανενός είδους ειδική κατάρτιση, αλλά εμπειρία σχετικά με τα νομικά, συνήθως προβλήματα που ελλοχεύουν μέσα σε όχι εντελώς σαφείς συμβάσεις. Στόχος της ανασκόπησης εγγράφων είναι ο εντοπισμός «σκοτεινών» σημείων στις συμβάσεις ή στις απαιτήσεις του πελάτη ή σε οποιοδήποτε άλλο έγγραφο, όπου μπορεί να περιγράφονται δεσμεύσεις που δεν είναι ξεκάθαρες και στα δύο συμβαλλόμενα μέρη. Χαρακτηριστικό παράδειγμα αποτελούν, πολιτικά έγγραφα (νομοθεσία, κρατικές οδηγίες), έγγραφα σχετικά με το σύστημα (οδηγός χρήσης, διοικητικό εγχειρίδιο συστημάτων, σχέδιο του συστήματος και κατάλογος απαιτήσεων, τίτλοι ιδιοκτησίας) και έγγραφα σχετικά με την ασφάλεια (προηγούμενη έκθεση λογιστικού ελέγχου και αξιολόγησης κινδύνου, αποτελέσματα δοκιμής συστημάτων, σχεδιασμός ασφαλείας συστημάτων,

διαδικασίες ασφαλείας) που μας παρέχουν αρκετές και σημαντικές πληροφορίες για το σχηματισμό μιας άρτιας εικόνας του οργανισμού και της αξίας και λειτουργικότητας του νέου έργου για αυτόν. Βασικό πλεονέκτημα της μεθόδου είναι ότι χρειάζεται εμπειρία από τα στελέχη, χωρίς όμως ειδική εξειδίκευση, πέραν των γνώσεων που έχουν αποκομιστεί λόγω εμπειρίας. Αντίθετα, βασικό μειονέκτημα, είναι ο αρκετός χρόνος που απαιτείται για μια σε βάθος ανάλυση.

8. Μέθοδος Δελφών(Delphi)

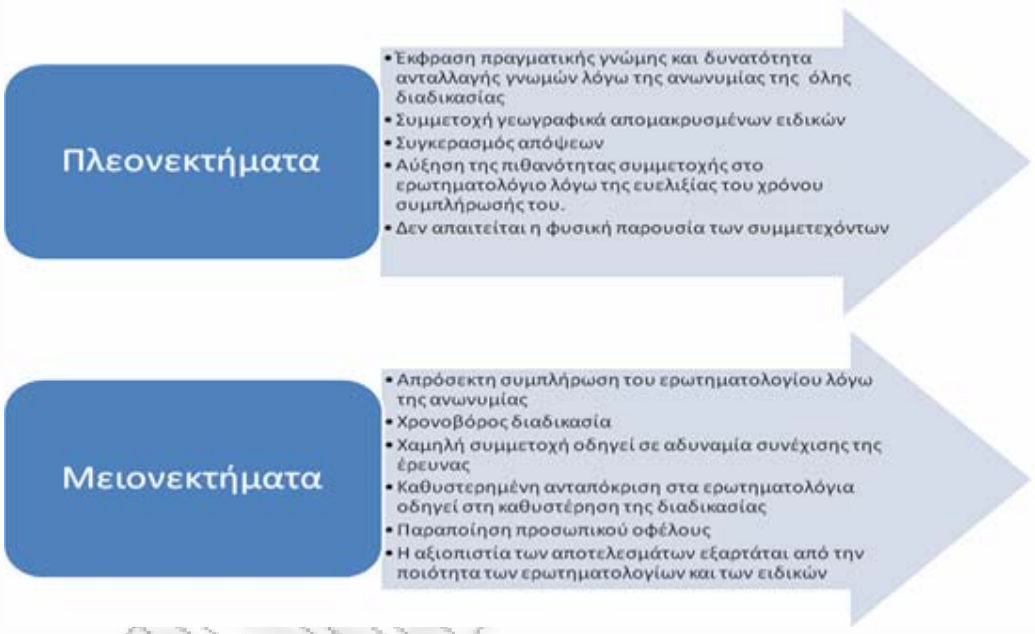
Η μέθοδος των Δελφών χρησιμοποιείται για να καταλήξει σε μια ανεξάρτητη και κοινή άποψη μέσα σ ΄ ένα σύνολο απαντήσεων διαφορετικών ειδικών, σε συγκεκριμένο ερώτημα. Είναι ίσως, η πιο γνωστή μέθοδος, στην οποία χρησιμοποιείται η κρίση ομάδων ειδικών, πλην όμως δεν εφαρμόζεται συχνά καθώς παρουσιάζει ειδικές δυσκολίες. Η μέθοδος Δελφών ορίζεται ως «μέθοδος για την οργάνωση μιας διαδικασίας επικοινωνίας, ώστε μια ομάδα να μπορεί να αντιμετωπίζει ένα πολύπλοκο πρόβλημα με αποτελεσματικό τρόπο» [20].

Η μέθοδος περιλαμβάνει τη συλλογή κρίσεων για κάποιο συγκεκριμένο θέμα, μέσω κατάλληλα σχεδιασμένων ερωτηματολογίων, από ανώνυμους και απομονωμένους συμμετέχοντες. Η βασική ιδέα της μεθόδου είναι εξάλειψη της προσωπικής επαφής, ώστε οι συμμετέχοντες να σκέφτονται ελεύθερα και χωρίς τους περιορισμούς που εμφανίζονται στις ομάδες. Η μέθοδος, προσπαθεί να αντλήσει τη γνώση και την εμπειρία πολλών ειδικών ταυτόχρονα πάνω στο εξεταζόμενο θέμα. Ωστόσο, αποτελείται από δύο έως πέντε επαναλήψεις, με επικρατέστερο αριθμό επαναλήψεων τις δύο ή τρεις. Σε κάθε επανάληψη, σχεδιάζεται και αποστέλλεται ένα ερωτηματολόγιο, και κατόπιν συλλέγονται και αναλύονται τα αποτελέσματα. Τελική επιδίωξη της μεθόδου, είναι η επίτευξη μιας γενικής συναίνεσης μεταξύ των συμμετεχόντων, η οποία είναι και το τελικό αποτέλεσμα.

Τα βήματα που ακολουθούνται στη μέθοδο των Δελφών είναι τα εξής:

- Εντοπισμός του προς επίλυση προβλήματος
- Σχεδιασμός του ερωτηματολογίου του οποίου οι απαντήσεις οδηγούν θεωρητικά στη λύση του προβλήματος ή στη λήψη απόφασης

- Υποβολή ερωτηματολογίου στους ειδικούς
- Συλλογή απαντήσεων και διαχωρισμός μεταξύ τους ανάλογα με την απόκλιση που έχουν από το σύνολο
- Οι ειδικοί που έδωσαν τις αποκλίνουσες απαντήσεις καλούνται να εξηγήσουν τη θέση τους και οι συγκεκριμένες ερωτήσεις αναδιαμορφώνονται
- Επανεκτίμηση ερωτημάτων από ειδικούς
- Επανάληψη των βημάτων μέχρις ότου βρεθεί μια κοινή συνισταμένη των απόψεων.



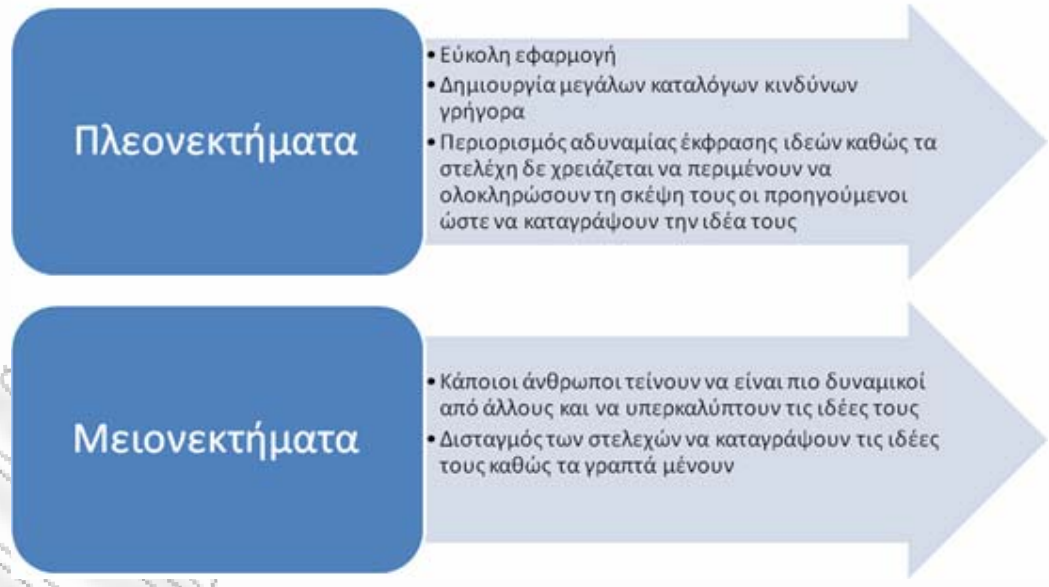
Σχήμα 21: Πλεονεκτήματα και μειονεκτήματα της μεθόδου Δελφών

Εξαιτίας της δυσκολίας εφαρμογής αλλά και των ιδιαίτερων ικανοτήτων που απαιτούνται από τη συγκεκριμένη εφαρμογή η χρήση της είναι περιορισμένη. Για την αντιμετώπιση των μειονεκτημάτων της, προτείνεται αρχικά η χρήση της μερικής ανωνυμίας. Για παράδειγμα, ο οργανωτής της μεθόδου, γνωρίζει τους συμμετέχοντες και τις απόψεις τους, οι συμμετέχοντες όμως δε γνωρίζουν ποια απάντηση έδωσε ποιος. Επίσης, πολύ σημαντικό είναι η έμφαση στο σχεδιασμό του ερωτηματολογίου (εύκολο και γρήγορο) ώστε να χρειαστούν οι ελάχιστες δυνατές επαναλήψεις. Επίσης, πρέπει να βρεθούν κίνητρα για τους συμμετέχοντες ώστε να

πειστούν να απαντήσουν σύντομα και να μην έχουμε καθυστέρηση της όλης διαδικασίας. Επιπλέον, για να μην υπάρχει χαμηλή συμμετοχή πρέπει να επιλεγούν συμμετέχοντες οι οποίοι ενδιαφέρονται για το συγκεκριμένο ερωτηματολόγιο καθώς επίσης και οι ειδικοί πρέπει να επιλεγούν με αντικειμενικά κριτήρια. Τέλος, για να μην υπάρχουν παραποιήσεις πρέπει να επιλεγεί ένας οργανωτής ο οποίος να μην έχει λόγο να προβεί σε παραποιήσεις (π. χ κάποιος που δεν ενδιαφέρεται για το έργο).

9. Ειδικές Ομάδες

Η τεχνική των ειδικών ομάδων είναι σχεδόν ίδια με την ομαδική παραγωγή ιδεών, με την ουσιαστική διαφορά ότι οι συμμετέχοντες δεν έχουν προφορική επικοινωνία. Κάθε ένας από τους συμμετέχοντες καταγράφει τις ιδέες του σε συγκεκριμένη φόρμα [20]. Αφού όλοι οι συμμετέχοντες ολοκληρώσουν την καταγραφή των ιδεών τους, οι φόρμες δίνονται στον οργανωτή ο οποίος και διαβάζει τις ιδέες αφήνοντας χρόνο για τη συζήτησή τους. Υποστηρίζεται ότι εκτός από του μεγαλύτερου αριθμού ιδεών που παράγονται με αυτόν τον τρόπο, παράγονται και ιδέες καλύτερης ποιότητας από την ομαδική παραγωγή ιδεών.



Σχήμα 22: Πλεονεκτήματα και μειονεκτήματα ειδικών ομάδων

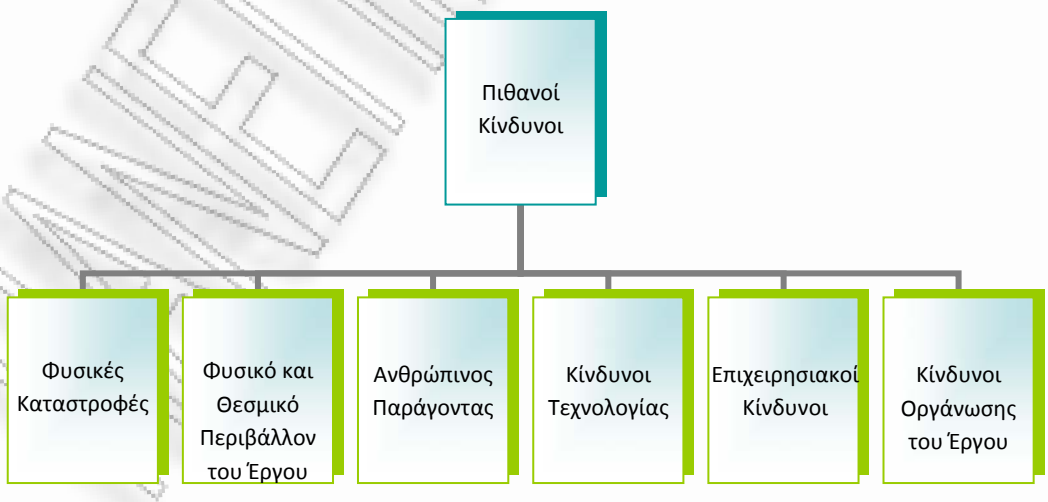
Τέλος, για το μετριασμό των μειονεκτημάτων της μεθόδου των ειδικών ομάδων προτείνεται ο συντονιστής να ενθαρρύνει τους συμμετέχοντες που δεν είναι τόσο δυναμικοί να εκφράσουν και να υποστηρίξουν τις ιδέες τους, καθώς επίσης για την

αποφυγή των δισταγμών των στελεχών στην καταγραφή των ιδεών τους προτείνεται να χρησιμοποιούνται ανώνυμες φόρμες ώστε να μη φαίνονται άμεσα οι ιδέες των στελεχών.

4.4 Αναγνώριση Απειλών

Αφού ολοκληρώθηκε το πρώτο βήμα και έχουν συλλεχθεί όλες οι απαραίτητες πληροφορίες προχωράμε στο δεύτερο βήμα της διαδικασίας εκτίμησης κινδύνων που δεν είναι άλλο από την αναγνώριση των απειλών των πιθανών κινδύνων. Τα πρόσωπα που θα κληθούν να συμπληρώσουν τον κατάλογο των πιθανών απειλών θα πρέπει εκτός από τις αναγκαίες γνώσεις και την εμπειρία, να διαθέτουν και πλούσια φαντασία και διορατικότητα ώστε να μπορέσουν να διακρίνουν και κινδύνους πέραν των τυποποιημένων. Φυσικά, καθώς η εκτίμηση κινδύνων είναι μια επιστημονική διαδικασία δε μπορεί να βασιστεί μόνο στη φαντασία αυτών που την πραγματοποιούν, αλλά απαιτεί ένα συνδυασμό όλων των παραπάνω για να επέλθει το επιθυμητό αποτέλεσμα. Για το λόγο αυτό είναι χρήσιμο να στελεχωθεί μία ομάδα κατάλληλων προσώπων που θα επιτελέσουν αυτή τη διαδικασία και όχι να ανατεθεί ως ευθύνη ενός μόνο προσώπου.

Οι πιθανοί κίνδυνοι μπορούν να κατηγοριοποιηθούν ανάλογα με την προέλευσή τους [15]. Στο Σχήμα 23 φαίνονται οι πιθανοί κίνδυνοι, στα πλαίσια των οποίων θα αναζητηθούν παρακάτω οι πιθανές απειλές ενός πληροφοριακού συστήματος.



Σχήμα 23: Κατηγορίες πιθανών κινδύνων

- ***Φυσικές καταστροφές***

Η πρώτη κατηγορία κινδύνων στους οποίους μπορεί να εκτεθεί ένα πληροφοριακό έργο είναι οι φυσικές καταστροφές. Τέτοιου είδους καταστροφές θα μπορούσαν να προσβάλλουν το οποιοδήποτε έργο και όχι μόνο κάποιο πληροφοριακό, καθώς ουσιαστικά προσβάλλουν τις κτιριακές εγκαταστάσεις του οργανισμού και εμμέσως και τα πληροφοριακά συστήματα που στεγάζονται σε αυτές.

Στην κατηγορία αυτή ανήκουν οι σεισμοί, οι πλημμύρες, οι καθιζήσεις του εδάφους, οι χιονοθύελλες και άλλα τέτοιου είδους φυσικά φαινόμενα. Η κατηγορία αυτή είναι φυσικά κάπως πιο ιδιόμορφη καθώς εξαρτάται και από τη γεωγραφική θέση της εκάστοτε εγκατάστασης. Μια πιο λεπτομερής περιγραφή των εν λόγω κινδύνων δε κρίνεται αναγκαία καθώς είναι προφανής ο τρόπος με τον οποίο μπορούν να προσβάλλουν την άρτια εξέλιξη του έργου.

- ***Φυσικό και θεσμικό περιβάλλον του έργου***

Η δεύτερη κατηγορία αναφέρεται στο περιβάλλον του έργου. Με τον όρο περιβάλλον αναφερόμαστε στις εγκαταστάσεις του οργανισμού, στις γειτονικές προς αυτόν εγκαταστάσεις και στις κρατικές παροχές.

Ας εξετάσουμε πρώτα τις εγκαταστάσεις του ίδιου του οργανισμού. Ένας πρώτος εχθρός του πληροφοριακού έργου είναι η παλαιότητα των εγκαταστάσεων. Τα προβλήματα που μπορούν να προέλθουν από αυτήν επικεντρώνονται κυρίως στο δίκτυο υδροδότησης και ηλεκτροδότησης. Ένας παλιός σωλήνας, που θα μπορούσε να χρησιμοποιείται ακόμα και για τη θέρμανση του χώρου, ο οποίος δεν έχει συντηρηθεί σωστά, μπορεί να καταστρέψει τον εξοπλισμό του υπό ανάπτυξη συστήματος εάν σπάσει και τα νερά βρουν πρόσβαση προς το δωμάτιο όπου αυτός φυλάσσεται ή έχει ήδη εγκατασταθεί. Η ηλεκτροδότηση παίζει εξίσου σημαντικό ρόλο, καθώς οι ατέλειες σε αυτή μπορούν να προκαλέσουν ένα βραχυκύκλωμα με καταστροφικές συνέπειες, όπως μία πυρκαγιά ή να τεθεί το σύστημα εκτός λειτουργίας για κάποιο χρονικό διάστημα. Η απρόβλεπτη πτώση του συστήματος ενδέχεται να επιφέρει απώλεια σημαντικών δεδομένων, καταστροφή μέρους του hardware και του software, αλλά και χρηματικές απώλειες από τη μη λειτουργία του

συστήματος έστω και για λίγες ώρες. Επίσης θα ήταν απογοητευτικό να ολοκληρωθεί ένα μέρος του συστήματος και να μη μπορεί να τεθεί σε λειτουργία λόγω έλλειψης ισχύος.

Οι γειτονικές εγκαταστάσεις και γενικά ο περιβάλλον χώρος του οργανισμού θα μπορούσαν εμμέσως να αποτελέσουν απειλή για το νέο πληροφοριακό έργο. Ένα προφανές παράδειγμα αποτελεί η εκδήλωση πυρκαγιάς σε γειτονικό κτίσμα που θα μπορούσε να επεκταθεί και στις εγκαταστάσεις του οργανισμού. Για αυτό το λόγο σημαντική είναι και η επιλογή της θέσης μέσα στην εγκατάσταση όπου θα τοποθετηθεί το νέο σύστημα.

Με τον όρο κρατικές παροχές αναφερόμαστε σε όλες εκείνες διαδικασίες του οργανισμού τις οποίες επηρεάζει ο κρατικός παράγοντας. Πρώτα από όλα είναι το νομικό πλαίσιο που καθορίζει τις διαδικασίες του οργανισμού, την τήρηση βάσεων δεδομένων και τη ροή πληροφοριών. Το αναπτυσσόμενο έργο πληροφορικής θα πρέπει να υπακούει στις νομοθετικές ρυθμίσεις έτσι ώστε να μπορεί να χρησιμοποιηθεί και να μην επιβληθούν κυρώσεις στον οργανισμό από τη μη εξουσιοδοτημένη χρήση συστημάτων και ούτε να καθυστερήσει η ολοκλήρωση του έργου από αλλαγές που θα το συμμορφώνουν με την υπάρχουσα νομοθεσία. Επιπροσθέτως στις κρατικές παροχές περιλαμβάνονται και οι τεχνολογίες οι οποίες μπορεί να υποστηριχθούν αλλά και τα σχέδια του κράτους για εκσυγχρονισμό, για παράδειγμα των δικτύων ροής πληροφορίας. Μια νέα τεχνολογία, που έχει εξαιρετικές δυνατότητες, αλλά δε μπορεί ουσιαστικά να τεθεί σε εφαρμογή λόγω έλλειψης κρατικής υποδομής, όπως η ύπαρξη και χρήση παλαιών δικτύων μικρής χωρητικότητας, θα ήταν ουσιαστικά άχρηστη και η εισαγωγή της στο νέο σύστημα μόνο επιζήμια θα μπορούσε να χαρακτηριστεί. Στην αντίπερα όχθη, εάν τα κρατικά σχέδια για εισαγωγή νέων τεχνολογιών δε ληφθούν υπόψιν, υπάρχει ο κίνδυνος να μη χρησιμοποιηθούν τελικά τα βέλτιστα συστήματα στην υλοποίηση του νέου έργου με αποτέλεσμα το νέο έργο λογισμικού να θεωρηθεί απαρχαιωμένο, ακόμα και από την έναρξη της λειτουργίας του.

- ***Ανθρώπινος παράγοντας***

Η επόμενη πηγή κινδύνων είναι ο ανθρώπινος παράγοντας. Αυτή αναφέρεται σε άτομα που σκόπιμα θα προσπαθήσουν να βλάψουν τη λειτουργία του συστήματος ή να την εκμεταλλευτούν για προσωπικό τους όφελος ζημιώνοντας τον οργανισμό στον οποίο ανήκουν. Τέτοια πρόσωπα μπορεί να ανήκουν στο προσωπικό του οργανισμού ή να είναι πρόσωπα που δεν ανήκουν σε αυτόν, αλλά μπορούν να αποκτήσουν πρόσβαση στα πληροφοριακά του συστήματα.

Τα πρόσωπα που δεν ανήκουν στον οργανισμό και επιθυμούν τη ζημίωση αυτού είναι κυρίως οι ανταγωνιστές του. Αυτοί ενδεχομένως να προσπαθήσουν να αποκτήσουν πρόσβαση στις βάσεις δεδομένων του νέου συστήματος και να αντλήσουν πληροφορίες για το προσωπικό, για μελλοντικές στρατηγικές, για καινοτομίες του οργανισμού ή για άλλου είδους αποθηκευμένες πληροφορίες, προσβάλλοντας με αυτόν τον τρόπο την αξιοπιστία, την ακεραιότητα και την εμπιστευτικότητα του έργου. Με αυτόν τον τρόπο η εταιρία μπορεί να απολέσει ευκαιρίες αιφνιδιασμού της αγοράς, ενδεχομένως το μονοπώλιο της, να χαλάσουν μελλοντικές συνεργασίες που βρίσκονταν υπό συζήτηση ή ακόμα να χάσει στελέχη πολύτιμα για αυτήν που θα δελεαστούν από προτάσεις ανταγωνιστών που γνωρίζουν το βιογραφικό τους αλλά και την αξία τους για την ευδοκίμηση της εταιρίας. Επιπροσθέτως, οι εισβολείς θα μπορούσαν ακόμα και να εκβιάσουν τον οργανισμό, για τη μη κοινοποίηση των στοιχείων που καπηλεύτηκαν.

Πέραν της διαρροής πληροφοριών οι ανταγωνιστές που θα αποκτήσουν πρόσβαση στο λογισμικό του οργανισμού, μπορούν ακόμα και να το καταστρέψουν. Δολιοφθορές θα μπορούσαν να προκληθούν και στον τεχνικό εξοπλισμό του έργου όμως αυτή είναι μία ακραία κατάσταση και αναφέρεται πιο πολύ σε ειδικές περιπτώσεις. Και αφού αναφερθήκαμε σε ειδικές περιπτώσεις, μπορούμε εδώ να αναφέρουμε και τον κίνδυνο από επιθέσεις τρομοκρατών και αναρχικών προς το λογισμικό και το υλικό του οργανισμού. Όλα αυτά φυσικά με την προϋπόθεση ότι δεν υπάρχει η απαραίτητη ασφάλεια των δικτύων αλλά και των εγκαταστάσεων και ότι υπάρχει κίνητρο για τη διενέργεια τέτοιων επιθέσεων.

Μία άλλη μερίδα προσώπων, που θα μπορούσαν να πλήξουν το κύρος και την αξιοπιστία που αποπνέει το έργο, είναι οι hackers, οι οποίοι μπορούν να φέρουν αναστάτωση και να προκαλέσουν καταστροφές στο νέο σύστημα μόνο και μόνο για την προσωπική τους ικανοποίηση.

Πέραν όμως των παραπάνω, υπάρχουν και πρόσωπα που ανήκουν στο δυναμικό του οργανισμού, τα οποία θα μπορούσαν να θέσουν σε κίνδυνο την ακεραιότητα και την αξιοπιστία του έργου. Κίνητρο αυτών, η ικανοποίηση προσωπικών φιλοδοξιών, χρηματικά οφέλη ή ακόμα και η έκφραση της δυσαρέσκειάς τους προς τους διοικούντες του οργανισμού. Αναφερόμαστε σε στελέχη που είτε είναι εξουσιοδοτημένα να έχουν πρόσβαση σε ευαίσθητα δεδομένα και λογισμικό μεγάλης αξίας είτε μπορούν να αποκτήσουν τέτοια πρόσβαση σε τέτοια δεδομένα λόγω ελλιπούς ασφάλειας αυτών.

Τα στελέχη αυτά θα μπορούσαν να αποκρύψουν πληροφορίες ή να παραποιήσουν δεδομένα ώστε να παρουσιάζονται ως ιδιαίτερα ικανά για να εξελιχθούν στην ιεραρχία του οργανισμού δημιουργώντας προβλήματα στην τήρηση βάσης δεδομένων. Επίσης μπορούν να αποκαλύψουν πληροφορίες ή να καταστρέψουν δεδομένα και λογισμικό παρακινούμενοι και φυσικά πληρωμένοι από εξωτερικούς παράγοντες, όπως είναι οι ανταγωνιστές του οργανισμού. Τέλος, δυσαρεστημένοι υπάλληλοι από την εξέλιξή τους, τις αποδοχές τους ή τη συμπεριφορά των ανωτέρων τους προς αυτούς, ενδεχομένως να επιχειρήσουν να βλάψουν τη λειτουργία του οργανισμού προσβάλλοντας τη λειτουργία και την ανάπτυξη ενός τόσο ζωτικής σημασίας έργου.

Ολοκληρώνοντας αναφέρουμε τα πρόσωπα που είτε ανήκουν είτε όχι στο δυναμικό του οργανισμού θα προσπαθήσουν να εκμεταλλευτούν τα ευαίσθητα δεδομένα αυτού στα οποία θα έχουν τη δυνατότητα να αποκτήσουν πρόσβαση. Ενδεικτικά αναφέρουμε την πρόσβαση σε υλικό δικογραφιών, ιστορικό ασθενών ή περιουσιακά στοιχεία προσώπων, για περιπτώσεις που το νέο πληροφοριακό σύστημα ανήκει σε κάποιον από τους αντίστοιχους οργανισμούς της κρατικής μηχανής.

- ***Κίνδυνοι τεχνολογίας***

Η πρώιμη υιοθέτηση νέων τεχνολογιών προσφέρει ένα δυνατό πλεονέκτημα σε σχέση με τους ανταγωνιστές ενός οργανισμού, καθώς παρέχει μεγαλύτερη ταχύτητα, ασφάλεια και αξιοπιστία στις διαδικασίες του οργανισμού, καλύτερη λειτουργικότητα των συστημάτων, αλλά και ανοίγει το δρόμο για περαιτέρω

ανάπτυξη. Αποτελεί όμως και τη σημαντικότερη ίσως εστία κινδύνων που μπορούν να προσβάλλουν ένα πληροφοριακό έργο. Οι κίνδυνοι αυτοί χαρακτηρίζονται ως κίνδυνοι τεχνολογίας και αφορούν τις νέες τεχνολογίες που πρόκειται να εισαχθούν με την ολοκλήρωση του έργου και την προσαρμογή αυτών στα ήδη υπάρχοντα συστήματα του οργανισμού.

Η χρήση νέων τεχνολογιών, που δεν έχουν δοκιμαστεί και αξιολογηθεί σε πραγματικές συνθήκες, συνοδεύονται από τον κίνδυνο να αποδειχθούν, σε βάθος χρόνου, μη λειτουργικές, χωρίς σημαντικό επιχειρησιακό όφελος και ενδεχομένως επιζήμιες για το κύρος του οργανισμού. Τα νέα συστήματα που θα εισαχθούν μπορεί να μη μπορούν να ανταποκριθούν στις ανάγκες του οργανισμού, να αδυνατούν να παρακολουθήσουν τις λειτουργίες της αγοράς, ή απλά να αποδειχθούν ελαττωματικά. Οι κίνδυνοι αυτοί φυσικά, συνοδεύουν κάθε καινοτομία που εισάγεται στη λειτουργία ενός οργανισμού. Όταν όμως αναφερόμαστε σε ένα πληροφοριακό έργο μεγάλης κλίμακας, γίνεται αντιληπτό, πως η αποτυχία αυτού θα προκαλέσει τεράστια ζημιά στον οργανισμό εξαιτίας των κονδυλίων που θα χαθούν. Παράλληλα σε ένα τέτοιο έργο ένας οργανισμός μπορεί να έχει στηρίξει όλες τις προοπτικές ανάπτυξής του και με την αποτυχία αυτού να απολέσει κάθε δυνατότητα να παρουσιαστεί ανταγωνιστικός στον τομέα που ειδικεύεται.

Προσπαθώντας οι υπεύθυνοι σχεδιασμού του έργου να ελαχιστοποιήσουν τον παραπάνω κίνδυνο, μπορεί να προτιμήσουν τεχνολογίες που έχουν ήδη χρησιμοποιηθεί και έχει αποδειχθεί η λειτουργικότητά τους και οι υπηρεσίες που μπορεί να προσφέρει η υιοθέτησή τους. Εδώ όμως υπάρχει ο κίνδυνος αυτές οι τεχνολογίες, βραχυχρόνια να θεωρηθούν απαρχαιωμένες και να μη μπορούν παρακολουθήσουν τους ρυθμούς ανάπτυξης που απαιτούνται για να είναι η εταιρία ανταγωνιστική. Με την αντίθεση αυτών των δύο κινδύνων γίνεται φανερή η αναγκαιότητα της μελέτης διαχείρισης κινδύνων ώστε να προβλεφθεί, όσο αυτό είναι εφικτό, το επίπεδο τεχνολογίας που πρέπει να χρησιμοποιηθεί για να μεγιστοποιηθούν τα οφέλη του οργανισμού. Η διαχείριση κινδύνων θα πρέπει να προβλέψει ακόμα και αν η χρονική περίοδος είναι η κατάλληλη για την υλοποίηση ενός τέτοιου έργου, βάση των τεχνολογικών εξελίξεων που αναμένονται.

Ένας άλλος κίνδυνος που απειλεί ένα έργο πληροφορικής εξαιτίας της χρήσης νέων τεχνολογιών, είναι η μη συμβατότητα των νέων συστημάτων με τον ήδη υπάρχον εξοπλισμό. Δηλαδή θα πρέπει να μελετηθεί αν τα νέα συστήματα μπορούν να συνδεθούν και να εναρμονιστούν με τα υπάρχοντα συστήματα, να εκτιμηθεί το κόστος και ο χρόνος που απαιτείται για αυτήν τη σύνδεση, αλλά και να προσδιοριστούν οι τυχόν αντικαταστάσεις και αλλαγές που πρέπει να πραγματοποιηθούν στον υπάρχον εξοπλισμό. Η εκτίμηση αυτή είναι ιδιαίτερα σημαντική, καθώς είναι σαφές πως το νέο υλικό και λογισμικό δε θα πρέπει να καθιστά άχρηστη την τρέχουσα υποδομή, αλλά θα πρέπει να "συνεργάζεται" με αυτήν αρμονικά για να εξασφαλιστεί η ορθή και η όσο το δυνατόν αποδοτικότερη λειτουργία του οργανισμού.

Πέραν όμως των συνδέσεων με τα άλλα συστήματα του οργανισμού, θα πρέπει να προβλεφθεί και ο κίνδυνος μη συμβατότητας του εξοπλισμού του ίδιου του έργου. Καθώς θα πρόκειται για εντελώς νέες τεχνολογίες υπάρχει ο κίνδυνος τα διάφορα μέρη υλικού και λογισμικού να μη μπορούν να συνδεθούν απευθείας μεταξύ τους, αλλά να απαιτούνται ιδιόμορφες συνδεσμολογίες, που αν δεν έχουν προβλεφθεί και εισαχθεί στον αρχικό σχεδιασμό του έργου, θα μπορούσαν να το θέσουν εκτός χρονοδιαγράμματος αλλά και να αυξήσουν το κόστος υλοποίησης του. Παράλληλα όλες αυτές οι συνδεσμολογίες θα πρέπει να παρουσιάζουν ευελιξία σε τροποποιήσεις, που ενδεχομένως να χρειαστεί να πραγματοποιηθούν στο μέλλον.

- ***Επιχειρησιακοί κίνδυνοι***

Η επόμενη κατηγορία κινδύνων είναι οι επιχειρησιακοί κίνδυνοι. Οι κίνδυνοι αυτοί απορρέουν από τη διαδικασία επιχειρησιακής ένταξης των νέων τεχνολογιών στον τρόπο λειτουργίας του οργανισμού.

Υπάρχει ο κίνδυνος οι νέες τεχνολογίες να μη μπορούν να αφομοιωθούν άμεσα από τη λειτουργία του οργανισμού, με αποτέλεσμα το κάθε τμήμα του έργου που θα ολοκληρώνεται να καθυστερεί να τεθεί σε λειτουργία και να προκαλεί έτσι καθυστερήσεις και στην περαιτέρω εξέλιξη του έργου. Επίσης, θα πρέπει να υπάρχει εξ' αρχής σαφές πλάνο των διαδικασιών στις οποίες θα συμμετάσχουν τα

νέα συστήματα, έτσι ώστε η χρονική στιγμή της παράδοσης τους κάθε τμήματος να ταυτίζεται με τη στιγμή έναρξης της λειτουργίας τους και της αξιοποίησης των δυνατοτήτων τους. Ο κίνδυνος να ανευρίσκονται διαρκώς νέες ανάγκες που θα μπορούσαν να καλυφθούν από το νέο λογισμικό, λόγω πρόχειρου αρχικού σχεδιασμού, μπορεί να οδηγήσει σε καθυστερήσεις λόγω τροποποιήσεων της τελευταίας στιγμής αλλά και λόγω της αναζήτησης πλήρους τρόπου αξιοποίησης του έργου, όταν ήδη έχουν αρχίσει να ολοκληρώνονται τμήματα αυτού.

Κίνδυνος όμως στην επιχειρησιακή ένταξη των νέων τεχνολογιών μπορεί να προέλθει και από το επίπεδο εκπαίδευσης του προσωπικού. Είναι πολύ πιθανό το μεγαλύτερο μέρος του προσωπικού να μη μπορεί να χρησιμοποιήσει τα νέα συστήματα δημιουργώντας έτσι καθυστερήσεις, καθώς θα απαιτηθεί επιπλέον χρόνος για την εκπαίδευση αυτού, έτσι ώστε να είναι σε θέση να χειριστεί τα νέα συστήματα. Η εκπαίδευση του προσωπικού θα πρέπει να πραγματοποιηθεί πριν την ολοκλήρωση του έργου για να αποφευχθούν οι επιπλέον καθυστερήσεις. Επιπροσθέτως η διοίκηση του οργανισμού οφείλει να ελέγξει το επίπεδο εκπαίδευσης του προσωπικού της, για να προλάβει λάθος χειρισμούς, που θα μπορούσαν να δημιουργήσουν προβλήματα στη λειτουργία του πληροφοριακού έργου αλλά και να βλάψουν το κύρος του οργανισμού. Παράλληλα με αυτό τον έλεγχο και γνωρίζοντας τις δυνατότητες του προσωπικού της θα μπορεί να το τοποθετήσει στις κατάλληλες θέσεις για την καλύτερη δυνατή αξιοποίηση των δυνατοτήτων του έργου.

Πέραν όμως της εκπαίδευσης του προσωπικού σε θέματα τεχνολογίας, τα διάφορα στελέχη θα πρέπει να ενημερωθούν και να κατανοήσουν την αξία και την ευαισθησία του νέου συστήματος, ώστε να σεβαστούν και τη διαδικασία εκπαίδευσής τους αλλά και τις διαδικασίες ασφαλείας που συνοδεύουν το έργο. Η απείθαρχη συμπεριφορά του προσωπικού και η άρνηση προσαρμογής στις νέες συνθήκες θα μπορούσε να προκαλέσει σοβαρά προβλήματα στην ανάπτυξη και τη βιωσιμότητα του έργου.

- ***Κίνδυνοι οργάνωσης του έργου***

Η τελευταία κατηγορία κινδύνων πηγάζει από την οργάνωση του έργου. Το είδος και το πλήθος των κινδύνων αυτών είναι άμεσα συνυφασμένο με την εμπειρία των προσώπων που λαμβάνουν τις αποφάσεις, για το σχεδιασμό και την υλοποίηση του έργου.

Πρώτη και κύρια μέριμνα των προσώπων αυτών είναι οι διαδικασίες λήψης αποφάσεων και διοίκησης του έργου. Τα προβλήματα ξεκινούν όταν δεν υπάρχει η απαραίτητη εμπειρία και τεχνογνωσία για λήψη αποφάσεων, για προβλήματα που ανακύπτουν κατά την πορεία εκτέλεσης του έργου και που απαιτούν την άμεση αντίδραση των υπευθύνων. Η αδράνεια αυτών, αλλά και η χρονοτριβή έως ότου φθάσουν στη λήψη της σωστής απόφασης επιβαρύνουν σαφώς τη διάρκεια ολοκλήρωσης του έργου. Φυσικά ακόμα μεγαλύτερη επιβάρυνση θα επιφέρει η λήψη μιας βεβιασμένης απόφασης από πρόσωπα χωρίς την απαιτούμενη κατάρτιση, που σε βάθος χρόνου θα αποδειχθεί λανθασμένη. Ο χρόνος υλοποίησης του έργου θα επιβαρυνθεί και από τη σύγχυση δικαιοδοσιών και αρμοδιοτήτων μεταξύ στελεχών που καλούνται να λάβουν τις αποφάσεις. Ο τομέας ευθύνης του καθενός θα πρέπει να είναι αυστηρά καθορισμένος και οι αποφάσεις του να γίνονται σεβαστές από το υπόλοιπο περιβάλλον του έργου.

Είναι σαφές πως η παραπάνω σύγχυση είναι πιθανότερο να εμφανιστεί στην περίπτωση κοινοπραξίας για την εκτέλεση του έργου, όπου πέραν του διαχωρισμού των ευθυνών απαιτείται και η αρμονική συνεργασία μεταξύ των εμπλεκομένων.

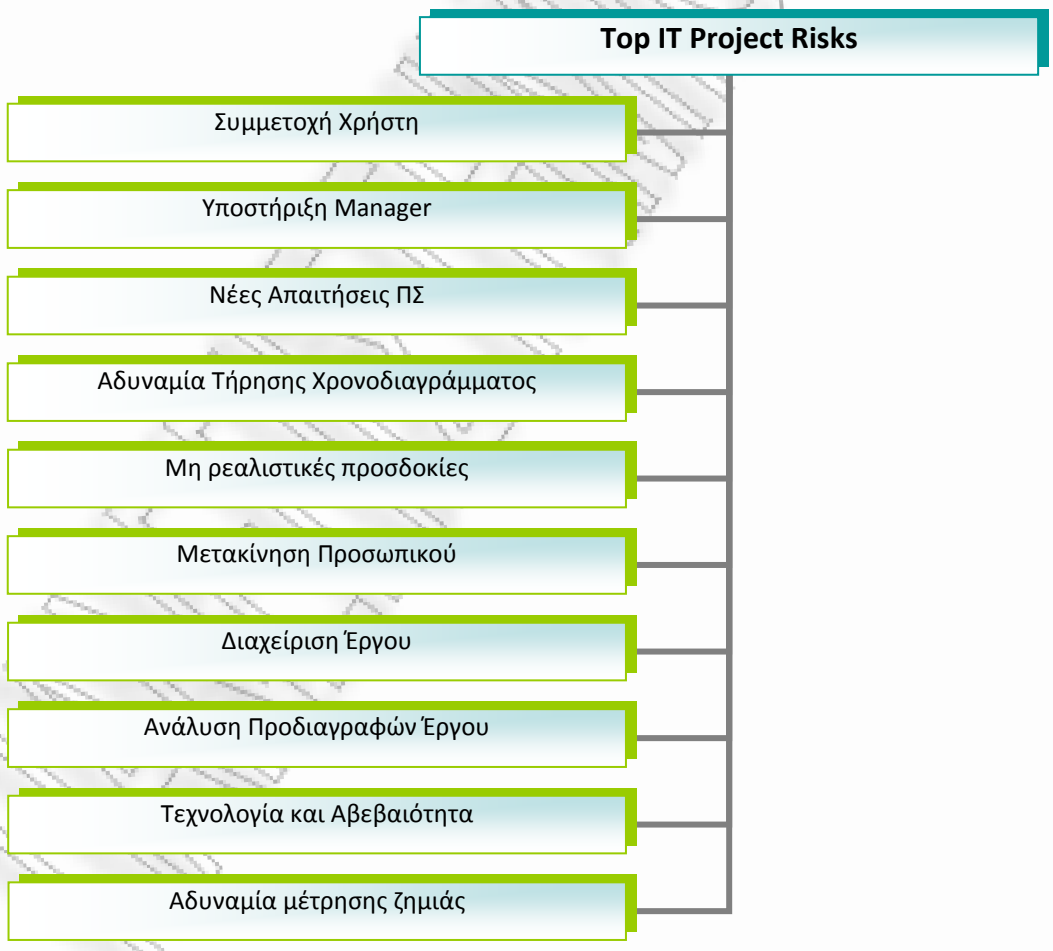
Ευθύνη των διοικούντων του έργου είναι και σύναψη σαφών και ασφαλών συμφωνιών με τους προμηθευτές εξοπλισμού. Η αναξιοπιστία ενός προμηθευτή και η αθέτηση των αρχικών συμφωνιών μπορεί να προκαλέσει καθυστερήσεις στην προμήθεια του εξοπλισμού που απαιτείται. Θα πρέπει επίσης να έχει προβλεφθεί η περίπτωση προβληματικών προμηθειών ή η καταστροφή υλικού κατά τη διαδικασία εγκατάστασής του, έτσι ώστε να είναι άμεση η αντικατάστασή του.

Τέλος, η υλοποίηση του πληροφοριακού έργου μπορεί να απειληθεί από κακή οργάνωση στον τομέα της χρηματοδότησής του. Ο κίνδυνος μπορεί να προέλθει από τον ασαφή καθορισμό του τρόπου και του χρόνου (είτε βάση χρονοδιαγράμματος είτε βάση της προόδου του έργου) διάθεσης των κονδυλίων και είναι ακόμα πιο πιθανός στην περίπτωση που οι χρηματοδότες είναι περισσότεροι του ενός. Καθυστερήσεις στην κάλυψη των δαπανών για οποιοδήποτε

λόγο θα καθυστερήσουν και το χρόνο ολοκλήρωσης του έργου, ενώ η ασάφεια στις υποχρεώσεις του κάθε χρηματοδότη μπορεί να οδηγήσει ακόμα και στην περικοπή κονδυλίων με αποτέλεσμα να μειωθούν και η ποιότητα και οι δυνατότητες του υλοποιούμενου πληροφοριακού συστήματος. Ακόμα, για ένα τέτοιο έργο, με τόσο υψηλό προϋπολογισμό, θα πρέπει να ληφθεί υπόψη και η πιθανότητα αδυναμίας κάλυψης των δαπανών από το χρηματοδότη, γεγονός που θα επέφερε τεράστιες απώλειες στην ανάδοχο εταιρία.

4.5 Σημαντικότεροι Κίνδυνοι Έργων Π.Σ

Έχει διαπιστωθεί ότι υπάρχουν δέκα παγκόσμιοι κίνδυνοι σε έργα πληροφορικής όπως φαίνεται στο Σχήμα 24 και οι περισσότεροι από αυτούς τους κίνδυνους δε σχετίζονται με τη τεχνολογία ή την ανάπτυξη λογισμικού, αλλά προσεγγίζουν κινδύνους επικοινωνίας και ανθρώπινων πόρων [21].



Σχήμα 24: Top IT Project Risks

Ακολούθως αναλύονται οι επιρροές που μπορεί να προκαλέσουν οι παραπάνω κίνδυνοι σε έργα πληροφορικής.

- ***Συμμετοχή Χρήστη***

Οι χρήστες είναι πολύ σημαντικός παράγοντας για την επιτυχή υλοποίηση ενός έργου πληροφορικής. Εάν οι χρήστες δεν εμπλέκονται στον προγραμματισμό του έργου, μπορεί να πραγματοποιήσουν καθυστερημένες αλλαγές, και αυτό με τη σειρά του μπορεί να προκαλέσει σημαντικές αυξήσεις στο κόστος του έργου. Το κλειδί της επιτυχίας είναι όσο πιο νωρίς είναι εφικτό να συμμετέχει ο χρήστης στο έργο και να υπάρχει συνεχής ενημέρωση στο χρήστη για τυχόν αλλαγές κατά τη διάρκεια υλοποίησης του έργου.

- ***Υποστήριξη Manager***

Η σωστή υποστήριξη του manager είναι εξίσου σημαντική για την επιτυχία του έργου πληροφορικής. Κατά τα αρχικά στάδια του έργου είναι σημαντικό να είναι ξεκάθαρο στον manager ποιος είναι ο χορηγός του έργου και αντίστοιχα ο χορηγός πρέπει να γνωρίζει ότι είναι χορηγός και ότι είναι εκεί για να βοηθήσει το έργο να επιτύχει. Οι ρόλοι και οι αρμοδιότητες αφορούν τόσο την ομάδα υλοποίησης του έργου όσο τον manager και τον χορηγό.

- ***Νέες Απαιτήσεις ΠΣ***

Όπως ήδη έχει αναφερθεί ο χρήστης είναι ο πιο σημαντικός παράγοντας για την επιτυχία του πληροφοριακού έργου. Συχνά οι χρήστες κατά την πορεία υλοποίησης του έργου αντιλαμβάνονται ότι το σύστημα έχει επιπλέον απαιτήσεις και επιθυμούν να πραγματοποιήσουν αλλαγές. Πρέπει λοιπόν να υπάρχει έλεγχος και σωστή διαχείριση των αλλαγών γιατί αποτυχημένες και βεβιασμένες αλλαγές μπορεί να φέρουν σε αποτυχία το πληροφοριακό έργο. Επίσης, κατά την πραγματοποίηση των αλλαγών πρέπει να είναι γνωστός ο χρόνος και το κόστος που θα απαιτηθεί.

- **Αδυναμία Τήρησης Χρονοδιαγράμματος**

Αδυναμία τήρησης του χρονοδιαγράμματος μπορεί να προέλθει από διάφορους λόγους, όπως για παράδειγμα, ελλιπής κατανόηση των παραδοτέων του έργου, χαμηλή εκτίμηση της απαιτούμενης δουλειάς, λάθος εκτίμηση του χρόνου λήξης του έργου και τέλος η αυτοπεποίθηση που ισχύει κάποιες φορές ότι τίποτα απρόοπτο δε θα συμβεί που θα μπορέσει να επηρεάσει το πληροφοριακό έργο. Το χρονοδιάγραμμα είναι δύσκολο να δημιουργηθεί. Υπάρχουν όμως αρκετές τεχνικές που μπορούν να αντιμετωπίσουν τις ατέλειες των χρονοδιαγραμμάτων όπως παρουσιάζονται παρακάτω:

- Ανάλυση πιθανών κινδύνων, χρονοδιαγράμματος και προϋπολογισμού
- Επιλογή κατάλληλου στελέχους που θα αφοσιωθεί στο αντικείμενο της δουλειάς
- Σύγκριση εκτιμήσεων με αντίστοιχα έργα υλοποιημένα στο παρελθόν

➢ ***Μη ρεαλιστικές προσδοκίες***

Εάν οι πελάτες και οι χρήστες του Π.Σ δεν είναι ενήμεροι για την πρόοδο του έργου, ενδεχομένως να περιμένουν κάτι εντελώς διαφορετικό από το Π.Σ που θα τους παραδοθεί. Γι ‘ αυτό το λόγο πρέπει από κοινού να συμφωνούνται και να υπογράφονται οι απαιτήσεις του συστήματος, το κόστος, το χρονοδιάγραμμα, ο σχεδιασμός και η δοκιμή των σχεδίων για να βεβαιωθούν και οι δύο πλευρές ότι έχουν τις ίδιες προσδοκίες.

➢ **Μετακίνηση Προσωπικού**

Η μετακίνηση προσωπικού σε μια εταιρία μπορεί να προκαλέσει σημαντικές αλλαγές στο έργο. Αν για παράδειγμα, θεωρηθεί κάποιος υπάλληλος ότι έχει τη τεχνογνωσία να συμμετέχει στην ομάδα του project διαχείρισης κινδύνων, τότε κρίνεται αναγκαία η μετακίνησή του. Πρέπει να ενισχύεται η εκπαίδευση και να είναι ξεκάθαροι οι ρόλοι του προσωπικού στο project. Εάν οι αλλαγές του προσωπικού στην εταιρία είναι εφικτές, πρέπει να δημιουργηθεί σχέδιο

εκπαίδευσης ούτως ώστε οι αλλαγές του προσωπικού να μην επηρεάσουν το χρονοδιάγραμμα και το κόστος.

- **Διαχείριση Έργου**

Εάν ο διαχειριστής του έργου αρνείται τη συμμετοχή των χρηστών στο project, ή προσπαθεί να οργανώσει το χρονοδιάγραμμα του έργου μόνος του, τότε υπάρχει σοβαρός κίνδυνος για το έργο. Ο project manager πρέπει να στηρίζει την πρόοδο του έργου, να επιλύει άμεσα οποιοδήποτε πρόβλημα προκύπτει, να αποφεύγει να σπαταλάει πολύ χρόνο εστιάζοντας σε μια πτυχή του έργου, να έρχεται σε συνεχή επικοινωνία με τον χορηγό του έργου και τα ενδιαφερόμενα μέρη και τέλος να είναι επικοινωνιακός με το προσωπικό και διπλωμάτης αλλά ειλικρινής όταν αναφέρεται στους κινδύνους. Επίσης, θα πρέπει να επαναλαμβάνεται μέχρι να γίνει πλήρως αντιληπτό το κομμάτι που επιθυμεί να επικοινωνήσει στο προσωπικό, και να χρησιμοποιεί διαφορετικές μεθόδους (π. χ επικοινωνία πρόσωπο με πρόσωπο, διαγράμματα, email, ιστοσελίδες, κλπ.). Τέλος, αν τα χρονοδιαγράμματα δεν τηρηθούν δε θα πρέπει να διστάζει να το μεταφέρει στον χορηγό και στα ενδιαφερόμενα μέρη.

- **Ανάλυση Προδιαγραφών Έργου**

Η ελλιπής ή καθόλου κατανόηση του έργου από τη μεριά του χρήστη, του manager και του χορηγού πρόκειται για έναν πολύ σημαντικό κίνδυνο. Εάν οι απαιτήσεις και οι στόχοι του έργου δεν είναι κατανοητοί το έργο βρίσκεται σε συνεχή κίνδυνο.

- **Τεχνολογία και Αβεβαιότητα**

Δεν μπορεί να αγνοηθεί η τεχνολογία όταν αναφερόμαστε σε έργα πληροφορικής. Κάθε project πληροφορικής εμπεριέχει κινδύνους λόγω της φύσης του έργου. Κάθε manager και χορηγός πρέπει να είναι ενήμερος για ενδεχόμενους κίνδυνους που μπορεί να προκύψουν. Πρέπει αρχικά να αξιολογήσει αν υπάρχει η δυνατότητα να υλοποιηθεί το έργο, πόσο οικείο είναι στο περιβάλλον, πόση εμπειρία υπάρχει στο λογισμικό, στο δίκτυο που απαιτείται και στις διεπαφές με

τους χρήστες. Εάν χρειάζεται να χρησιμοποιηθεί νέα πλατφόρμα, νέο λογισμικό και νέες διεπαφές η αβεβαιότητα του κινδύνου αυξάνετε. Επίσης, οι εκτιμήσεις του κόστους, του χρονοδιαγράμματος και της ποιότητας πρέπει να προσαρμόζονται αναλόγως.

- **Αδυναμία μέτρησης ζημιάς**

Συχνά στη διαχείριση των κινδύνων δεν είναι σαφής η ζημιά που προκύπτει σε περίπτωση που το έργο αποτύχει. Εάν ο Project Manager και οι υπόλοιποι ενδιαφερόμενοι δεν γνωρίζουν το μέγεθος της ζημιάς, σημαίνει ότι δε μπορούν να υποστηρίξουν τη διαδικασία διαχείρισης κινδύνων για το πληροφοριακό έργο που τους έχει ανατεθεί.

4.6 Ανάλυση Ευπαθειών

Η ανάλυση των απειλών σε ένα Π.Σ πρέπει να περιλαμβάνει και ανάλυση των ευπαθειών που σχετίζονται με το περιβάλλον του συστήματος [15]. Ο στόχος του συγκεκριμένου βήματος είναι η δημιουργία μιας λίστας με τις πιθανές ευπάθειες του Π.Σ. Στο Σχήμα 25 εμφανίζονται διάφορα παραδείγματα ευπαθειών, πιθανών κινδύνων και απειλών:

Ευπάθεια (Αδυναμία) ΠΣ	Πιθανός Κίνδυνος	Πιθανή Απειλή
Τα ID (αναγνωριστικά) χρηστών έχουν αφαιρεθεί από το σύστημα	Χρήστης	Πρόσβαση σε εμπιστευτικά δεδομένα
Ατέλειες ασφάλειας συστήματος	Μη εξουσιοδοτημένοι χρήστες (hacker, δυσαρεστημένοι υπάλληλοι, τρομοκράτες κ. α)	Μη εξουσιοδοτημένη πρόσβαση σε εμπιστευτικά δεδομένα του συστήματος
Τα μηχανήματα πρόληψης φωτιάς/νερού κ. α δε λειτουργούν	Φωτιά/Αμέλεια Υπαλλήλων	Εκτοξευτήρες νερού που ενεργοποιούνται στο κέντρο του data center

Σχήμα 25: Ζεύγος Ευπάθειας/Απειλών

Οι προτεινόμενες μέθοδοι για τον προσδιορισμό των ευπαθειών του συστήματος είναι η χρήση διάφορων πηγών ευπάθειας (π. χ ερωτηματολόγια, συνεντεύξεις, ειδικές ιστοσελίδες προμηθευτών κ. α), η εκτέλεση δοκιμών ασφαλείας καθώς και η δημιουργία μιας λίστας δυνητικών ευπαθειών (αδυναμιών) του Π.Σ. Αξίζει να σημειωθεί ότι ο τύπος της ευπάθειας που υφίστανται καθώς και η μεθοδολογία που θα χρησιμοποιηθεί για την αντιμετώπιση της, εξαρτάται από το Π.Σ και από τη φάση του Κύκλου Ζωής που βρισκόμαστε (SDLC):

- Αν το Π.Σ δεν έχει ακόμα σχεδιαστεί, η μεθοδολογία αναζήτησης ευπαθειών θα πρέπει να επικεντρωθεί σε πολιτικές ασφαλείας, προγραμματισμένες δοκιμές ασφαλείας κ. α.
- Αν το Π.Σ έχει τεθεί σε εφαρμογή, ο εντοπισμός των ευπαθειών πρέπει να περιλαμβάνει συγκεκριμένες πληροφορίες, όπως για

παράδειγμα χαρακτηριστικά προγραμματισμένων ελέγχων ασφαλείας, και τα διάφορα αποτελέσματα που προκύπτουν από αυτές τις δοκιμές.

- Αν το Π.Σ έχει τεθεί σε λειτουργία θα πρέπει να περιλαμβάνει ανάλυση των χαρακτηριστικών ασφαλείας και των ελέγχων ασφαλείας που χρησιμοποιούνται για την προστασία του Π.Σ, τόσο τεχνικά όσο και διαδικαστικά.

Ωστόσο, μπορούν να χρησιμοποιηθούν προληπτικές μέθοδοι για την αξιολόγηση της αποτελεσματικότητας αναγνώρισης των ευπαθειών του Π.Σ. Για παράδειγμα η μέθοδος ***ST&E*** (Security Test & Evaluation) έχει στόχο να διασφαλίσει ότι οι έλεγχοι που εφαρμόζονται πληρούν τις διεθνής πολιτικές ασφάλειας, επίσης η μέθοδος ***penetration testing*** (δοκιμή διείσδυσης) έχει στόχο να αξιολογήσει το Π.Σ από θέματα ασφαλείας και να εντοπίσει πιθανές αποτυχίες του συστήματος στο συγκεκριμένο κομμάτι.

Επίσης, σ' αυτό το βήμα είναι σημαντικό να δημιουργηθεί μία λίστα απαιτήσεων ασφαλείας από το προσωπικό της εταιρίας αξιολογώντας αν πληρούνται οι υπάρχουσες ή σχεδιαζόμενες πολιτικές ασφαλείας. Μια λίστα ελέγχου ασφαλείας περιέχει τα βασικά πρότυπα ασφαλείας που μπορούν να χρησιμοποιηθούν για τη συστηματική αξιολόγηση των ευπαθειών του Π.Σ (π. χ hardware, software, πληροφορίες, προσωπικό κ. α) και διαφόρους ελέγχους ασφαλείας ανάλογα με το τμήμα της εταιρίας (π. χ διοίκηση, λειτουργία, τεχνικό τμήμα).

Οι έλεγχοι ασφαλείας που αφορούν τη διοίκηση πρέπει να δίνουν μεγάλη σημασία στην ανάθεση αρμοδιοτήτων, συνεχή υποστήριξη του ΠΣ, στην ικανότητα αντιμετώπισης περιστατικών, στην περιοδική επανεξέταση των ελέγχων ασφαλείας, στην αξιολόγηση των κινδύνων, στην εκπαίδευση σε θέματα ασφάλειας και τεχνικής κατάρτισης, στον διαχωρισμό των καθηκόντων κ.α.

Οι έλεγχοι ασφαλείας που αφορούν τη λειτουργία της εταιρίας πρέπει να περιλαμβάνουν ελέγχους διασφάλισης της ηλεκτρικής τροφοδοσίας, ελέγχους διασφάλισης δεδομένων, προστασία των εγκαταστάσεων (π. χ γραφεία, server, Η/Υ κ. α), ελέγχους υγρασίας, θερμοκρασίας κ.α.

Τέλος, οι έλεγχοι ασφαλείας που αφορούν το τεχνικό τμήμα της εταιρίας πρέπει να περιλαμβάνουν ελέγχους κρυπτογραφίας, προσβάσεων, ταυτοποίηση και αυθεντικοποίηση χρηστών, ανίχνευση εισβολέων κ.α.

4.7 Ανάλυση Ελέγχων

Στο βήμα αυτό οι υπεύθυνοι σχεδιασμού του έργου καλούνται να αξιολογήσουν τους υπάρχοντες μηχανισμούς ελέγχου των πληροφοριακών συστημάτων του οργανισμού [15]. Οι μηχανισμοί αυτοί έχουν να κάνουν με την ασφάλεια του έργου και δεν αφορούν όλες τις κατηγορίες κινδύνων που μπορούν να το προσβάλλουν. Η αξιολόγηση αυτή σκοπό έχει να εντοπιστούν τυχόν ελλείψεις και αδυναμίες στα συστήματα ασφαλείας ούτως ώστε να είναι πιο εύκολος αργότερα ο σχεδιασμός των διαδικασιών ασφαλείας του νέου πληροφοριακού συστήματος. Στο βήμα αυτό θα φανεί αρκετά χρήσιμη η συλλογή πληροφοριών που έγινε στο πρώτο βήμα.

Μπορούμε να διακρίνουμε τους ελέγχους σε αποτρεπτικούς και σε ελέγχους εντοπισμού σφαλμάτων. Αποτρεπτικοί είναι οι έλεγχοι που στοχεύουν στο να εμποδίσουν τη δημιουργία επικίνδυνων καταστάσεων για τον οργανισμό, ενώ οι έλεγχοι εντοπισμού έχουν την ευθύνη να εντοπίζουν τις όποιες ανεπιθύμητες καταστάσεις εμφανίζονται στη λειτουργία των συστημάτων.

Οι έλεγχοι ασφαλείας πραγματοποιούνται είτε από προσωπικό ασφαλείας είτε από διάφορα ηλεκτρονικά συστήματα είτε από πληροφοριακά συστήματα.

Το προσωπικό ασφαλείας οφείλει να ελέγχει τα πρόσωπα που εισέρχονται στους χώρους όπου διενεργούνται οι εργασίες εγκατάστασης του συστήματος, τα πρόσωπα που εισέρχονται στους χώρους αποθήκευσης του εξοπλισμού, αλλά και τα μέλη του προσωπικού που χρησιμοποιούν τα ήδη παραδοθέντα τμήματα του έργου και αποκτούν πρόσβαση σε ευαίσθητο λογισμικό και βάσεις δεδομένων. Ακόμα το προσωπικό ασφαλείας έχει την ευθύνη φύλαξης των εγκαταστάσεων κατά τις ώρες μη λειτουργίας του οργανισμού.

Πέραν όμως του προσωπικού φύλαξης των εγκαταστάσεων του οργανισμού υπάρχει και το προσωπικό φύλαξης του λογισμικού του έργου. Τα στελέχη αυτά παρακολουθούν τη λειτουργία των συστημάτων, έτσι ώστε να μπορούν να επέμβουν άμεσα σε περίπτωση κάποιας δυσλειτουργίας του συστήματος και να προλάβουν δυσμενέστερες επιπτώσεις αυτής. Επίσης παρακολουθούν τα τερματικά

που αποκτούν πρόσβαση στα διάφορα τμήματα του πληροφοριακού συστήματος (χρήση software, βάσεων δεδομένων) για τον εντοπισμό τυχόν μη εξουσιοδοτημένων χρηστών. Για το σκοπό αυτό φυσικά χρησιμοποιούν το κατάλληλο λογισμικό που τους επιτρέπει την πρόσβαση για έλεγχο σε κάθε ευαίσθητο κομμάτι του συστήματος. Παράλληλα θα πρέπει να υπάρχουν και συστήματα που προστατεύουν το σύστημα από ανεπιθύμητους εισβολείς.

Ο εξοπλισμός (σε hardware και software) θα πρέπει να ελεγχθεί και να αξιολογηθεί ως προς την επάρκεια και την αποτελεσματικότητά του. Παράλληλα θα πρέπει να αξιολογηθεί και το ίδιο το προσωπικό για τις τεχνικές γνώσεις του και τις δυνατότητές του να παρακολουθεί και να ελέγχει τη λειτουργία του συστήματος, να εποπτεύει τους χρήστες των συστημάτων και να εντοπίζει τις όποιες παράτυπες καταστάσεις εμφανίζονται στη λειτουργία του συστήματος. Θα πρέπει να ελεγχθούν και για την αντίληψη που έχουν για τη σημαντικότητα των καθηκόντων τους για την ορθή λειτουργία και την ασφάλεια του έργου λογισμικού.

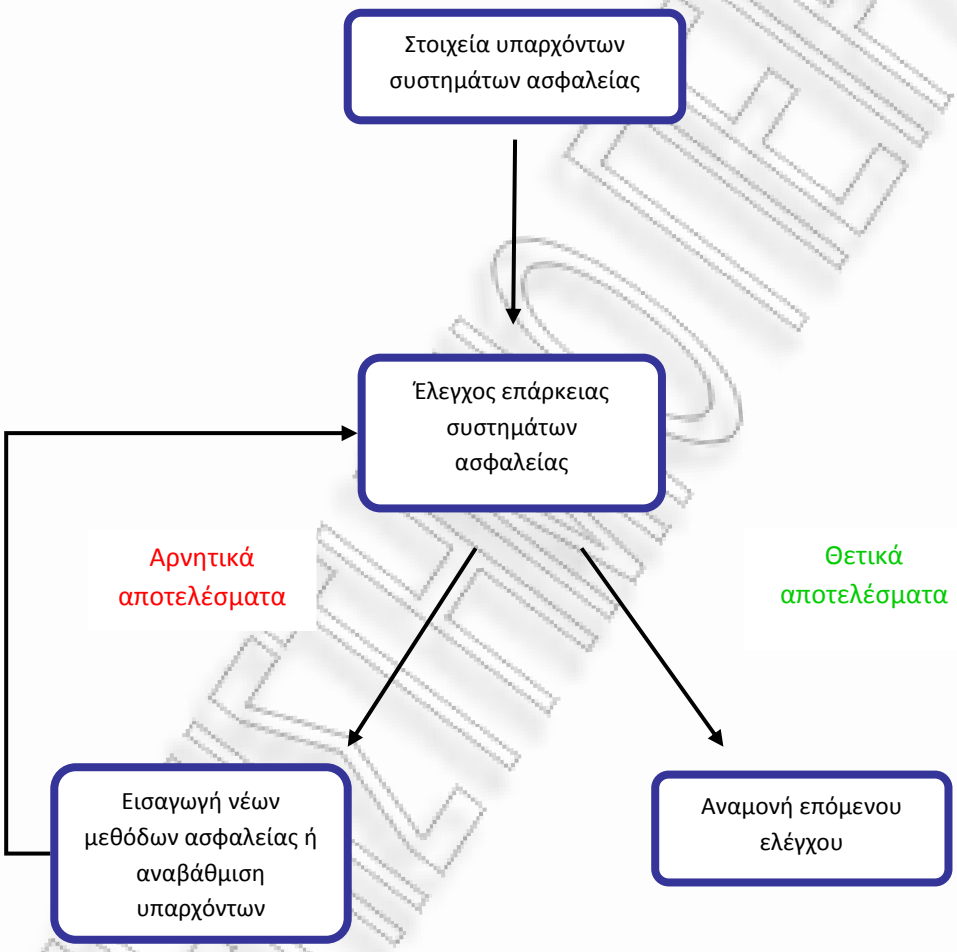
Υπάρχουν και τα ηλεκτρονικά συστήματα που ελέγχουν την τήρηση των συνθηκών ασφαλείας στους χώρους όπου βρίσκεται εγκατεστημένο το υλικό του πληροφοριακού έργου. Τέτοια είναι τα συστήματα πυρασφαλείας, τα συστήματα ελέγχου θερμοκρασίας και υγρασίας στο δωμάτιο εγκατάστασης του υλικού, θερμοστάτες στα διάφορα τμήματα του συστήματος, μετρητές τάσης και άλλα τέτοιου είδους μέσα ελέγχου της ασφαλούς λειτουργίας των συστημάτων.

Όλες οι παραπάνω διαδικασίες θα πρέπει να ελεγχθούν ως προς την ύπαρξή τους πρώτα από όλα, την αρτιότητα της λειτουργίας τους, την αποτελεσματικότητά τους, αλλά και τη συμβατότητά τους με το νέο λογισμικό και υλικό. Εκτός αυτών όμως, θα πρέπει να αξιολογηθεί και η κρισιμότητα της χρήσης τους, καθώς τέτοιοι έλεγχοι καθυστερούν τη λειτουργία των συστημάτων και αυξάνουν την πολυπλοκότητά τους και θα ήταν επιζήμια τελικά η εισαγωγή τους σε τομείς του έργου που δεν εκτίθενται ιδιαίτερα σε κίνδυνο.

Η πληροφορίες αυτού του βήματος σε συνδυασμό με την αναφορά εκτίμησης κινδύνων θα αποτελέσουν ένα πολύ χρήσιμο εργαλείο, κατά την κατάρτιση σχεδίου δράσης, για τη μείωση ή την εξάλειψη της πιθανότητας εμφάνισης των διαφόρων κινδύνων. Οι ελλείψεις ή αδυναμίες θα πρέπει να καλυφθούν και οι διαδικασίες ασφαλείας να περάσουν ξανά από έλεγχο επάρκειας των δυνατοτήτων τους. Ο

έλεγχος αυτός φυσικά θα πρέπει να επαναλαμβάνεται σε όλη τη διάρκεια υλοποίησης του έργου και τα συστήματα συνεχώς να αναβαθμίζονται για διατήρηση ικανοποιητικών επιπέδων ασφαλείας.

Στο Σχήμα 26 περιγράφονται σχηματικά οι διεργασίες ελέγχου και προσθήκης των συστημάτων ασφαλείας.



Σχήμα 26: Διαδικασία ελέγχου συστημάτων ασφαλείας

Κεφάλαιο 5: Ανάλυση Κινδύνων

5.1 Εισαγωγή

Ο βασικός σκοπός της διαδικασίας διαχείρισης κινδύνων είναι η λήψη μέτρων σχετικά με τους εντοπιζόμενους κινδύνους. Ο τρόπος με τον οποίο ξεχωρίζουμε τους κινδύνους εκείνους στους οποίους είναι συμφέρον να αντιδράσουμε είναι η ανάλυσή τους. Στο παρόν κεφάλαιο θα παρουσιαστεί η διαδικασία ποιοτικής αποτίμησης του επιπέδου έκθεσης σε κάθε κίνδυνο και του συνολικού επιπέδου έκθεσης σε κίνδυνο όλου του έργου, οι διαδικασίες ποσοτικής αποτίμησης των κινδύνων, αλλά και η παρουσίαση του τρόπου σύνταξης αναφοράς με τα αποτελέσματα όλων των βημάτων της διαδικασίας εκτίμησης κινδύνων.

Η διαδικασία αξιολόγησης κινδύνων, είτε είναι ποιοτική είτε είναι ποσοτική [11, 15], ακολουθεί τη διαδοχή των βημάτων της διαδικασίας ανάλυσης κινδύνων. Δηλαδή, πρώτα πραγματοποιείται η εκτίμηση της πιθανότητας εμφάνισης ενός κινδύνου, κατόπιν η αξιολόγηση των επιπτώσεων του και τέλος γίνεται η συνεκτίμηση των παραπάνω για την εξαγωγή συμπερασμάτων ως προς σοβαρότητα των κινδύνων για την ακεραιότητα του έργου. Η δομή αυτή χρησιμοποιείται κατά την ποιοτική αξιολόγηση που περιγράφεται παρακάτω. Η ποσοτική αξιολόγηση όμως, η οποία έχει την ίδια δομή, αναφέρεται πιο επιγραμματικά, παρουσιάζοντας τις εισόδους και εξόδους της και τα εργαλεία και τις μεθόδους που χρησιμοποιεί.

Σημειώνεται ότι η ποσοτική ανάλυση κινδύνων είναι υπερσύνολο της ποιοτικής, καθώς περιέχει όλα τα στοιχεία της ποιοτικής ανάλυσης και επιπλέον τη δυνατότητα μαθηματικής ανάλυσής. Αν και η ποσοτική ανάλυση κινδύνων δίνει μεγαλύτερη και ουσιαστική πληροφόρηση στην ομάδα διαχείρισης κινδύνων, είναι αρκετά δύσκολο να εφαρμοστεί σε πραγματικές συνθήκες και συνήθως παραλείπεται. Βέβαια, σε έργα μεγάλου προϋπολογισμού είναι πολλές φορές απαραίτητη η ποσοτική ανάλυση , καθώς η χρήση μόνο ποιοτικών δεδομένων μπορεί να οδηγήσει σε μεγάλες απώλειες.

5.2 Ποιοτική ανάλυση κινδύνων

Η ποιοτική ανάλυση κινδύνων βασίζεται σε εκτίμηση της πιθανότητας εμφάνισης του κινδύνου και της συνέπειας που αυτός έχει στο έργο, τα οποία όμως δεν εκφράζονται σε απόλυτα μεγέθη. Συνήθως, για την έκφραση της πιθανότητας εμφάνισης κινδύνων και της συνέπειας, χρησιμοποιούνται λεκτικές διαβαθμίσεις που δημιουργούν συγκεκριμένες κλίμακες (π. χ Ελάχιστο, Λίγο, Πολύ, Πάρα πολύ). Οι κλίμακες είναι το πρώτο και ουσιαστικότερο εργαλείο της ποιοτικής ανάλυσης. Τις κλίμακες διαδέχεται ο πίνακας κινδύνων που είναι το εργαλείο υπολογισμού της έκθεσης και τέλος, ακολουθεί η κατάταξη των κινδύνων, με βάση την έκθεση.

5.2.1 Εκτίμηση πιθανότητας εμφάνισης κινδύνων

Καθώς έχουν επισημανθεί οι πιθανοί κίνδυνοι και έχουν σκιαγραφηθεί οι υπάρχοντες έλεγχοι ασφαλείας που απειλούν και προστατεύουν αντίστοιχα το πληροφοριακό έργο, επόμενο βήμα είναι η εκτίμηση της πιθανότητας εμφάνισης καθενός από τους παραπάνω κινδύνους.

Κατά τη διαδικασία εκτίμησης της πιθανότητας εμφάνισης των κινδύνων τρία στοιχεία που θα πρέπει να ληφθούν υπόψη [15]:

- Το κίνητρο και οι δυνατότητες της κάθε πηγής κινδύνων
- Η φύση των ευπαθειών
- Η παρουσία και η αποτελεσματικότητα των υπαρχόντων ελέγχων

Η διαδικασία εκτίμησης της πιθανότητας εμφάνισης ενός κινδύνου δεν είναι απλή. Καταρχήν τα πρόσωπα που θα προβούν σε αυτή την εκτίμηση θα πρέπει να έχουν την κατάλληλη κατάρτιση, σωστή ενημέρωση και την απαιτούμενη πείρα ούτως ώστε να μπορέσουν να εκτιμήσουν ορθολογικά την πιθανότητα παρουσίας του κάθε ανεπιθύμητου γεγονότος. Μια λανθασμένη εκτίμηση μπορεί να έχει καταστροφικές συνέπειες για την αξιοπιστία και τη χρησιμότητα της όλης διαδικασίας διαχείρισης κινδύνων. Μια αισιόδοξη εκτίμηση για την πιθανότητα εμφάνισης κάποιων απειλών μπορεί να οδηγήσει στην υποτίμησή τους και τη μη λήψη των κατάλληλων μέτρων για την αντιμετώπισή τους. Από την άλλη,

απαισιόδοξες εκτιμήσεις θα έχουν ως αποτέλεσμα την άσκοπη διάθεση κονδυλίων και την αύξηση της πολυπλοκότητας και των καθυστερήσεων στη λειτουργία των συστημάτων, για αντιμετώπιση κινδύνων, που δεν αποτελούν ουσιαστική απειλή για την υλοποίηση του έργου λογισμικού.

- ***Ποιοτικές κλίμακες***

Για την ποιοτική ανάλυση κινδύνων απαιτούνται δύο, το λιγότερο κλίμακες. Η μια θα πρέπει να περιγράφει την πιθανότητα εμφάνισής του κινδύνου και η άλλη τη συνέπεια του κινδύνου στο έργο, σε περίπτωση εμφάνισης. Μπορούμε λοιπόν, να κατατάξουμε τον κάθε κίνδυνο ανάλογα με την πιθανότητα εμφάνισής του σε κάποια από τις πέντε παρακάτω κατηγορίες [11, 15].

Πιθανότητα Εμφάνισης	Ορισμός πιθανότητας
Πολύ υψηλή	Ο κίνδυνος είναι σχεδόν βέβαιο γεγονός ότι θα εμφανιστεί, και οι αρμόδιες διαδικασίες ελέγχου αποδεικνύονται αναποτελεσματικές για την αντιμετώπισή του
Υψηλή	Ο κίνδυνος είναι πολύ πιθανό να εμφανιστεί, και οι απαιτούμενες διαδικασίες ελέγχου παρουσιάζουν μεγάλες αδυναμίες και ελλείψεις
Μέτρια	Ο κίνδυνος δεν έχει μεγάλη πιθανότητα να εμφανιστεί, και οι διαδικασίες ελέγχου ενδεχομένως να τον αντιμετωπίσουν αποτελεσματικά
Χαμηλή	Ο κίνδυνος έχει μικρή πιθανότητα εμφάνισης, και οι διαδικασίες ελέγχου δύνανται να τον αντιμετωπίσουν με επιτυχία
Πολύ χαμηλή	Ο κίνδυνος είναι σχεδόν αδύνατο να εμφανιστεί, και οι διαδικασίες ελέγχου ουσιαστικά “αδιαπέραστες”

Σχήμα 27: Κατηγορίες Κατάταξης Κινδύνων ανάλογα με την πιθανότητα εμφάνισης

Η κλίμακα πιθανότητας εμφάνισης κινδύνου βρίσκεται μεταξύ 0.0 (καμία πιθανότητα) και 1.0 (βεβαιότητα). Ο ακριβής υπολογισμός της πιθανότητας

εμφάνισης ενός κινδύνου είναι μια πολύ δύσκολη και επίπονη διαδικασία, και τα αποτελέσματά της είναι δύσκολο να ελεγχθούν για την ακρίβεια και την ορθότητά τους. Για αυτό συχνά χρησιμοποιείται μια γενική κλίμακα τυποποιημένων πιθανοτήτων, ανάλογα με τα επίπεδα πιθανότητας του παραπάνω πίνακα. Οι τυποποιημένες τιμές της κλίμακας αυτής, ανάλογα με το πόσο πιθανή είναι η εμφάνιση ενός γεγονότος, είναι 0.1 , 0.3 , 0.5 , 0.7 , 0.9.

Είδαμε παραπάνω πως μπορούμε να κατατάξουμε τους κινδύνους ανάλογα με την πιθανότητα εμφάνισής τους. Το δύσκολο όμως και επίπονο κομμάτι αυτής της διαδικασίας είναι το πως θα καθοριστεί η πιθανότητα εμφάνισης της κάθε απειλής. Για το σκοπό αυτό θα φανούν εξαιρετικά χρήσιμες οι πληροφορίες που συλλέχθηκαν για τον οργανισμό και τους στόχους που θα έχει να επιτελέσει το νέο πληροφοριακό έργο, καθώς και για τους υπάρχοντες ελέγχους ασφαλείας. Για παράδειγμα η χρήση τεχνολογιών που εφαρμόζονται για πρώτη φορά εμφανίζουν υψηλή επικινδυνότητα να παρουσιάσουν δυσλειτουργίες στη χρήση τους και να μη μπορέσουν τελικά να ανταποκριθούν στις απαιτήσεις του οργανισμού, ενώ η χρησιμοποίηση δοκιμασμένων συστημάτων δεν προβληματίζει τόσο για τη λειτουργικότητα της χρησιμοποίησής των. Αντιμετωπίζουν όμως με τη σειρά τους τον κίνδυνο να καταστούν απαρχαιωμένες σε μικρό χρονικό διάστημα από την εκκίνηση της λειτουργίας τους κάτι που έχει πολύ μικρές πιθανότητες να συμβεί με τη χρήση νέων και σύγχρονων τεχνολογιών.

Ένα δεύτερο παράδειγμα αποτελούν οι απειλές από ανταγωνιστές. Ένα έργο με κοινωφελείς προεκτάσεις όπως η διαδικτυακή σύνδεση νοσοκομείων για την μεταφορά αρχείων με το ιστορικό των ασθενών φαντάζει αδύνατο να έχει να αντιμετωπίσει των κίνδυνο δολιοφθορών από ανταγωνιστές ή τρομοκρατικών επιθέσεων, αλλά κινδυνεύει από τη χρήση των στοιχείων των ασθενών από πρόσωπα που επιδιώκουν την εκμετάλλευση των στοιχείων αυτών για προσωπικό όφελος. Ενδεικτικά αναφέρονται οι λίστες των δωρητών οργάνων, η κοινοποίηση των οποίων μπορεί να θέσει σε κίνδυνο τις ζωές των δωρητών από επιτήδειους που αναζητούν απεγνωσμένα κάποιο όργανο και διαθέτουν τα χρήματα και τα μέσα για να το αποκτήσουν με κάθε τρόπο. Τέλος ένα ακόμα παράδειγμα ενδεικτικό της διαφορετικότητας του κάθε υπό υλοποίηση έργου, είναι τα καιρικά φαινόμενα που μπορούν να απειλήσουν τις εγκαταστάσεις του οργανισμού και που

διαφοροποιούνται ανάλογα με τη γεωγραφική θέση του οργανισμού και γενικότερα το περιβάλλον όπου βρίσκονται οι εγκαταστάσεις.

- ***Πίνακας Κινδύνων***

Ο πίνακας κινδύνων χρησιμοποιείται στην ποιοτική ανάλυση για τον υπολογισμό της έκθεσης των κινδύνων. Σύμφωνα με την κοινή πρακτική η έκθεση υπολογίζεται από το γινόμενο:

Πιθανότητα εμφάνισης * Συνέπεια σε περίπτωση εμφάνισης

Συνεπώς, οι διαστάσεις του πίνακα κινδύνων προσδιορίζονται από τον αριθμό επιπέδων των κλιμάκων πιθανότητας εμφάνισης και συνέπειας σε περίπτωση εμφάνισης [11, 15].

Έκθεση του Έργου σε Κίνδυνο					
Πιθανότητα (Π)	***Έκθεση= Π*Σ***				
0,9 Πολύ Υψηλή	0,05	0,09	0,18	0,36	0,72
0,7 Υψηλή	0,04	0,07	0,14	0,28	0,56
0,5 Μέση	0,03	0,05	0,10	0,20	0,40
0,3 Χαμηλή	0,02	0,03	0,06	0,12	0,24
0,1 Πολύ Χαμηλή	0,01	0,01	0,02	0,04	0,08
	0,05 Πολύ Χαμηλή	0,10 Χαμηλή	0,20 Μέση	0,40 Υψηλή	0,80 Πολύ Υψηλή
Συνέπεια (Σ)					
Αποδεκτός Κίνδυνος	***Μη επιθυμητός Κίνδυνος***		***Μη αποδεκτός Κίνδυνος***		

Σχήμα 28: Παράδειγμα έκθεσης κινδύνων κατά PMI, 2000

Ο παραπάνω πίνακας, παρουσιάζει μια ουσιαστική διαφοροποίηση σε σχέση με τους άλλους πίνακες κινδύνων. Σε αυτόν τον πίνακα, η βαρύτητα που δίνεται στην πιθανότητα εμφάνισης και στη συνέπεια δεν είναι ίδια. Η διαφορά βαρύτητας εκφράζεται μέσω της μη γραμμικότητας της κλίμακας της συνέπειας σε αντίθεση με

την κλίμακα της πιθανότητας. Η διαφοροποίηση αυτή, έχει ως αποτέλεσμα το γινόμενο της χαμηλής πιθανότητας με την πολύ υψηλή συνέπεια να οδηγεί σ ΄ έναν πολύ υψηλό κίνδυνο, , ενώ το γινόμενο της πολύ υψηλής πιθανότητας με τη χαμηλή συνέπεια να οδηγεί σ ΄ έναν μέσο κίνδυνο. Δηλαδή, είναι σίγουρα πιο σημαντικό να υπάρχει μικρή πιθανότητα να γίνει μια καταστροφή, από το να υπάρχει μεγάλη πιθανότητα να συμβεί κάτι ασήμαντο.

- ***Κατάταξη κίνδυνων***

Το Σχήμα 29 δίνει την εικόνα της κατάταξης κινδύνων που θα είχαμε σ ΄ ένα έργο σε περίπτωση που χρησιμοποιούσαμε τον πίνακα ποιοτικής ανάλυσης κατά PMI [11]. Ανεξάρτητα από το πρότυπο ποιοτικής ανάλυσης που χρησιμοποιεί ο αναλυτής είναι πάντα χρήσιμη η απεικόνιση των κινδύνων σε πίνακα κατάταξης κινδύνων έργου.

Κωδικός Κινδύνου	Έκθεση κατά PMI	Σειρά κατάταξης
A5	0,36	2
B6	0,03	7
B7	0,10	4
B9	0,14	3
Γ3	0,10	4
Δ3	0,56	1
E11	0,09	5
A4	0,07	6

Σχήμα 29: Κατάταξη Κινδύνων κατά PMI

5.2.2 Ανάλυση Επιπτώσεων

Το επόμενο βήμα για την εκτίμηση ενός κινδύνου, αποτελεί η αξιολόγηση των επιπτώσεων στην πορεία υλοποίησης του έργου, από την εμφάνιση κάποιας εκ των απειλών [15]. Προτού προχωρήσουμε στην παρουσίαση της διαδικασίας αξιολόγησης κινδύνων αναφέρουμε κάποιες πληροφορίες σχετικά με το έργο πληροφορικής, των οποίων η γνώση είναι απαραίτητη για την επιτυχημένη ολοκλήρωση του βήματος αυτού.

- Η αποστολή του συστήματος, δηλαδή οι διαδικασίες που θα επιτελούνται από το πληροφοριακό σύστημα
- Η κρισιμότητα του συστήματος και της βάσης δεδομένων, δηλαδή η αξία και η σημασία του συστήματος για τη λειτουργία και την ανάπτυξη του οργανισμού.
- Η ευαισθησία του συστήματος και της βάσης δεδομένων

Οι πληροφορίες αυτές μπορούν να συλλεχθούν από υπάρχουσες εκθέσεις της λειτουργίας του οργανισμού, όπως η έκθεση ανάλυσης αντίκτυπου ενός στόχου ή η έκθεση αξιολόγησης κρισιμότητας μιας διαδικασίας. Η έκθεση ανάλυσης αντίκτυπου ενός στόχου παρουσιάζει το επίπεδο των κινδύνων που συνοδεύουν την εφαρμογή μιας διαδικασίας μαζί με τα προτερήματα αυτής βασισμένη σε μια ποιοτική ή ποσοτική αξιολόγηση της ευαισθησίας και της κρισιμότητας αυτών των προτερημάτων. Η έκθεση αξιολόγησης κρισιμότητας μιας διαδικασίας αναγνωρίζει και δίνει προτεραιότητα στα ευπαθή και κρίσιμα προτερήματα του οργανισμού που παίζουν σημαντικό ρόλο στην επίτευξη των στόχων αυτού.

Εάν τέτοιου είδους εκθέσεις δεν υπάρχουν, τότε η ευαισθησία συστημάτων και πληροφοριών μπορεί να καθοριστεί με βάση το επίπεδο προστασίας που απαιτείται για τη διατήρηση της διαθεσιμότητας, της ακεραιότητας και της εμπιστευτικότητας αυτών. Ανεξάρτητα από τη μέθοδο που θα χρησιμοποιηθεί για τον καθορισμό της ευαισθησίας του πληροφοριακού συστήματος και της βάσης δεδομένων του, οι υπεύθυνοι υλοποίησης του έργου, με τη συνεργασία της διοίκησης του οργανισμού για τον οποίο υλοποιείται αυτό, οφείλουν να είναι σε θέση να καθορίσουν το επίπεδο των επιπτώσεων από την ενδεχόμενη δυσλειτουργία ή προσβολή από εξωτερικούς παράγοντες του συστήματος.

Για την αξιολόγηση των επιπτώσεων λοιπόν θα ήταν χρήσιμες οι πληροφορίες από τις συναντήσεις με τους διοικούντες του οργανισμού, οι οποίοι αποφάσισαν την προσθήκη ενός τέτοιου συστήματος στο δυναμικό του οργανισμού. Ακολουθεί μια συνοπτική περιγραφή των στόχων ασφαλείας που πρέπει να επιτευχθούν και τις συνέπειες από τη μη επιτυχημένη προστασία αυτών:

- ***Απώλεια ακεραιότητας*:** Η ακεραιότητα συστημάτων και πληροφοριών αναφέρεται στην απαίτηση αυτά να προστατεύονται από την ανάρμοστη τροποποίηση ή καταστροφή αλλά και την απαίτηση

άμεσης αποκατάστασης της λειτουργίας τους σε περίπτωση που αυτή παρουσιάσει προβλήματα. Η ακεραιότητα χάνεται εάν πραγματοποιούνται μη προγραμματισμένες αλλαγές είτε σκόπιμα, είτε τυχαία ή όταν τμήματα του εξοπλισμού παρουσιάζουν ελαττωματική λειτουργία ή ακόμα και όταν έχουν γίνει σφάλματα στο σχεδιασμό του έργου. Η απώλεια ακεραιότητας στη βάση δεδομένων του συστήματος ή στο λογισμικό του και ο μη έγκαιρος εντοπισμός των σφαλμάτων μπορεί να οδηγήσει σε ανακρίβειες, απάτες σε βάρος του οργανισμού ή σε λανθασμένες αποφάσεις από τη διοίκηση εξαιτίας της χρήσης αλλοιωμένων πληροφοριών. Επίσης, η παραβίαση της ακεραιότητας μπορεί να αποτελέσει το πρώτο βήμα σε μια επιτυχή επίθεση ενάντια στη διαθεσιμότητα ή την εμπιστευτικότητα των συστημάτων. Η δυσλειτουργία λογισμικού και υλικού θα επιβαρύνουν τον αρχικό προϋπολογισμό για την υλοποίηση του έργου αλλά και θα προκαλέσουν μεγάλες καθυστερήσεις στην ολοκλήρωση αυτού. Και πάλι με αυτόν τον τρόπο προσβάλλεται η διαθεσιμότητα των συστημάτων.

- ***<u>Απώλεια διαθεσιμότητας.</u>*** Τμήματα του πληροφοριακού συστήματος ή και ολόκληρο το σύστημα δεν είναι διαθέσιμο είτε διότι δεν έχουν ολοκληρωθεί οι εργασίες εγκατάστασής του βάση των χρονοδιαγραμμάτων, είτε διότι παρουσίασε σφάλματα κατά τη χρήση του και τέθηκε εκτός λειτουργίας έως ότου διορθωθεί το πρόβλημα. Η απώλεια της διαθεσιμότητας μπορεί να είναι, όπως είδαμε παραπάνω, απόρροια της απώλειας της ακεραιότητας του συστήματος. Όποια κι αν είναι η αιτία όμως, η ζημία για τον οργανισμό είναι πολύ μεγάλη καθώς χάνονται τα χρηματικά οφέλη που ενδεχομένως να αποκομίζονται από τη λειτουργία του συστήματος (π.χ. διακοπή παραγωγικής διαδικασίας, αδυναμία διάθεσης υπηρεσιών ή προϊόντων μέσω του διαδικτύου), αποδιοργανώνονται οι διαδικασίες του οργανισμού, χάνονται ευκαιρίες που θα βοηθούσαν στην ανάπτυξη και στην αύξηση των κερδών του, ενώ παράλληλα πλήττεται και το κύρος και η αξιοπιστία του οργανισμού. Το είδος και το επίπεδο των απωλειών εξαρτάται από το είδος του οργανισμού και τους σκοπούς που εξυπηρετεί το

πληροφοριακό σύστημα, γίνεται όμως φανερό, πόσο σημαντική είναι η τήρηση των χρονοδιαγραμμάτων για την ολοκλήρωση του έργο, η πρόληψη για την αποφυγή σφαλμάτων και παραλήψεων που θα θέσουν το σύστημα εκτός λειτουργίας, αλλά και η πρόβλεψη για την άμεση αποκατάσταση της διαθεσιμότητας του συστήματος σε περίπτωση που τελικά δεν αποφευχθεί η διακοπή της λειτουργίας του.

- ***Απώλεια εμπιστευτικότητας.*** Η εμπιστευτικότητα συστημάτων και δεδομένων αναφέρεται στην προστασία των πληροφοριών από μη εξουσιοδοτημένη κοινοποίηση. Οι επιπτώσεις μιας τέτοιας κοινοποίησης μπορούν να κυμανθούν από τη διακινδύνευση της εθνικής ασφάλειας έως την απώλεια αιφνιδιασμού της αγοράς από την εισαγωγή ενός νέου προϊόντος ή τη μείωση των τιμών και γενικά οποιαδήποτε ενέργεια που δεν αναμένουν οι ανταγωνιστές. Μπορούν ακόμα να διαρρεύσουν τα μελλοντικά σχέδια του οργανισμού επιτρέποντας στους ανταγωνιστές να προετοιμάσουν τα δικά τους σχέδια ή ακόμα και να γνωστοποιηθούν ευαίσθητα προσωπικά δεδομένα στελεχών του οργανισμού ή άλλων προσώπων, στοιχεία των οποίων υπάρχουν στις βάσεις δεδομένων του συστήματος. Πέραν όλων των άλλων η μη εξουσιοδοτημένη, παράνομη ή ακούσια δημοσιοποίηση τέτοιων πληροφοριών θα μπορούσε να οδηγήσει στην απώλεια της δημόσιας εμπιστοσύνης, την αμηχανία της διοίκησης ή ακόμα και τη λήψη νομικής δράσης ενάντια στον οργανισμό, για κοινοποίηση ευαίσθητων προσωπικών δεδομένων που διατηρούσε στη βάση δεδομένων του και που αφορούν τρίτα πρόσωπα, είτε αυτά ανήκουν στον οργανισμό είτε όχι. Ένα παράδειγμα αποτελεί η διαρροή του ιστορικού ασθενών που νοσηλεύθηκαν σε κάποιο ιδιωτικό νοσοκομείο και το οποίο βρισκόταν στη βάση δεδομένων του νοσοκομείου.

Οι επιπτώσεις που απορρέουν από την εμφάνιση των κινδύνων δε μπορούν πάντα να μετρηθούν και να αποτιμηθούν. Οι επιπτώσεις από την καταστροφή υλικού ή λογισμικού μπορούν να αποτιμηθούν από το κόστος αγοράς και εγκατάστασης νέου εξοπλισμού και από την καθυστέρηση με την οποία επιβαρύνει την εξέλιξη του έργου. Γενικά οι επιπτώσεις που επιφέρουν επιπλέον κόστος ή

καθυστερήσεις είναι εύκολο να ποσοτικοποιηθούν και να εκτιμηθεί η σοβαρότητά τους. Επιπτώσεις όμως, όπως η απώλεια ευκαιριών σε μια ανταγωνιστική αγορά, η απώλεια μονοπωλίου, η καθυστέρηση στην παράδοση προϊόντων ή στην παροχή υπηρεσιών και η επικείμενη δυσαρέσκεια των πελατών, η προσβολή του κύρους και της αξιοπιστίας του οργανισμού, η δημιουργία τριβών στη σχέση της διοίκησης με το προσωπικό, δε μπορούν να ποσοτικοποιηθούν. Αυτές θα πρέπει αξιολογηθούν ποιοτικά. Για το σκοπό αυτό μπορούμε να κατατάξουμε τις επιπτώσεις από τον κάθε κίνδυνο σε κάποιον από τους παρακάτω πέντε χαρακτηρισμούς:

1. Πολύ Σοβαρές
2. Σοβαρές
3. Μέτριες
4. Ελεγχόμενες
5. Αμελητέες

Καθένα από τα παραπάνω επίπεδα περιγράφει τη σοβαρότητα των επιπτώσεων, που επιφέρει η εμφάνιση ενός κινδύνου, για τον οργανισμό. Μπορούμε να αντιστοιχίσουμε στις πέντε αυτές διαβαθμίσεις την κλίμακα που χρησιμοποιήσαμε και για την πιθανότητα εμφάνισης ενός κινδύνου. Αντί αυτής όμως θα χρησιμοποιήσουμε μια μη γραμμική κλίμακα η οποία τονίζει περισσότερο την επιθυμία των διοικούντων του οργανισμού να αποφύγουν κινδύνους με πολύ σοβαρές συνέπειες. Η νέα κλίμακα είναι 0.05 , 0.1 , 0.2 , 0.4 , 0.8. Η κλίμακα αυτή θα μπορούσε να διαφοροποιηθεί και να προσαρμοστεί στα ζητούμενα του κάθε οργανισμού.

Το Σχήμα 30 δίνει μια περιγραφή της σημασίας του κάθε επιπέδου κινδύνου [22]:

Αξιολόγηση επιπτώσεων κινδύνων στους ευπαθείς τομείς ενός έργου					
Ευπαθείς τομείς	**Αμελητέες 0.05**	**Ελεγχόμενες 0.1**	**Μέτριες 0.2**	**Σοβαρές 0.4**	**Πολύ Σοβαρές 0.8**
Κόστος	Αμελητέα αύξηση του κόστους	Αύξηση κόστους <5%	Αύξηση κόστους 5-10%	Αύξηση κόστους 10-20%	Αύξηση κόστους >20%
Χρονοδιά-γραμμα	Αμελητέα ολίσθηση χρον/τος	Ολίσθηση χρον/τος <5%	Ολίσθηση χρον/τος 5-10%	Ολίσθηση χρον/τος 10-20%	Ολίσθηση χρον/τος >20%
Σκοπός	Μικρή παρέκκλιση από το στόχο ελάχιστα παρατηρήσιμη	Μικρά τμήματα του στόχου έχουν επηρεαστεί	Μεγάλα τμήματα του στόχου έχουν επηρεαστεί	Παρέκκλιση από το στόχο σε μη αποδεκτά επίπεδα για τον αγοραστή	Το έργο που παρήχθη είναι λειτουργικά άχρηστο
Ποιότητα	Υποβιβασμός της ποιότητας	Μόνο πολύ	Μείωση της ποιότητας απαιτείται	Μείωση της ποιότητας	Το έργο που παρήχθη

	ελάχιστα παρατηρήσιμος	απαιτητικές εφαρμογές επηρεάζονται	έγκριση από τον αγοραστή	σε μη αποδεκτά επίπεδα για τον αγοραστή	δεν μπορεί να χρησιμοποιηθεί

Σχήμα 30: Επίπεδο επιπτώσεων ανά ευπαθή τομέα ενός έργου

Στον παραπάνω πίνακα παρουσιάζονται οι επιπτώσεις των κινδύνων σε βάρος της πορείας υλοποίησης του πληροφοριακού συστήματος. Πέραν αυτών όμως θα πρέπει να εκτιμώνται και οι επιπτώσεις στη λειτουργία του οργανισμού από την ενδεχόμενη εμφάνιση κάποιων κινδύνων. Οι επιπτώσεις αυτές βέβαια πηγάζουν από την προσβολή κάποιου από τους παραπάνω τέσσερις ευπαθείς τομείς. Το επιπλέον κόστος ανάλογα με την αρχική συμφωνία μπορεί να επιβαρύνει είτε την ανάδοχο εταιρία είτε τον ίδιο τον οργανισμό. Η μη τήρηση των χρονοδιαγραμμάτων σημαίνει πως πλήττεται η διαθεσιμότητα του έργου. Η παρέκκλιση από τους αρχικούς στόχους που θα πρέπει να εκπληρώνει το νέο λογισμικό, πλήττει ουσιαστικά εξαρχής την ακεραιότητα του έργου ενώ η υποβάθμιση της ποιότητάς του δημιουργεί αμφιβολίες για την ασφαλή (ακεραιότητα – εμπιστευτικότητα) και εποικοδομητική λειτουργία του συστήματος.

Παράλληλα, ιδιαίτερη σημασία έχει και η πρόβλεψη μιας αλυσίδας επιπτώσεων. Δηλαδή η εμφάνιση ενός κινδύνου μπορεί να προκαλεί προβλήματα σε περισσότερους του ενός τομείς του έργου. Για παράδειγμα μπορεί η δυσλειτουργία ενός τμήματος του έργου να απαιτεί την αντικατάσταση ή την επιπλέον επεξεργασία του εξοπλισμού γεγονός όμως που θα επηρεάσει και το κόστος και το χρόνο υλοποίησης του έργου αλλά πιθανώς και την ποιότητα αυτού.

Συνεπώς, γίνεται φανερό πως για την ορθή αξιολόγηση των επιπτώσεων θα πρέπει να συνυπολογίζονται και οι ιδιαίτερες συνθήκες που διέπουν τη λειτουργία του κάθε έργου πληροφορικής. Για παράδειγμα για έναν οργανισμό που εκτελεί δημοπρασίες μέσω διαδικτύου η καθυστέρηση παράδοσης του έργου ή η αναγκαστική διακοπή της λειτουργίας τμημάτων που έχουν ήδη παραδοθεί, για επιδιορθώσεις λόγω εσφαλμένης λειτουργίας ή λόγω δυσκολίας διασύνδεσης με τα

υπόλοιπα τμήματα του έργου που είναι υπό παράδοση, μπορεί να επιφέρει τεράστιες οικονομικές απώλειες για τον οργανισμό από την αδυναμία διάθεσης των προϊόντων του, ενώ κάποιες προσαυξήσεις στο κόστος παραγωγής ή κάποιες παραχωρήσεις στην ποιότητα του έργου, ενδεχομένως να μην αποτελούσαν σημαντικά πλήγματα. Αντίστοιχα η δικτυακή οργάνωση της μισθοδοσίας ενός τομέα του δημοσίου δε θα είχε ιδιαίτερη επιβάρυνση από κάποια ολιγοήμερη καθυστέρηση στην ολοκλήρωση των εργασιών, καθώς απλώς θα καθυστερούσε ο εκσυγχρονισμός των διαδικασιών, ενώ οι μισθοδοσίες θα πραγματοποιούνταν και θα καταγράφονταν με τις ήδη υπάρχουσες μεθόδους.

Ιδιαίτερη αντιμετώπιση θα πρέπει να έχουν και τα αντίστοιχα τμήματα του ίδιου του έργου. Διαφορετική βαρύτητα έχουν οι παραχωρήσεις στην ασφάλεια οικονομικών συναλλαγών και διαφορετική στην ασφάλεια παρουσίασης διαφημιστικού υλικού. Επίσης διαφορετικές είναι οι επιπτώσεις από την πτώση ενός server και διαφορετικές από τη δυσλειτουργία ενός τερματικού.

Από όλα τα παραπάνω αντιλαμβανόμαστε την ανάγκη συνεργασίας με τη διοίκηση του οργανισμού για την ορθή κατηγοριοποίηση των επιπτώσεων από την εμφάνιση ενός κινδύνου, καθώς η κάθε περίπτωση απαιτεί τη δική της ιδιαίτερη αντιμετώπιση, αλλά και αίτηση της συμβολής ειδικών σε τεχνικά θέματα για την κατανόηση της σημασίας και της δυσκολίας αντιμετώπισης των προβλημάτων που μπορεί να αντιμετωπίζει το κάθε τμήμα του έργου.

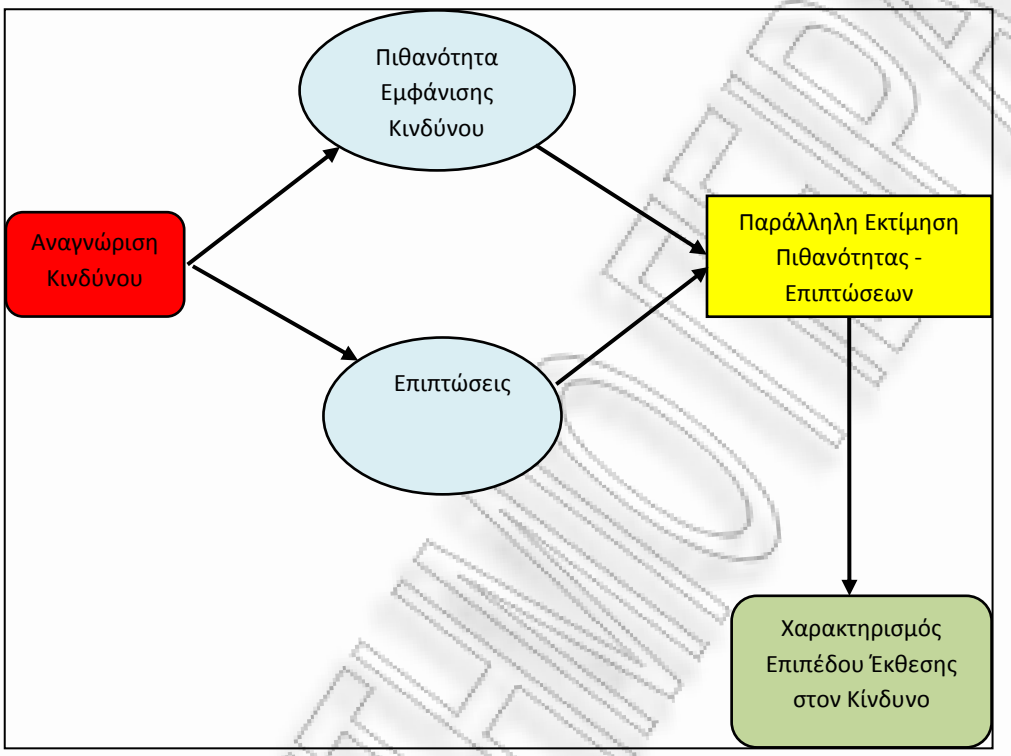
5.2.3 Χαρακτηρισμός Επιπέδου Έκθεσης σε Κάθε Κίνδυνο

Σκοπός του βήματος αυτού είναι να αξιολογηθεί το επίπεδο κινδύνου για το υπό κατασκευή πληροφοριακό σύστημα [15]. Η αξιολόγηση αυτή θα πραγματοποιηθεί μέσω της παράλληλης εξέτασης της πιθανότητας εμφάνισης ενός κινδύνου και των επιπτώσεων αυτού και μπορεί να εκφραστεί από:

- Την πιθανότητα κάποια δεδομένη πηγή κινδύνου να επιδιώξει να επιφέρει κάποια δυσμενή επίπτωση
- Το μέγεθος των επιπτώσεων από μια τέτοια επιτυχημένη προσπάθεια

- Η επάρκεια των προγραμματιζόμενων ή υπαρχόντων ελέγχων ασφαλείας για τη μείωση ή την εξάλειψη του κινδύνου

Τα παραπάνω συνοψίζονται στο Σχήμα 31:



Σχήμα 31: Διαδικασία αξιολόγησης επιπέδου έκθεσης σε κίνδυνο

Για την εκτίμηση της σοβαρότητας ενός κινδύνου συνυπολογίζεται η πιθανότητα εμφάνισης με το επίπεδο των επιπτώσεων. Για να επιτευχθεί αυτό πολλαπλασιάζουμε τις τυποποιημένες τιμές που υπολογίσαμε προηγουμένως για πιθανότητα και επίπτωση και ανάλογα με το αριθμητικό αποτέλεσμα χαρακτηρίζουμε τον κίνδυνο υψηλής, μέτριας ή χαμηλής σημασίας. Στο Σχήμα 32 παρουσιάζονται τα αποτελέσματα από το συνδυασμό όλων των επιπέδων πιθανότητας εμφάνισης και επιπτώσεων [22]:

Αριθμητικά αποτελέσματα συνυπολογισμού των διαφόρων επιπέδων πιθανότητας και επιπτώσεων					
Πιθανότητα	***Βαθμολογία επιπέδου έκθεσης σε κίνδυνο***				
0.9	0.05	0.09	0.18	0.36	0.72
0.7		0.07	0.14	0.28	0.56
0.5		0.05	0.10	0.20	0.40
0.3			0.06	0.12	0.24
0.1					0.08
	0.05	***0.10***	***0.20***	***0.40***	***0.80***
	Επιπτώσεις σε ένα συγκεκριμένο τομέα (π.χ. κόστος, χρόνος, ποιότητα) (μη γραμμική κλίμακα)				

Σχήμα 32: Αριθμητικά αποτελέσματα συνυπολογισμού των διαφόρων επιπέδων πιθανότητας και επιπτώσεων

Ο χαρακτηρισμός των κινδύνων ως υψηλού επιπέδου (κόκκινο), μετρίου (κίτρινο), ή χαμηλού (πράσινο), διαφαίνεται μέσω των χρωμάτων των κελιών του πίνακα όπως προκύπτουν από τα αριθμητικά αποτελέσματα των υπολογισμών.

Το Σχήμα 33 παρουσιάζει τι αντιπροσωπεύει το κάθε επίπεδο κινδύνου:

Επίπεδο κινδύνου	***Περιγραφή κινδύνου και απαραίτητες ενέργειες***
Υψηλό	Εάν μία κατάσταση αξιολογείται ως υψηλός κίνδυνος, τότε υπάρχει ισχυρή ανάγκη για διορθωτικά μέτρα. Ενδεχομένως τα μέτρα αυτά να μην επαρκούν και να αποφασιστεί η ματαίωση υλοποίησης του έργου. Αν τελικά το υπάρχον σύστημα μπορεί να συνεχίσει να λειτουργεί, ένα πρόγραμμα διορθωτικής δράσης πρέπει να τεθεί σε ισχύ το συντομότερο δυνατόν
Μέτριο	Εάν μία κατάσταση εκτιμάται ως μέσος κίνδυνος, διορθωτικές ενέργειες απαιτούνται και ένα σχέδιο πρέπει να αναπτυχθεί για να ενσωματώσει αυτές τις ενέργειες εντός μιας λογικής χρονικής περιόδου.

Χαμηλό	Εάν μία κατάσταση περιγράφεται ως χαμηλός κίνδυνος, η διοίκηση του οργανισμού πρέπει να καθορίσει αν θα γίνουν διορθωτικές ενέργειες ή αποφασίζει να δεχτεί τον κίνδυνο.

Σχήμα 33: Περιγραφή επιπέδων κινδύνου

Τέλος, οι έξοδοι από αυτή την παραπάνω διαδικασία αξιολόγησης επιπέδου έκθεσης στους κινδύνους είναι οι εξής [22]:

- ***Συνολικό επίπεδο έκθεσης σε κινδύνους του έργου***

Το επίπεδο κινδύνου μπορεί να παρουσιάσει τη συνολική έκθεση σε κίνδυνο του έργου σχετικά με άλλα πληροφοριακά έργα συγκρίνοντας το αριθμητικό αποτέλεσμα του συνυπολογισμού πιθανότητας – επιπτώσεων. Μπορεί να χρησιμοποιηθεί για την ορθή κατανομή προσωπικού και πόρων σε τμήματα του έργου με διαφορετική διαβάθμιση κινδύνου, ή και μεταξύ διαφορετικών έργων που έχει αναλάβει η ίδια εταιρία, για τη λήψη αποφάσεων σχετικών με ανάλυση οφέλους - κόστους για το έργο και για την υποστήριξη προτάσεων για εκκίνηση, συνέχιση ή ματαίωση της υλοποίησης του έργου λογισμικού.

- ***Λίστα κινδύνων βάση προτεραιότητας***

Οι κίνδυνοι μπορούν να καταταχθούν με την χρήση ενός πλήθους κριτηρίων. Αυτά μπορεί να είναι το επίπεδο κινδύνου (υψηλό, μέτριο και χαμηλό) ή ο βαθμός στον οποίο μπορεί να προκαλέσει απώλεια εργασίας. Οι κίνδυνοι μπορούν ακόμα να κατηγοριοποιηθούν σε αυτούς που απαιτούν άμεση επέμβαση και σε αυτούς των οποίων ο χειρισμός μπορεί να γίνει και στο μέλλον χωρίς επιπρόσθετες επιπτώσεις. Κίνδυνοι που αφορούν το κόστος, τις χρονοτριβές, τη λειτουργικότητα και την ποιότητα μπορούν να εξεταστούν ξεχωριστά χρησιμοποιώντας διαφορετική αξιολόγηση του επιπέδου τους. Σοβαροί κίνδυνοι πρέπει να έχουν επιπλέον περιγραφή για τη βάση της εκτιμώμενης πιθανότητας και των επιπτώσεών τους.

- ***Λίστα κινδύνων που απαιτούν επιπλέον ανάλυση και διαχείριση***

Κίνδυνοι που έχουν χαρακτηριστεί ως υψηλοί ή μέτριοι είναι σοβαροί υποψήφιοι για περισσότερη ανάλυση, συμπεριλαμβανομένης και ποσοτικής ανάλυσης κινδύνου και διενέργεια διαχείρισης κινδύνων.

- ***Τάση αποτελεσμάτων ποιοτικής ανάλυσης κινδύνων***

Καθώς η ανάλυση επαναλαμβάνεται, μπορεί να γίνει φανερή κάποια τάση των αποτελεσμάτων της που θα κάνει την αντίδραση έναντι του κινδύνου ή την επιπλέον ανάλυσή του περισσότερο ή λιγότερο επιτακτική και σημαντική.

5.3 Ποσοτική Ανάλυση Κινδύνου

Η ποσοτική ανάλυση κινδύνων θεωρείται περισσότερο επιστημονική μέθοδος ανάλυσης των κινδύνων, καθώς, σε αντίθεση με την ποιοτική ανάλυση, βασίζεται σε μαθηματικούς υπολογισμούς [11, 15]. Αυτό δεν είναι ακριβές, καθώς η αξία της ποιοτικής ανάλυση είναι εξίσου μεγάλη, ιδιαίτερα όταν ο χρόνος και οι ανθρώπινοι πόροι είναι περιορισμένοι.

Η διαδικασία αυτή χρησιμοποιεί διάφορες τεχνικές για να:

- Υπολογίσει την πιθανότητα επίτευξης ενός συγκεκριμένου στόχου του έργου.
- Ποσοτικοποιήσει την έκθεση σε κίνδυνο του έργου και να υπολογίσει τον επιπλέον χρόνο και το επιπλέον κόστος που ενδεχομένως να απαιτείται.
- Αναγνωρίσει τους κινδύνους που απαιτούν τη μεγαλύτερη προσοχή ποσοτικοποιώντας τη συμβολή τους στη συνολική έκθεση σε κίνδυνο του έργου.
- Αναγνωρίσει ρεαλιστικούς και πραγματοποιήσιμους στόχους για το κόστος, το χρόνο, τις δυνατότητες και την ποιότητα του έργου.

Η ποσοτική ανάλυση κινδύνου συνήθως έπεται χρονικά της ποιοτικής. Απαιτεί πρώτα από όλα τον πλήρη καθορισμό του κινδύνου. Η ποιοτική και η ποσοτική αξιολόγηση κινδύνων μπορούν να χρησιμοποιούνται διακριτά ή και μαζί. Η συνεκτίμηση του χρόνου και των κονδυλίων που είναι διαθέσιμα και η ανάγκη για ποιοτικές ή ποσοτικές εκθέσεις για τον κίνδυνο και τις επιπτώσεις του, θα

καθορίσουν ποια μέθοδος θα χρησιμοποιηθεί. Η τάση των αποτελεσμάτων της ποσοτικής διαδικασίας καθώς αυτή επαναλαμβάνεται, θα υποδείξει την ανάγκη για περισσότερη ή λιγότερη διενέργεια διαχείρισης κινδύνου.

5.3.1 Επιθυμητά Στοιχεία για την Ποσοτική Αξιολόγηση Κινδύνου

Τα επιθυμητά στοιχεία που χρειάζονται για την όσο το δυνατό πιο πλήρη και ορθή ποσοτική ανάλυση των κινδύνων είναι τα εξής [22]:

- ***Σχεδιασμός εκτίμησης κινδύνων***. Περιγράφει με ποιο τρόπο σχεδιάζονται, εφαρμόζονται και ελέγχονται, οι διαδικασίες αναγνώρισης κινδύνων και ποιοτικής και ποσοτικής τους ανάλυσης καθ' όλη τη διάρκεια υλοποίησης του έργου.
- ***Κατάλογος αναγνωρισμένων κινδύνων.***
- ***Κατάλογος σημαντικότερων κινδύνων.***
- ***Κατάλογος κινδύνων που χρειάζονται επιπλέον ανάλυση.***
- ***Πληροφορίες πρότερης πείρας***. Πληροφορίες από παλαιότερα, παρόμοια ολοκληρωμένα έργα, μελέτες για παρόμοια έργα από ειδικούς σε θέματα κινδύνων ή σε τεχνολογικά θέματα και βάσεις δεδομένων που μπορεί να είναι διαθέσιμες από άλλες βιομηχανικές ή ιδιωτικές πηγές.
- ***Απόψεις ειδικών***. Αυτές μπορεί να προέρχονται από τα μέλη της ομάδας που έχει αναλάβει το σχεδιασμό του έργου, από άλλους ειδικούς στο αντικείμενο που ανήκουν στην εταιρία αλλά και από πρόσωπα που δεν ανήκουν στο δυναμικό της (π. χ μηχανικοί και στατιστικολόγοι).
- ***Αποτελέσματα ποιοτικής αξιολόγησης κινδύνων*** (εάν αυτή έχει προηγηθεί).
- ***Αποτελέσματα άλλων εκθέσεων***. Εκθέσεις που θα μπορούσαν να φανούν ιδιαίτερα χρήσιμες είναι αυτές που αφορούν στον υπολογισμό της διάρκειας ολοκλήρωσης του κάθε τμήματος του έργου για την κατάρτιση του συνολικού χρονοδιαγράμματος υλοποίησης του έργου, το σχηματισμό καταλόγου με τα έξοδα του έργου και του τρόπου

υπολογισμού αυτών και τη δημιουργία μοντέλων των τεχνικών δυνατοτήτων του έργου.

5.3.2 Μέθοδοι ποσοτικής ανάλυσης κινδύνων

Υπάρχουν διάφορες μέθοδοι ποσοτικής ανάλυσης κινδύνων, αλλά αυτές που συχνότερα χρησιμοποιούνται ακολουθούν αναλυτικά παρακάτω [11]:

- ***Αναμενόμενη τιμή***

Δεδομένου ότι ένα συγκεκριμένο γεγονός είτε θα προκύψει είτε όχι, δεν έχει νόημα να εστιαζόμαστε στην αναμενόμενη τιμή ενός συγκεκριμένου γεγονότος ανεξάρτητα από τα υπόλοιπα. Αντιθέτως, αν συνδυαστούν οι αναμενόμενες τιμές πολλών πιθανών γεγονότων, τότε μπορεί να προκύψει μια αναμενόμενη τιμή που θα είναι εκείνη που περιμένουμε συνολικά να προκύψει ως αποτέλεσμα όλων των πιθανών γεγονότων σε ένα έργο. Το τελευταίο στοιχείο είναι σημαντικό και μπορεί να βοηθήσει στην πρόγνωση της εξέλιξης ενός πληροφοριακού συστήματος.

Ένα παράδειγμα της αναμενόμενης τιμής είναι η έκθεση ενός κινδύνου, η οποία υπολογίζεται από το γινόμενο της ***πιθανότητας εμφάνισης*** και της ***συνέπειας*** που θα προκύψει. Επειδή, όπως αναφέρθηκε παραπάνω δεν επιφέρει αποτέλεσμα να εξετάζουμε την μεμονωμένη αναμενόμενη τιμή ενός κινδύνου, υποθέτουμε ότι υπάρχουν ‘n’ αβέβαια γεγονότα (κίνδυνοι) και η συνολική αναμενόμενη τιμή ή αλλιώς συνολική έκθεση θα είναι:

$$Eσ = \sum_{j=1}^{n} (Πj * Σj)$$

Η συνέπεια μπορεί να εκφράζεται με πρόσημο και η συνήθης σύμβαση είναι η απειλή να εκφράζεται με θετικό πρόσημο, ενώ η ευκαιρία με αρνητικό. Ωστόσο, δεν εκφράζεται απαραίτητα σε μονάδες κόστους. Συχνά, εκφράζεται σε μονάδες χρόνου και σπανιότερα σε άλλες ειδικές μετρικές (π. χ μονάδες απόδοσης).

Όπως φαίνεται στον Σχήμα 34, η συνολική έκθεση του έργου είναι 12.900€. Αυτή η τιμή στην πράξη είναι ένας δείκτης, καθώς δε πρόκειται ποτέ να προκύψει αυτή η τιμή. Παρόλα αυτά, αν θεωρήσουμε ότι, με βάση τις πιθανότητες, κάποιοι

κίνδυνοι από αυτούς που αναφέρονται θα προκύψουν και κάποιοι όχι, η συνολική έκθεση που υπολογίστηκε θα βρίσκεται κοντά στο τελικό, πραγματικό αποτέλεσμα. Αυτό φυσικά ισχύει με την προϋπόθεση ότι η συνέπεια κάθε κινδύνου έχει υπολογιστεί σωστά.

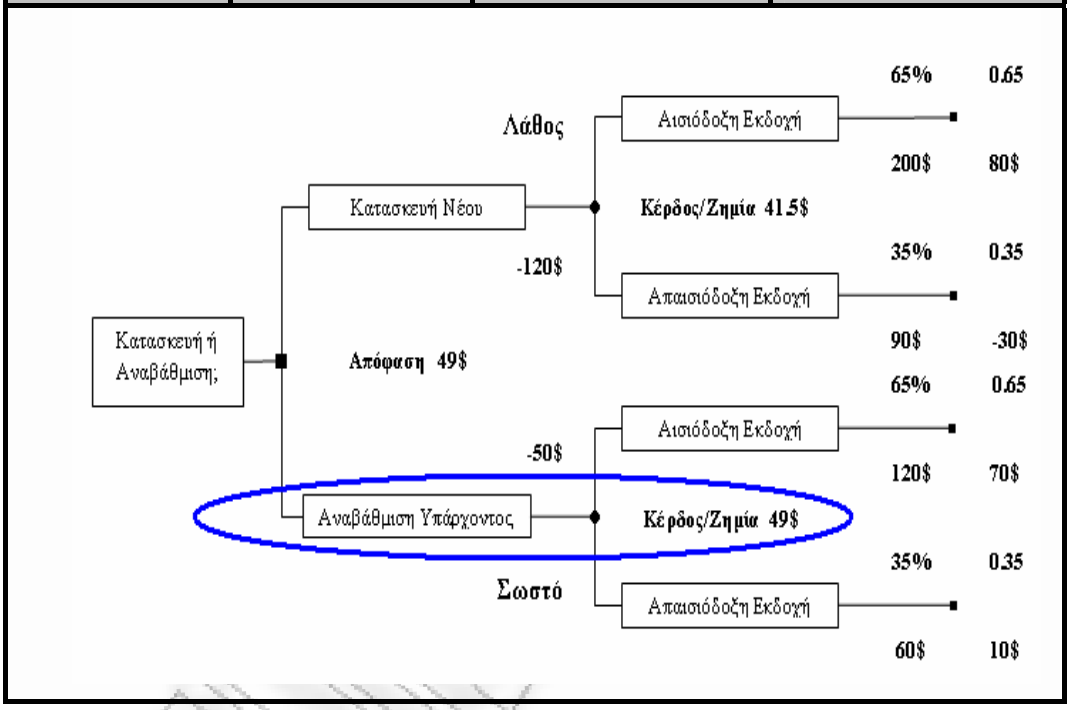
Κωδικός Κινδύνου	Πιθανότητα Εμφάνισης (%)	Συνέπεια (€)	Έκθεση (€)
A5	50	5.000	2.500
B6	60	6.000	3.600
B7	30	-10.000	-3.000
B9	30	30.000	9.000
Γ3	10	8.000	800
		Συνολική Έκθεση	***12.900***

Σχήμα 34: Παράδειγμα υπολογισμού Συνολικής Έκθεσης Κινδύνου

- ***Δέντρα Αποφάσεων***

Τα δέντρα αποφάσεων είναι διαγράμματα που περιγράφουν τη διαδικασία λήψης μιας απόφασης λαμβάνοντας υπόψη τις εναλλακτικές επιλογές που είναι διαθέσιμες. Συνυπολογίζουν τις πιθανότητες εμφάνισης των κινδύνων και τα κόστη ή τα κέρδη από κάθε λογική διαδρομή γεγονότων ή μελλοντικών αποφάσεων. Η χρήση ενός δέντρου αποφάσεων μας παρέχει την απόφαση με το μεγαλύτερο αναμενόμενο κέρδος όταν όλοι οι αβέβαιοι παράγοντες, το κόστος, το κέρδος και οι εναλλακτικές αποφάσεις έχουν ποσοτικοποιηθεί. Σε μεγάλα όμως συστήματα, όπου τα δέντρα αποφάσεων μπορούν να γίνουν πολύ μεγάλα, εξυπηρετεί ιδιαίτερα η χρήση ειδικού λογισμικού. Στο Σχήμα 35 δίνεται ένα παράδειγμα χρήσης ενός τέτοιου δέντρου αποφάσεων.

Ορισμός Απόφασης	Αποτίμηση Απόφασης	Αποτίμηση Επιλογής	Αποτίμηση Ενδεχομένου
(Όνομα Απόφασης)	(Κόστος Απόφασης)	(Πιθανότητα / Εκτιμώμενο Κέρδος/Ζημία)	(Πιθανότητα / Κέρδος/Ζημία = Οφέλη – Κόστος)



Σχήμα 35: Παράδειγμα δέντρου αποφάσεων

Το δέντρο αυτό μας δείχνει τις επιλογές που έχουμε, το κόστος υλοποίησης αυτών, τα οφέλη από αυτές με την πιθανότητα που τα συνοδεύουν και την τελικά πιο συμφέρουσα επιλογή βάση του αναμενόμενου κέρδους. Το αναμενόμενο κέρδος της κάθε επιλογής υπολογίζεται ως εξής:

Αναμενόμενο Κέρδος/Ζημία = Πιθανότητα Γεγονότος[1] * Κέρδος/Ζημία + Πιθανότητα Γεγονότος[2] * Κέρδος/Ζημία

Κέρδος/Ζημία = Όφελος - Κόστος

✓ Για την πρώτη επιλογή έχουμε:

Αναμενόμενο Κέρδος/ Ζημία = 0.65*(200-120) + 0.35*(90-120) = 41.5$

✓ Για τη δεύτερη επιλογή έχουμε:

Αναμενόμενο Κέρδος/ Ζημία = 0.65*(120-50) + 0.35*(60-50) = 49$

Επομένως, η πιο συμφέρουσα απόφαση βάση του αναμενόμενου κέρδους είναι η δεύτερη με κέρδος 49$.

➢ ***Προσομοίωση Monte Carlo***

Η προσομοίωση Monte Carlo είναι πιθανότατα η πιο γνωστή μέθοδος ποσοτικής ανάλυσης κινδύνων και βασίζεται στη θεωρία των τυχαίων αριθμών. Ιδιαίτερα όσον αφορά τη διαχείριση κινδύνων σε μεγάλα έργα, οι εφαρμογές της είναι σημαντικές και μπορούν να δώσουν αποτελέσματα ικανά να βοηθήσουν τη Διοίκηση του έργου στη λήψη μιας απόφασης [23]. Λόγω της δυσκολίας όμως που παρουσιάζεται κατά την εφαρμογή της, θα σταθούμε μόνο στο θεωρητικό μέρος της συγκεκριμένης μεθόδου.

Η μέθοδος Monte Carlo αρχικά αναπτύχθηκε για το Manhattan Project των Αμερικανικών ένοπλων δυνάμεων και τη προσπάθειά του να επιλύσει μοντέλα διάχυσης της ατομικής ενέργειας κατά τη διάρκεια του δευτέρου παγκοσμίου πολέμου. Παρόλα αυτά, τώρα εφαρμόζεται σε ένα ευρύ φάσμα προβλημάτων. Ουσιαστικά, επιλέγονται τυχαία τιμές για να δημιουργηθούν πιθανά σενάρια ενός προβλήματος. Αυτές οι τιμές λαμβάνονται μέσα από μια συγκεκριμένη κλίμακα και επιλέγονται για να αναπαραστήσουν τη διασπορά μιας πιθανότητας (π.χ. γραμμική διασπορά κλπ).

Στην προσομοίωση Monte Carlo, η διαδικασία τυχαίας επιλογής επαναλαμβάνεται πολλές φορές για να δημιουργήσει πολλαπλά σενάρια. Κάθε φορά που επιλέγεται τυχαία μια τιμή, διαμορφώνει ένα πιθανό σενάριο και ταυτόχρονα μια πιθανή λύση στο πρόβλημα. Μαζί αυτά τα σενάρια δίνουν μια σειρά των πιθανών λύσεων, μερικές από τις οποίες είναι περισσότερο και άλλες λιγότερο πιθανές. Όταν πλέον έχουν δημιουργηθεί πολλά σενάρια (10.000 ή

περισσότερα), η μέση λύση θα δώσει μια κατά προσέγγιση απάντηση στο πρόβλημα. Η ακρίβεια αυτής της απάντησης μπορεί να βελτιωθεί με την προσομοίωση περισσότερων σεναρίων. Στην πραγματικότητα, η ακρίβεια μιας προσομοίωσης Monte Carlo είναι ανάλογη προς την τετραγωνική ρίζα του αριθμού σεναρίων που χρησιμοποιήθηκαν. Η προσομοίωση Monte Carlo πλεονεκτεί ως μέθοδος καθώς παρέχει μια ωμή προσέγγιση, που είναι σε θέση να λύσει προβλήματα για τα οποία καμία άλλη λύση δεν υπάρχει. Δυστυχώς, αυτό επίσης σημαίνει ότι απαιτείται εντατική χρήση υπολογιστή και είναι καλύτερα να αποφεύγεται εάν απλούστερες λύσεις είναι εφικτές.

- ***Ανάλυση Ευαισθησίας***

Η ανάλυση ευαισθησίας είναι μια από τις πιο γνωστές τεχνικές που προσδιορίζει το μέγεθος της επιρροής καθεμίας από τις παραμέτρους ενός συστήματος στο ίδιο σύστημα [24]. Με τη χρήση αυτής της τεχνικής, μπορεί κανείς να προσδιορίσει ποιες είναι οι σημαντικές μεταβλητές ενός προβλήματος και να εστιάσει τη διαχείριση των κινδύνων σε αυτές. Η ανάλυση ευαισθησίας, χρησιμοποιείται, συνήθως, όταν η μονοσήμαντη εκτίμηση μιας μεταβλητής θεωρείται παρακινδυνευμένη. Ουσιαστικά, η ανάλυση ευαισθησίας βοηθά στο να καθοριστεί ποιοι κίνδυνοι έχουν τις ποιο σοβαρές αρνητικές επιπτώσεις στη λειτουργία του έργου. Εξετάζει την έκταση των επιπτώσεων στη λειτουργία του πληροφοριακού συστήματος από την εμφάνιση μιας απειλής, όταν οι υπόλοιποι κίνδυνοι δεν εκδηλώνονται.

- ***Τεχνική PERT/CPM***

Ένας από τους υψηλότερος κίνδυνος που ενέχει ένα έργο είναι ο χρονικός προγραμματισμός του. Οι δύο πιο γνωστές μεθοδολογίες για να γίνει ο προγραμματισμός αυτός είναι, η μεθοδολογία αξιολόγησης και παρακολούθησης έργου (**P**roject **E**valuation & **R**eview **T**echnique, **PERT**) και η μέθοδος κρίσιμης διαδρομής (**C**ritical **P**ath **M**ethod, **CPM**). Ουσιαστικά και οι δύο αυτές μεθοδολογίες στηρίζονται στην ίδια φιλοσοφία και αυτό έχει σαν αποτέλεσμα να θεωρούνται σαν

μία ενιαία μμέθοδος που βοηθά αντίστοιχα το κομμάτι της διαχείρισης κινδύνου ενός έργου.

Αν και η επιστημονική βάση των δύο μεθόδων δεν είναι καθόλου δύσκολο να γίνει κατανοητή από τους επιστήμονες, το κυριότερο πρόβλημα που συχνά εμφανίζεται κατά τη χρήση τους είναι η αδυναμία των στελεχών να παρακολουθήσουν και να κατανοήσουν τη στατιστική επεξεργασία. Προγράμματα λογισμικού επιπρόσθετα σε πακέτα προγραμματισμού έργων έχουν μετριάσει το πρόβλημα αυτό.

Η μέθοδος PERT, στηρίζεται στα χαρακτηριστικά των κατανομών που περιγράφουν τη στοχαστική διάρκεια κάθε δραστηριότητας. Ουσιαστικά στηρίζεται στο κεντρικό οριακό θεώρημα της θεωρίας των πιθανοτήτων και προσδιορίζει τη συνολική διάρκεια ενός έργου, βασιζόμενη στις κατανομές διάρκειας των δραστηριοτήτων της κρίσιμης διαδρομής.

Η τεχνική PERT αν και είναι η πιο τυπική περίπτωση διαχείρισης του κινδύνου ενός έργου που αφορά τη διάρκειά του, σαν μέθοδος δε θεωρείται πανάκεια. Ουσιαστικά, για να ισχύουν οι εκτιμήσεις της PERT, θα πρέπει όλες οι κατανομές που περιγράφουν τις διάρκειες των δραστηριοτήτων του έργου να είναι όλες ίδιες κάτι το οποίο δε μπορεί πάντα να συμβαίνει. Επίσης, η μέθοδος PERT δε μπορεί να χειριστεί αποτελεσματικά την καθυστέρηση που προκαλεί η ύπαρξη διακριτών κινδύνων (π.χ πιθανότητα να καθυστερήσει η εισαγωγή του Π.Σ 50 ημέρες). Τα προβλήματα αυτά διορθώνονται με τη χρήση της προσομοίωσης Monte Carlo, η οποία αν και απαιτεί περισσότερο χρόνο και τεχνική γνώση, μπορεί να παρακάμψει τα προβλήματα που δεν μπορεί να διαχειριστεί η PERT.

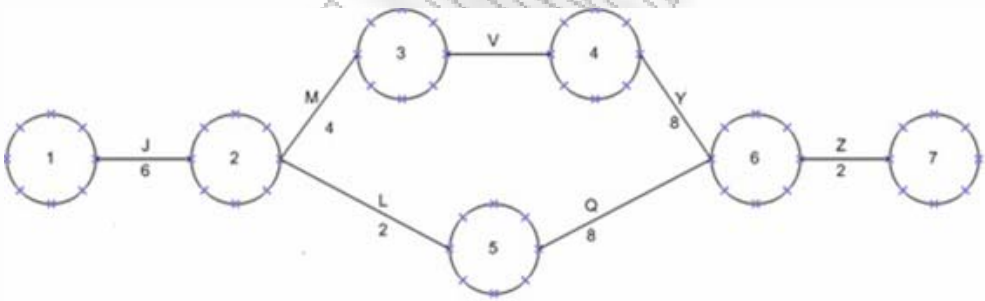
Παρ ΄ όλο που και οι δύο μέθοδοι χρησιμοποιούν την έννοια της κρίσιμης διαδρομής διαφέρουν σε κάποια σημεία. Για παράδειγμα, η CPM χρησιμοποιείται μόνο για εκτίμηση χρόνου για κάθε δραστηριότητα και δεν υπάρχει χρήση στατιστικής για την αβεβαιότητα. Επίσης, η CPM περιλαμβάνει μια μαθηματική διαδικασία ανταλλαγής μεταξύ της διάρκειας του έργου και του κόστους του και τονίζει την ανάλυση της ανακατανομής των πόρων από μια εργασία σε άλλη για να επιτευχθεί η μεγαλύτερη μείωση στη διάρκεια του έργου με το λιγότερο κόστος.

Στο παρακάτω σχήμα εμφανίζεται μια πρωτότυπη μορφή των διαγραμμάτων PERT οι ακμές του οποίου αντιστοιχούν σε δραστηριότητες και οι κορυφές

αντιστοιχούν σε ορόσημα, δηλαδή περιστατικά που δηλώνουν την ολοκλήρωση κάποιων δραστηριοτήτων. Τα ορόσημα αριθμούνται έτσι ώστε τα τελικά ορόσημα κάθε δραστηριότητας να έχουν μεγαλύτερη τάξη από τα αρχικά ορόσημα. Καμία δραστηριότητα δεν μπορεί να ξεκινήσει πριν όλες οι προηγούμενες δραστηριότητες ολοκληρωθούν και τα αντίστοιχα ορόσημα παραχθούν.

Ο χρόνος ολοκλήρωσης μιας δραστηριότητας σε ένα διάγραμμα PERT θεωρείται τυχαία μεταβλητή που ακολουθεί μια κατανομή b (βήτα). Αν κάθε δραστηριότητα της κρίσιμης διαδρομής περιγράφεται από μια κατανομή με αισιόδοξη τιμή a, και απαισιόδοξη τιμή b, τότε υπολογίζεται ότι η μέση τιμή της κατανομής (προσδοκώμενος χρόνος δραστηριοτήτων) είναι ***m = (a + 4m + b)/6***.

Η κρίσιμη διαδρομή (critical path) ενός διαγράμματος PERT, δηλαδή η μεγαλύτερη από άποψη χρόνου ολοκλήρωσης διαδρομή που οδηγεί από το ορόσημο έναρξης στο ορόσημο ολοκλήρωσης του έργου, είναι ίση με την προσδοκώμενη χρονική διάρκεια ολοκλήρωσης του έργου. Στη περίπτωσή μας critical path είναι η διαδρομή (J – M – V – Y –Z).



Σχήμα 36: Παράδειγμα διαγράμματος PERT

5.3.3 Αποτελέσματα από την Ποσοτική Αξιολόγηση Κινδύνων:

Τα αποτελέσματα της ποσοτικής αξιολόγησης κινδύνων είναι τα εξής [22]:

- ***Λίστα κινδύνων με προτεραιότητα, που πηγάζει από την ποσοτική ανάλυση***. Η λίστα αυτή περιλαμβάνει τους κινδύνους που αποτελούν τη μεγαλύτερη απειλή για το πληροφοριακό σύστημα, μαζί με το υπολογιζόμενο μέγεθος του αντίκτυπού τους.
- ***Την πιθανότητα επίτευξης των στόχων για το κόστος και το χρόνο ολοκλήρωσης του έργου***.

- ***Τάσεις των αποτελεσμάτων της ποσοτικής αξιολόγησης κινδύνων***. Καθώς επαναλαμβάνεται η διαδικασία, μπορεί να εμφανιστεί μία συγκεκριμένη τάση των αποτελεσμάτων.

5.4 Διαφορές Ποσοτικής έναντι Ποιοτικής Αξιολόγησης Κινδύνων

Κατά τη διαδικασία αξιολόγησης κινδύνων θα πρέπει να ληφθούν υπόψη τα πλεονεκτήματα και τα μειονεκτήματα της ποσοτικής έναντι της ποιοτικής ανάλυσης [11]. Το κύριο πλεονέκτημα της ποιοτικής ανάλυσης είναι ότι θέτει προτεραιότητες μεταξύ των κινδύνων και αναγνωρίζει τους τομείς του έργου που χρειάζονται άμεση βελτίωση, καταδεικνύοντας τις ευπαθείς περιοχές αυτού. Το μειονέκτημα της ποιοτικής ανάλυσης είναι ότι δεν παρέχει συγκεκριμένα υπολογίσιμα μεγέθη για την εκτίμηση του ύψους των επιπτώσεων, με αποτέλεσμα η ανάλυση κόστους-κέρδους για προτεινόμενες δράσεις να είναι πολύ δύσκολη.

Αντίθετα, η ποσοτική ανάλυση πλεονεκτεί σε αυτόν τον τομέα, καθώς μας παρέχει τέτοιου είδους πληροφορίες και διευκολύνει τις αναλύσεις κόστους-κέρδους δίνοντάς μας συγκεκριμένες τιμές για τα οφέλη της δράσης μας. Το μειονέκτημα της ποσοτικής ανάλυσης είναι ότι τα αριθμητικά αποτελέσματα ενδεχομένως να μην οδηγούν σε ξεκάθαρα συμπεράσματα, και να απαιτείται για το λόγο αυτό επιπλέον ποιοτική εξέταση των αποτελεσμάτων αυτών.

Για να έχουμε μια πιο ολοκληρωμένη εικόνα, θα πρέπει να προστεθεί στα παραπάνω πως το κόστος και η πολυπλοκότητα της ποσοτικής αξιολόγησης είναι υψηλότερα από τα αντίστοιχα της ποιοτικής.

Συνοψίζοντας, μπορούμε να πούμε πως η ποιοτική ανάλυση βασίζεται κυρίως στη λογική και την εμπειρία και τις δυνατότητες των προσώπων που την εκπονούν, ενώ η ποσοτική βασίζεται στα αριθμητικά αποτελέσματα και στην αξιοπιστία των μεθόδων και των μοντέλων προσομοίωσης που χρησιμοποιούνται. Όταν τίθεται θέμα κόστους χρησιμοποιείται μόνο η ποιοτική αξιολόγηση για την εξαγωγή συμπερασμάτων, ενώ όταν το κόστος δεν αποτελεί ανασταλτικό παράγοντα συνήθως εκπονούνται και οι δύο για την εξαγωγή ασφαλέστερων συμπερασμάτων.

Τέλος σημειώνεται πως για την πληρέστερη αξιολόγηση των κινδύνων, είτε αυτή είναι ποιοτική είτε είναι ποσοτική, θα πρέπει να ληφθούν υπόψη και οι παράγοντες της επαναλαμβανόμενης εμφάνισης ενός κινδύνου σε μια

συγκεκριμένη χρονική περίοδο (για παράδειγμα σε ένα χρόνο) σε συνδυασμό με το κόστος των επιπτώσεων που επιφέρει σε κάθε εμφάνισή του.

5.5 Συστάσεις Ελέγχων

Κατά τη διάρκεια αυτού του βήματος, παρέχονται στοιχεία ελέγχου τα οποία μπορούν να μετριάσουν ή να εξαλείψουν τους κινδύνους που εμφανίζονται [15]. Ο στόχος των προτεινόμενων ελέγχων είναι να μειωθεί το επίπεδο των κινδύνων στο Π.Σ σε αποδεκτό επίπεδο. Οι ακόλουθοι παράγοντες πρέπει να λαμβάνονται υπόψη για την ελαχιστοποίηση ή εξάλειψη των κινδύνων που εντοπίστηκαν:

- Η αποτελεσματικότητα των προτεινόμενων επιλογών (π. χ συμβατότητα Π.Σ)
- Νομοθετικές & Κανονιστικές Διατάξεις
- Πολιτική Οργάνωσης
- Επιχειρησιακές Επιπτώσεις
- Ασφάλεια και Αξιοπιστία

Οι συστάσεις ελέγχων είναι το αποτέλεσμα της διαδικασίας αξιολόγησης των κινδύνων και είναι σημαντικό να σημειωθεί ότι όλοι οι πιθανοί έλεγχοι μπορούν να χρησιμοποιηθούν για τη μείωση των απειλών του συστήματος. Για να αξιολογηθεί ποια μέθοδος είναι συμφέρουσα για τον οργανισμό πρέπει να πραγματοποιηθεί μια ανάλυση κόστους-οφέλους για να αποδειχθεί ότι το κόστος της εφαρμογής των ελέγχων μπορεί να δικαιολογείτε από τη μείωση του επιπέδου του κινδύνου. Τέλος, πρέπει να αξιολογούνται οι επιπτώσεις που θα επιφέρουν οι έλεγχοι στον οργανισμό (π. χ επίδραση στην απόδοση του συστήματος, τεχνικές απαιτήσεις, αποδοχή χρηστών κ. α).

5.6 Σύνταξη Αναφοράς

Το τελευταίο βήμα της διαδικασίας εκτίμησης κινδύνων είναι η σύνταξη της τελικής αναφοράς των αποτελεσμάτων της. Η συγγραφή της αναφοράς αυτής θα πρέπει να γίνει με ιδιαίτερη προσοχή καθώς θα αποτελέσει βασικό εργαλείο για το επόμενο στάδιο της διαχείρισης κινδύνων που έχει να κάνει με το σχεδιασμό αντιμετώπισης των απειλών στις οποίες εκτίθεται το πληροφορικό έργο. Στην αναφορά αυτή περιλαμβάνονται όλοι οι πιθανοί κίνδυνοι που απειλούν το έργο, η

πιθανότητα εμφάνισης του καθενός, η έκταση των επιπτώσεων από την εκδήλωση καθενός από αυτούς, καθώς και τα αποτελέσματα της αξιολόγησης των κινδύνων αυτών είτε αυτή είναι ποιοτική είτε είναι ποσοτική.

Πέραν αυτών όμως η αναφορά για να είναι πλήρης θα πρέπει να περιλαμβάνει και τα παρακάτω:

- Τις πηγές από τις οποίες αντλήθηκαν όλες οι πληροφορίες
- Τις μεθόδους που χρησιμοποιήθηκαν για την έκδοση των αποτελεσμάτων
- Τα πρόσωπα που συμμετείχαν σε κάθε στάδιο της διαδικασίας
- Πλήρης τεκμηρίωση των συμπερασμάτων, των μεθόδων και των πηγών που χρησιμοποιήθηκαν (και αναγνώριση της αξιοπιστίας τους)
- Σχόλια και παρατηρήσεις ειδικών που εκφράστηκαν σε οποιοδήποτε βήμα της διαδικασίας

Ολοκληρώνοντας θα πρέπει να διευκρινιστεί ότι όλα τα παραπάνω βήματα της διαδικασίας εκτίμησης κινδύνων δε πραγματοποιούνται εφάπαξ, αλλά επαναλαμβάνονται σε όλη τη διάρκεια υλοποίησης του έργου, έτσι ώστε να συνυπολογίζονται οι αλλαγές των συνθηκών και να εκτιμώνται και πάλι οι ήδη αναγνωρισμένοι κίνδυνοι αλλά και να προστίθενται και νέοι στη λίστα των κινδύνων αν αυτό κριθεί αναγκαίο.

Κεφάλαιο 6: Αντιμετώπιση Κινδύνων

6.1 Εισαγωγή

Το τέταρτο στάδιο της διαδικασίας διαχείρισης κινδύνων είναι η αντιμετώπιση των κινδύνων η οποία στοχεύει είτε στο μετριασμό των ίδιων των κινδύνων και των επιπτώσεων τους, είτε στη δημιουργία σχεδίων έκτακτης ανάγκης σε περίπτωση που προκύψει ο κίνδυνος. Περιλαμβάνει τον καθορισμό προτεραιοτήτων και την αξιολόγηση και εφαρμογή των κατάλληλων μέτρων αντιμετώπισης των κινδύνων που απειλούν το πληροφοριακό σύστημα, είτε μειώνοντας τη πιθανότητα εμφάνισής τους είτε μετριάζοντας τις δυσμενείς επιπτώσεις από την εμφάνιση αυτών. Επειδή η πλήρης αποβολή των κινδύνων είναι συνήθως μη εφικτή, ευθύνη της ανώτερης διαχείρισης και των λειτουργικών και επιχειρησιακών στελεχών είναι να εφαρμόσουν τα μέτρα με το χαμηλότερο κόστος και τη μεγαλύτερη καταλληλότητα για να μειώσουν το βαθμό έκθεσης του έργου σε κίνδυνο σε αποδεκτό επίπεδο, με τις μικρότερες δυνατές παραχωρήσεις όσον αφορά στην καθυστέρηση της ολοκλήρωσής του, στην ποιότητά του και στην επίτευξη των στόχων για τους οποίους υλοποιείται.

Το κεφάλαιο αυτό, περιγράφει τις επιλογές μετριασμού του κινδύνου, τη στρατηγική μετριασμού κινδύνου, τη δημιουργία σχεδίων έκτακτης ανάγκης, μια προσέγγιση για την εφαρμογή των ελέγχων, κατηγορίες ελέγχων, την ανάλυση οφέλους-κόστους που χρησιμοποιείται για να δικαιολογήσει την εφαρμογή των συνιστάμενων μέτρων και την εκτίμηση του εναπομένοντος κινδύνου.

6.2 Στρατηγικές Αντιμετώπισης των Κινδύνων

Οι δύο στρατηγικές για την αντιμετώπιση των κινδύνων είναι ο ***μετριασμός των κινδύνων*** επιλέγοντας την κατάλληλη μέθοδο μετριασμού ή η ***δημιουργία σχεδίων έκτακτης ανάγκης*** [15]. Όσον αφορά τα σχέδια έκτακτης ανάγκης, είναι απαραίτητα γιατί περιλαμβάνουν συγκεκριμένες δράσεις σε περίπτωση που προκύψει ο κίνδυνος, και είναι σημαντικό να γνωρίζουμε πότε ενεργοποιείτε το σχέδιο έκτακτης ανάγκης (π. χ η παραίτηση σημαντικού μέλους της ομάδας διαχείρισης έργου και η

επιλογή νέου μέλους), και πότε πρέπει να απενεργοποιείτε (π. χ όταν το έργο αποκλίνει από το χρονοδιάγραμμα).

Όσον αφορά στρατηγική μετριασμού των κινδύνων για να προχωρήσουμε στην επιλογή της μεθόδου αντιμετώπισης τους, πρέπει στην αρχή του συγκεκριμένου σταδίου η ομάδα διαχείρισης των κινδύνων να έχει ως εισερχόμενο στοιχείο έναν κατάλογο από κινδύνους που μπορεί να επηρεάσουν το έργο, όπως αυτός προέκυψε από το στάδιο του εντοπισμού. Ο κατάλογος αυτός είναι ιεραρχημένος ανάλογα με τα αποτελέσματα του σταδίου της ανάλυσης των κινδύνων. Η απλοϊκή υπόθεση ότι θα πρέπει να αντιμετωπιστούν πρώτα οι σημαντικοί κίνδυνοι και μετά οι λιγότερο σημαντικοί δεν είναι πάντα σωστή. Ένας άλλος παράγοντας που θα πρέπει να λαμβάνεται υπόψη είναι και ο χρόνος στον οποίο ένας κίνδυνος αναμένεται να εκδηλωθεί. Είναι δηλαδή πιθανό, να χρειάζεται να αντιδράσουμε πρώτα σε έναν κίνδυνο με μικρότερη έκθεση από κάποιον άλλο, διότι περιμένουμε να εκδηλωθεί άμεσα. Επιπλέον, θα πρέπει να εξετάζει κανείς και τη δυνατότητα που έχει για την αντιμετώπιση ενός κινδύνου. Μπορεί να είναι σε θέση να αντιμετωπίσει άμεσα κάποιο κίνδυνο, ενώ δε μπορεί να κάνει το ίδιο για κάποιον άλλο.

Τα όπλα που έχει στη διάθεσή της η ομάδα διαχείρισης των κινδύνων για την αντιμετώπιση των κινδύνων εμφανίζονται παρακάτω [15]:

- ***Αποφυγή κινδύνου***. Η συγκεκριμένη μέθοδος όταν μπορεί να επιτευχθεί χωρίς σημαντικό κόστος, πρόκειται για την καλύτερη στρατηγική που μπορεί να ακολουθήσει κανείς. Πρόκειται πρακτικά, για μια αλλαγή που γίνεται στο έργο και εξαλείφει εντελώς τον κίνδυνο. Ουσιαστικά, χρησιμοποιείται μια εναλλακτική προσέγγιση που δε περιλαμβάνει τον κίνδυνο ή δεν υλοποιείται καθόλου το τμήμα του έργου που τίθεται σε κίνδυνο. Αυτή η μέθοδος δεν αποτελεί πάντα επιλογή, καθώς υπάρχουν έργα που εκτίθενται εν γνώση των υπευθύνων σε κίνδυνο για τη μεγιστοποίηση του κέρδους. Επιπρόσθετα ορισμένα τμήματα του έργου είναι ζωτικής σημασίας για τη λειτουργία του και προσφέρουν τα μέγιστα στην εκπλήρωση των στόχων του συστήματος και επομένως δε μπορούν να παραληφθούν. Μαζί με την αποφυγή του κινδύνου χάνονται και τα οφέλη που θα αποκομίζονταν από το αρχικό σχέδιο υλοποίησης και την έκθεση σε αυτόν. Παρόλα

αυτά αποτελεί την πιο αποτελεσματική μέθοδο αντιμετώπισης κινδύνων που μπορεί να εφαρμοστεί.

- ***Μεταφορά του κινδύνου.*** Η μέθοδος αυτή αφορά τη μεταφορά της επιβάρυνσης των επιπτώσεων σε τρίτους. Ένας τρόπος υλοποίησής της είναι η ***ασφάλιση*** των ευπαθών τομέων, που μεταφέρει το κόστος των επιπτώσεων στην ασφαλιστήρια εταιρία. Μια άλλη μέθοδος μεταφοράς των κινδύνων θα μπορούσαν να αποτελέσουν οι ***ρήτρες***. Με αυτόν τον τρόπο, ο κίνδυνος της καθυστέρησης ενός τμήματος του έργου, βαραίνει οικονομικά την αντίστοιχη εταιρία στην οποία έχει ανατεθεί η δημιουργία του έργου, μέσω μιας ρήτρας που θεσπίζεται κατά τη σύναψη του συμβολαίου. Ένας λίγο πιο σύνθετος τρόπος μεταφοράς του κινδύνου είναι η σύναψη ***«συμβολαίου κόστους πλέον ορισμένου κέρδους»*** (cost plus). Με αυτόν τον τρόπο, μέρος του κινδύνου, είτε ως ευκαιρία είτε ως απειλή μεταφέρεται στον κύριο του έργου. Ιδιαίτερη προσοχή πρέπει να δοθεί στο γεγονός, ότι η μεταφορά των κινδύνων συνήθως αφορά το κόστος και όχι το χρόνο ή την ποιότητα που δύσκολα ανακτώνται αν χαθούν. Συνεπώς, δεν αρκεί μόνο να μεταφέρει κανείς έναν κίνδυνο σε κάποιον άλλο, αλλά θα πρέπει να είναι σίγουρος ότι αυτή η μεταφορά θα είναι αποτελεσματική.
- ***Αποδοχή κινδύνου***. Αυτό πρακτικά σημαίνει ότι δεν προχωρούμε σε δυναμική αντίδραση αναφορικά με τον κίνδυνο, χωρίς όμως να χάνουμε παντελώς το ενδιαφέρον μας γι ‘ αυτόν. Όπως σε κάθε κίνδυνο, έτσι και σε αυτούς που αποφασίζουμε να αποδεχθούμε, καθορίζουμε ένα στέλεχος ως υπεύθυνο κινδύνου. Αν και δεν υλοποιούμε ενέργειες πριν από την εμφάνιση του κινδύνου, καθορίζουμε εναλλακτικά σχέδια, ιδιαίτερα σε περίπτωση που ο κίνδυνος έχει μεγάλη συνέπεια. Τέλος, δε παραλείπουμε να εξετάζουμε σε τακτά χρονικά διαστήματα την εξέλιξη των κινδύνων αυτών, καθώς η έκθεσή τους μπορεί να μεταβληθεί. Συνήθως, αποδεχόμαστε τους κινδύνους που δεν αναμένεται να επηρεάσουν σημαντικά τους στόχους του έργου μας. Ουσιαστικά, με την επιλογή της αποδοχής του κινδύνου, δεν επιβαρύνεται το έργο μας με επιπλέον κόστος και πολυπλοκότητα. Αυτή, όμως, είναι μια επικίνδυνη

επιλογή καθώς η αγνόηση ενός κινδύνου μπορεί να έχει καταστροφικές συνέπειες για την πορεία του έργου.

- ***Ελάφρυνση για τις απειλές και ενδυνάμωση για τις ευκαιρίες***: Αν δε μπορεί κανείς να αποφύγει ή να μεταφέρει έναν κίνδυνο, τότε πρέπει να προβεί σε ενέργειες με τις οποίες θα αλλάξει η έκθεση του κινδύνου. Οι ενέργειες αντιμετώπισης διαχωρίζονται σε εκείνες που εφαρμόζονται για να διαφοροποιήσουν την πιθανότητα εμφάνισης ενός κινδύνου (να μειώσουν την πιθανότητα των απειλών και αυξήσουν την πιθανότητα των ευκαιριών) και εκείνες που εφαρμόζονται για να διαφοροποιήσουν τη συνέπεια που ο κίνδυνους θα έχει στο έργο σε περίπτωση εμφάνισης. Οι πρώτες ονομάζονται ***προληπτικές*** ενέργειες και οι δεύτερες ***διορθωτικές***. Χαρακτηριστικό των δύο αυτών τύπων ενεργειών είναι ότι οι πρώτες δρουν σε αιτίες, οι οποίες καθορίζουν και την πιθανότητα εμφάνισης του κινδύνου, ενώ οι δεύτερες δρουν στις συνέπειες οι οποίες καθορίζουν τη σημαντικότητα του κινδύνου. Είναι προφανές ότι αν μεταβληθεί η πιθανότητα εμφάνισης είτε η βαρύτητα της συνέπειας, μεταβάλλεται αυτόματα και η έκθεση του κινδύνου.
- ***Περιορισμός των επιπτώσεων κινδύνου***. Περιορισμός του κινδύνου με την εφαρμογή μέτρων που μειώνουν τις δυσμενείς επιπτώσεις από την εκδήλωση αυτού.
- ***Προγραμματισμός κινδύνου***. Διαχείριση του κινδύνου με την ανάπτυξη σχεδίου που θέτει σε προτεραιότητα, διευκολύνει και υποστηρίζει τις διαδικασίες ελέγχων ασφαλείας.
- ***Έρευνα και αναγνώριση***. Μείωση των απωλειών μέσω της αναγνώρισης των ευπαθειών και της αναζήτησης μέτρων που ισχυροποιούν τους ευπαθείς τομείς και μειώνουν την πιθανότητα εμφάνισης των κινδύνων.

Τέλος, οι στόχοι και η αποστολή του οργανισμού, για λογαριασμό του οποίου εγκαθίσταται το πληροφοριακό σύστημα, θα πρέπει να λαμβάνονται υπόψη κατά την υιοθέτηση οποιασδήποτε από τις παραπάνω επιλογές. Η μέθοδος που θα εφαρμοστεί για το μετριασμό του κινδύνου ποικίλει ανάλογα με τη φύση του, αλλά

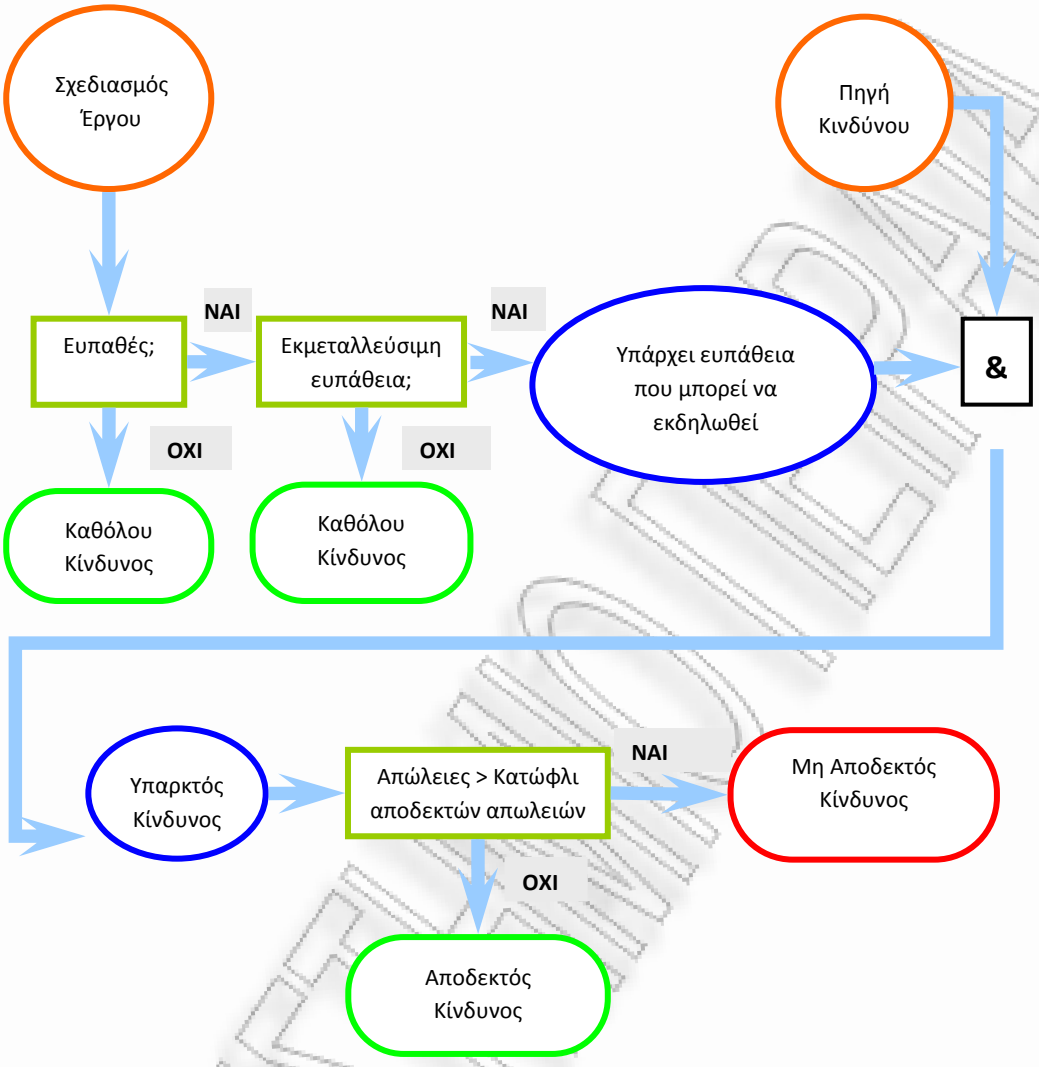
και τις ιδιαιτερότητες του κάθε έργου. Ο αποτελεσματικότερος τρόπος είναι να χρησιμοποιηθούν οι κατάλληλες τεχνολογίες μεταξύ των διαφόρων προϊόντων ασφαλείας, παράλληλα με την κατάλληλη επιλογή μεθόδου μετριασμού κινδύνου και τα μη τεχνικά, σχεδιαστικά και διοικητικά μέτρα.

6.3 Σημεία Δράσης Διαδικασίας Αντιμετώπισης Κινδύνων

Τα στελέχη που έχουν την ευθύνη για το σχεδιασμό και την υλοποίηση του έργου και που γνωρίζουν τους πιθανούς κινδύνους και τη σημαντικότητα αυτών, οφείλουν να απαντήσουν στα εξής ερωτήματα:

- ✓ Πότε και υπό ποιες συνθήκες θα πρέπει να δραστηριοποιηθούν;
- ✓ Πότε θα εφαρμόσουν τις διαδικασίες αντιμετώπισης των κινδύνων και προστασίας της πορείας υλοποίησης του έργου;

Το Σχήμα 37 δίνει τις απαντήσεις στα παραπάνω ερωτήματα με περιγραφικό τρόπο [15]:



Σχήμα 37: Σημεία Δράσης Διαδικασίας Μετριασμού Κινδύνου

Ουσιαστικά, κάθε τετραγωνάκι του παραπάνω διαγράμματος αποτελεί και ένα σημείο που θα πρέπει να εξεταστεί.

- **Υπάρχει ευπάθεια (αδυναμία).** Εφαρμογή τεχνικών για τη μείωση της πιθανότητας εμφάνισης της ευπάθειας.
- **Η ευπάθεια μπορεί να εκδηλωθεί.** Εφαρμογή των σχεδίων προστασίας του έργου και διοικητικών ελέγχων για την ελαχιστοποίηση της πιθανότητας εμφάνισης του κινδύνου ή την πλήρη αποτροπή της εμφάνισής του. Σχεδιασμός για την αντιμετώπιση των δυσμενών επιπτώσεων από την εκδήλωση του κινδύνου.
- **Οι απώλειες από την εκδήλωση του κινδύνου είναι πολύ μεγάλες.** Όταν η εφαρμογή του αρχικού σχεδιασμού προστασίας και των τεχνικών

και μη τεχνικών μέτρων για τον περιορισμό της έκτασης των επιπτώσεων αποδειχθεί επιζήμια ή αδύναμη να αντιμετωπίσει τον επικείμενο κίνδυνο, θα πρέπει να επαναληφθεί η διαδικασία, για την υιοθέτηση νέων μέτρων, ενώ δεν αποκλείεται και το ενδεχόμενο να κριθεί μη κερδοφόρα η υλοποίηση του έργου και να εγκαταλειφθεί.

Εάν αναφερόμαστε σε κινδύνους που οφείλονται σε εκούσια ανθρώπινη δράση θα πρέπει να προσθέσουμε και ένα τετραγωνάκι με τη σύγκριση κόστους-οφέλους για το δράστη πριν από αυτό της σύγκρισης των απωλειών με το κατώφλι των αποδεκτών απωλειών.

6.4 Μεθοδολογία Αντιμετώπισης Κινδύνων:

Όλα τα μέτρα ελέγχου που πρόκειται να εφαρμοστούν, θα πρέπει να υπακούν στον ακόλουθο κανόνα:

«Εξέταση των σημαντικότερων κινδύνων και επιδίωξη της ικανοποιητικής αντιμετώπισής τους με το χαμηλότερο κόστος και τις λιγότερες επιπτώσεις στην πορεία ολοκλήρωσης του έργου.»

Τα ακόλουθα βήματα περιγράφουν τη μεθοδολογία αντιμετώπισης των κινδύνων [15]:

1. **Καθορισμός προτεραιοτήτων ενεργειών**

Με βάση τα επίπεδα κινδύνου που παρουσιάζονται στην έκθεση αξιολόγησης κινδύνων, καθορίζεται η προτεραιότητα των ενεργειών που θα εφαρμοστούν. Στον τρόπο διάθεσης των πόρων, μέγιστη προτεραιότητα πρέπει να δοθεί στους κινδύνους που ταξινομούνται ως «Υψηλοί Κίνδυνοι» κατά τη διαδικασία αξιολόγησης κινδύνων, στα τμήματα του έργου που χαρακτηρίζονται ως πιο ευπαθή και βεβαίως στα τμήματα του έργου που διαδραματίζουν σημαντικό ρόλο στη λειτουργία του συστήματος. Αυτά τα ζεύγη ευπάθειας - ενδεχόμενου κινδύνου θα απαιτήσουν την άμεση διορθωτική δράση για την προστασία του πληροφοριακού συστήματος. Η έξοδοι του βήματος αυτού είναι μια κατάσταση των ενεργειών, που πρέπει να εφαρμοστούν, αξιολογημένων και ταξινομημένων από την επιτακτικότερη για εφαρμογή προς τη λιγότερο επιτακτική.

2. Αξιολόγηση προτεινόμενων ελέγχων

Οι μέθοδοι που συστήνονται για την αντιμετώπιση των κινδύνων μπορεί να μην είναι οι πιο κατάλληλες ή ακόμα και να μην είναι εφικτές για ένα συγκεκριμένο πληροφοριακό σύστημα. Σε αυτό το βήμα αναλύεται η δυνατότητα πραγματοποίησης (π.χ. συμβατότητα, αποδοχή χρηστών) και η αποτελεσματικότητα (π.χ. βαθμός προστασίας και επίπεδο μετριασμού κινδύνων) των συνιστάμενων επιλογών. Στόχος είναι να επιλεχθεί η πιο κατάλληλη μέθοδος ελέγχου για τον κάθε κίνδυνο. Οι έξοδοι του βήματος αυτού είναι μια λίστα εφικτών και αποτελεσματικών ελέγχων.

3. Ανάλυση οφέλους-κόστους

Για να βοηθηθεί η διαχείριση στη λήψη αποφάσεων και να προσδιοριστούν οι οικονομικώς αποδοτικότεροι μέθοδοι, εκτελείται μία ανάλυση οφέλους-κόστους. Με την ανάλυση αυτή λαμβάνουμε μια περιγραφή του κόστους και των κερδών που αποκομίζονται από την εφαρμογή ή τη μη εφαρμογή των διαφόρων μεθόδων. Το βήμα αυτό είναι πολύ σημαντικό καθώς μία μέθοδος μπορεί να κοστίζει περισσότερο από το ενδεχόμενο κόστος αποκατάστασης των επιπτώσεων ενός κινδύνου.

Η ανάλυση κόστους-οφέλους για τα νέα προτεινόμενα μέτρα ή για την ενίσχυση των ήδη υπαρχόντων περιλαμβάνει τα εξής:

- Καθορισμός επιπτώσεων από την εφαρμογή νέων ή την αναβάθμιση των υπαρχόντων ελέγχων
- Καθορισμός επιπτώσεων από τη μη εφαρμογή νέων ή την αναβάθμιση των υπαρχόντων ελέγχων
- Υπολογισμός του κόστους εφαρμογής. Αυτός μπορεί να περιλαμβάνει, χωρίς να περιορίζονται μόνο σε αυτά, τα ακόλουθα:
  - Αγορά hardware και software
  - Μείωση της αποτελεσματικότητας εάν οι επιδόσεις ή η λειτουργικότητα του συστήματος μειωθεί για να αυξηθεί η ασφάλεια
  - Κόστος εφαρμογής επιπρόσθετων πολιτικών και διαδικασιών

- Κόστος μίσθωσης επιπλέον προσωπικού για την εφαρμογή των προτεινόμενων πολιτικών, διαδικασιών ή υπηρεσιών
- Κόστος εκπαίδευσης
- Κόστος συντήρησης

➢ Αξιολόγηση του κόστους και των κερδών της εφαρμογής έναντι της κρισιμότητας του συστήματος και των δεδομένων για τον καθορισμό της αξίας για τον οργανισμό να εφαρμόσει τα νέα μέτρα, δεδομένου του κόστους τους και των λοιπών επιπτώσεών τους.

Όπως ακριβώς υπάρχει το κόστος για έναν αναγκαίο έλεγχο, υπάρχει και το κόστος από τη μη εφαρμογή του. Με το συσχετισμό του αποτελέσματος της μη εφαρμογής ενός ελέγχου με την εφαρμογή αυτού, η διοίκηση δύναται να αποφασίσει εάν είναι εφικτό να αποποιηθεί την εφαρμογή του.

4. Επιλογή μεθόδου

Με βάση τα αποτελέσματα της ανάλυσης κόστους - κέρδους, η διοίκηση προσδιορίζει τις πιο συμφέρουσες, με βάση το κόστος και την αποτελεσματικότητά τους, μεθόδους για τη μείωση του κινδύνου που απειλεί το πληροφοριακό σύστημα. Οι μέθοδοι που θα επιλεγούν θα πρέπει να συνδυάζουν τεχνικά, επιχειρησιακά και διοικητικά στοιχεία ελέγχου, για να διασφαλίσουν την άρτια προστασία του έργου πληροφορικής και του ίδιου του οργανισμού. Από το βήμα αυτό παίρνουμε τις μεθόδους που πρόκειται να εφαρμοστούν.

5. Ανάθεση αρμοδιοτήτων

Στο βήμα αυτό, καθορίζονται τα κατάλληλα πρόσωπα, είτε από το προσωπικό της αναδόχου εταιρίας είτε από το προσληφθέν προσωπικό με σύμβαση έργου, που έχουν τις απαραίτητες ειδικές γνώσεις και ικανότητες για να εφαρμόσουν τις επιλεγμένες μεθόδους αντιμετώπισης του κινδύνου και τους ανατίθενται συγκεκριμένες ευθύνες. Από το βήμα αυτό λαμβάνουμε τον κατάλογο των προσώπων που θα εφαρμόσουν το σχέδιο αντιμετώπισης του κινδύνου.

6. Ανάπτυξη σχεδίου εφαρμογής προστασίας του έργου

Στο βήμα αυτό γίνεται ο σχεδιασμός για την εφαρμογή των προστατευτικών μέτρων. Ο σχεδιασμός αυτός θα πρέπει το λιγότερο να περιλαμβάνει τις ακόλουθες πληροφορίες:

- Πιθανοί κίνδυνοι (ζεύγος ευπάθειας-απειλής) και το σχετικό επίπεδο έκθεσης σε αυτούς (όπως καθορίστηκε από τη διαδικασία αξιολόγησης κινδύνων)
- Προτεινόμενες μέθοδοι αντιμετώπισης
- Προτεραιότητες ενεργειών (προτεραιότητα σε στοιχεία πολύ υψηλού και υψηλού επιπέδου κινδύνου)
- Επιλεγμένες μέθοδοι αντιμετώπισης (καθορισμένες βάση του κατά πόσο είναι εφικτές και αποτελεσματικές, του οφέλους για την υλοποίηση του έργου και του κόστους)
- Απαιτήσεις για την εφαρμογή των επιλεγμένων μεθόδων
- Λίστα των υπεύθυνων ομάδων και προσώπων για την εφαρμογή της διαχείρισης κινδύνων
- Ημερομηνία εκκίνησης της εφαρμογής
- Χρονικός στόχος για ολοκλήρωση της εφαρμογής
- Απαιτήσεις για την υποστήριξη της εφαρμογής

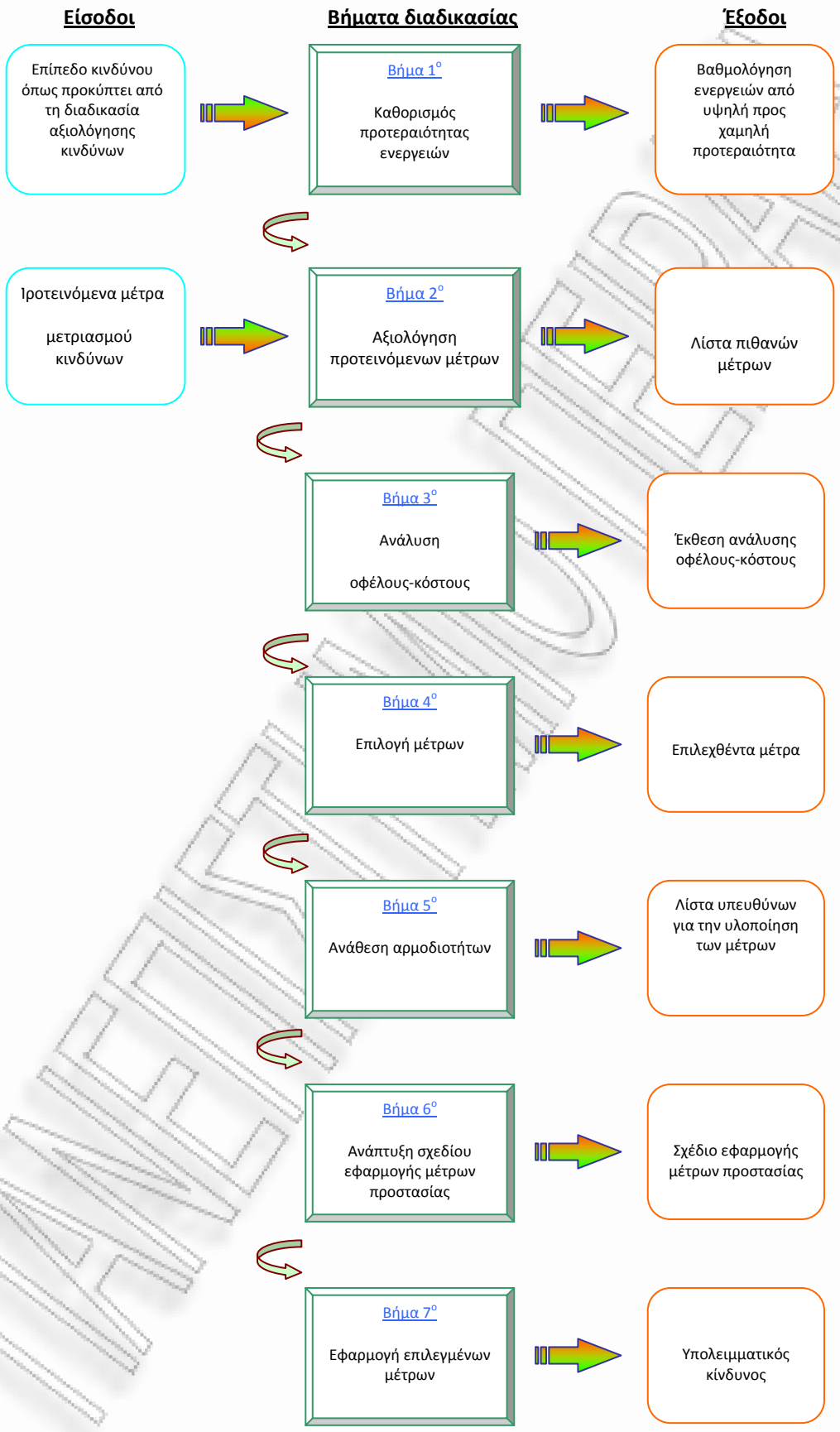
Το σχέδιο εφαρμογής θέτει την προτεραιότητα των ενεργειών, περιλαμβάνει όλα τα απαιτούμενα στοιχεία για τη λήψη ορθών επιλογών, καταγράφει τους υπεύθυνους εφαρμογής των ελέγχων και προβάλει τις ημερομηνίες εκκίνησης και ολοκλήρωσης της εφαρμογής (βάση του αρχικού στόχου). Το σχέδιο αυτό θα συνδράμει και θα επιταχύνει τη διαδικασία αντιμετώπισης των κινδύνων.

7. Αποτέλεσμα εφαρμογής επιλεγμένης μεθόδου

Ανάλογα με τις ιδιαιτερότητες του κάθε έργου, οι μέθοδοι που θα εφαρμοστούν μπορεί να μειώσουν το επίπεδο του κινδύνου, αλλά να μην εξαφανίσουν τελείως τον ίδιο τον κίνδυνο. Η έξοδος του βήματος αυτού είναι ο *υπολειμματικός κίνδυνος*, που θα παραμείνει και μετά την εφαρμογή της μεθόδου αντιμετώπισής του. Πρακτικά κανένα πληροφοριακό έργο δεν είναι πλήρως απαλλαγμένο από

κινδύνους και καμία εφαρμογή ελέγχου δε μπορεί να εγγυηθεί τη μείωση του επιπέδου του κινδύνου στο μηδέν.

Τα πρόσωπα που επιμελούνται του σχεδιασμού υλοποίησης του έργου και διαχειρίζονται τα κονδύλια που πρόκειται να διατεθούν, στο σημείο αυτό θα πρέπει να λάβουν την απόφαση εάν ο κίνδυνος που υπάρχει ακόμα (υπολειμματικός) είναι σε επίπεδο που μπορεί να γίνει αποδεκτός και επιτρέπει τη συνέχιση υλοποίησης του έργου. Φυσικά η διοίκηση θα πρέπει να συντάξει μια έκθεση, με την οποία θα περιγράφει το τελικό επίπεδο κινδύνου και τους λόγους για τους οποίους το επίπεδο αυτό είναι ικανοποιητικό και δεν απαιτούνται περαιτέρω ενέργειες για την αντιμετώπισή του. Σε διαφορετική περίπτωση ο κύκλος της διαδικασίας διαχείρισης κινδύνων θα πρέπει να επαναληφθεί για να αυξηθεί το επίπεδο ασφάλειας του έργου, εάν υπάρχει η δυνατότητα για κάτι τέτοιο και εάν είναι συμφέρουσα μια τέτοια ενέργεια. Διαφορετικά υπάρχει πάντα και το ενδεχόμενο ματαίωσης της υλοποίησης του πληροφοριακού έργου.



Σχήμα 38: Διάγραμμα προσέγγισης εφαρμογής μέτρων μετριασμού

6.5 Κατηγορίες Ελέγχων Αντιμετώπισης Κινδύνων

Τα μέτρα που εφαρμόζονται για την αντιμετώπιση των κινδύνων, μπορούν να κατηγοριοποιηθούν σε τεχνικά, διαχειριστικά και λειτουργικά. Για τη μεγιστοποίηση της προστασίας του έργου μπορεί να χρησιμοποιηθεί και ένας συνδυασμός τέτοιων μέτρων. Τα μέτρα προστασίας αν χρησιμοποιηθούν κατάλληλα μπορούν να αποτρέψουν την εμφάνιση ενός κινδύνου, να μετριάσουν το επίπεδο έκθεσης σε αυτόν ή και να προσφέρουν τα μέσα αντιμετώπισης των επιπτώσεων από την ενδεχόμενη εκδήλωση μιας απειλής.

Οι διαχειριστές κινδύνου καλούνται να επιλέξουν τον τρόπο με τον οποίο θα αντιμετωπίσουν τους κινδύνους, ανάμεσα από αυτές τις κατηγορίες, καθώς υπάρχουν συνήθως περισσότερες από μία προσεγγίσεις για την αντιμετώπιση ενός κινδύνου. Για παράδειγμα, ο έλεγχος πρόσβασης σε διάφορα τμήματα του έργου μπορεί να πραγματοποιηθεί μέσω σύνθετων κωδικών ασφαλείας που ελαχιστοποιούν την περίπτωση τυχαίας ή και οργανωμένης παραβίασης αυτών. Ο τεχνικός αυτός έλεγχος προϋποθέτει αύξηση της πολυπλοκότητας με την προσθήκη επιπλέον λογισμικού, αλλά και αύξηση του κόστους για την προμήθεια αυτού, τη στιγμή που ένας διαδικαστικός έλεγχος πρόσβασης θα είχε πολύ μικρότερο κόστος, αλλά δε θα παρείχε το ίδιο υψηλό επίπεδο ασφάλειας. Ένας διαδικαστικός έλεγχος θα μπορούσε να εφαρμοστεί απλά με τη βοήθεια ενός υπομνήματος, που θα παρουσιαζόταν σε όλα τα σχετιζόμενα πρόσωπα με το χειρισμό του λογισμικού και μια τροποποίηση στους κανόνες ασφαλείας του οργανισμού. Η εξασφάλιση όμως ότι οι χρήστες ακολουθούν με συνέπεια το υπόμνημα και τους κανόνες ασφαλείας είναι δύσκολη και απαιτεί την κατάρτιση συνείδησης ασφαλείας για την αποδοχή αυτών από τους χρήστες [15].

6.5.1 Τεχνικοί έλεγχοι ασφάλειας

Οι τεχνικοί έλεγχοι ασφάλειας διαμορφώνονται για να παρέχουν προστασία από συγκεκριμένους τύπους απειλών. Οι έλεγχοι αυτοί μπορούν να κυμανθούν από απλούς έως μεγάλης πολυπλοκότητας ελέγχους, που να περιλαμβάνουν αρχιτεκτονικές συστημάτων, στοιχεία εφαρμοσμένης μηχανικής, αλλά και πακέτα ασφάλειας που υλοποιούνται από την παράλληλη λειτουργία hardware, software

και ηλεκτρονικών συστημάτων. Όλα αυτά τα μέτρα θα πρέπει να συνεργαστούν για να διασφαλίσουν τα κρίσιμα και ευαίσθητα δεδομένα, τις πληροφορίες και τις λειτουργίες του πληροφοριακού μας συστήματος. Οι τεχνικοί έλεγχοι μπορούν να ομαδοποιηθούν στις ακόλουθες κατηγορίες σύμφωνα με το σκοπό που εξυπηρετούν:

- Έλεγχοι υποστήριξης
- Αποτρεπτικοί έλεγχοι
- Έλεγχοι ανίχνευσης και ανάκαμψης

Ακολούθως αναλύεται καθεμιά από τις παραπάνω κατηγορίες [15].

6.5.1.1 Υποστηρικτικοί τεχνικοί έλεγχοι

Οι έλεγχοι αυτοί είναι, από τη φύση τους, αλληλένδετοι με πολλούς άλλους ελέγχους. Υποστηρικτικοί τεχνικοί έλεγχοι είναι οι ακόλουθοι:

1. ***Έλεγχοι εξακρίβωσης***. Οι έλεγχοι αυτοί παρέχουν τη δυνατότητα να προσδιοριστούν μεμονωμένα οι χρήστες, οι διαδικασίες και οι πηγές πληροφοριών. Για να εφαρμοστούν άλλοι έλεγχοι ασφαλείας (π.χ. διακριτικός έλεγχος πρόσβασης, επιτακτικός έλεγχος πρόσβασης, υπευθυνότητα), είναι απαραίτητο τα θέματα και τα αντικείμενα να είναι ευπροσδιόριστα.
2. ***Διαχείριση κρυπτογραφικών κλειδιών***. Τα κρυπτογραφικά κλειδιά πρέπει να διαχειρίζονται με ασφάλεια, όταν κρυπτογραφικές λειτουργίες εφαρμόζονται στους διάφορους άλλους ελέγχους. Η διαχείριση αυτή περιλαμβάνει τη παραγωγή των κλειδιών, τη διανομή, την αποθήκευση και τη συντήρησή τους.
3. ***Διαχείριση ασφάλειας***. Τα χαρακτηριστικά γνωρίσματα ασφαλείας ενός πληροφοριακού συστήματος πρέπει να διαμορφωθούν έτσι ώστε να ικανοποιούν τις ανάγκες μιας συγκεκριμένης εγκατάστασης και να ελέγχουν αλλαγές στο λειτουργικό περιβάλλον. Η ασφάλεια των συστημάτων μπορεί να βασιστεί στην ασφαλή λειτουργία των συστημάτων και των εφαρμογών. Πολλά εμπορικά πρόσθετα προϊόντα ασφαλείας είναι διαθέσιμα στην αγορά.

4. ***Προστασίες συστήματος***. Πίσω από όλες τις λειτουργικές δυνατότητες ασφαλείας ενός συστήματος υπάρχει μια βάση εμπιστοσύνης στην τεχνική εφαρμογή. Αυτή αντιπροσωπεύει την ποιότητα της εφαρμογής από την άποψη των χρησιμοποιούμενων διαδικασιών σχεδιασμού και του τρόπου με τον οποίο η εφαρμογή ολοκληρώθηκε. Μερικά παραδείγματα προστασιών συστημάτων είναι η προστασία της υπολειμματικής πληροφορίας, ελαχιστότητα προσώπων που χρειάζεται να είναι ενήμεροι για μια διαδικασία, ο χωρισμός διαδικασιών, η διαμόρφωση, η διάταξη σε στρώματα, και η ελαχιστοποίηση των όσων, προσώπων ή συστημάτων καρπώνονται την εμπιστοσύνη του υπό εγκατάσταση πληροφοριακού μας συστήματος.

6.5.1.2 Αποτρεπτικοί τεχνικοί έλεγχοι ασφάλειας

Οι έλεγχοι αυτοί πραγματοποιούνται για να εμποδίσουν απειλές αλλοίωσης της ομαλής λειτουργίας του συστήματος να εκδηλωθούν. Τέτοιοι έλεγχοι περιλαμβάνουν τα εξής:

1. ***Επιβεβαίωση αυθεντικότητας***. Ο έλεγχος αυθεντικότητας παρέχει τα μέσα αναγνώρισης της ταυτότητας ενός αντικειμένου, εξασφαλίζοντας ότι αυτό διαθέτει την απαιτούμενη έγκριση για την οποιαδήποτε λειτουργία κληθεί να επιτελέσει. Οι μηχανισμοί επιβεβαίωσης αυθεντικότητας περιλαμβάνουν τους κωδικούς πρόσβασης, τους προσωπικούς αριθμούς αναγνώρισης, τα PIN, και τις νέες αναπτυσσόμενες τεχνικές επιβεβαίωσης που παρέχουν ισχυρή ταυτοποίηση των στοιχείων (π.χ. έξυπνη κάρτα, ψηφιακά πιστοποιητικά κ.α).

2. ***Έλεγχος εξουσιοδότησης***. Ο έλεγχος εξουσιοδότησης παρέχει μια ειδική και διαρκής διαχείριση των ενεργειών που εκτελούνται για ένα δεδομένο σύστημα (π.χ. η διοίκηση ή ο διαχειριστής μιας βάσης δεδομένων καθορίζει ποιος μπορεί να ενημερώσει ένα κοινόχρηστο αρχείο που είναι προσβάσιμο από μια ομάδα χρηστών διαδικτυακά).

3. ***Επιβολή ελέγχων πρόσβασης***. Η ακεραιότητα και η εμπιστευτικότητα των πληροφοριών διασφαλίζεται από τους ελέγχους πρόσβασης. Όταν εγκριθεί η αίτηση πρόσβασης ενός αντικειμένου σε κάποιες συγκεκριμένες διαδικασίες του συστήματος, είναι απαραίτητο να ακολουθηθούν οι καθορισμένες πολιτικές ασφαλείας (π.χ. MAC και DAC). Οι έλεγχοι αυτοί πραγματοποιούνται μέσω των μηχανισμών ελέγχου πρόσβασης που υπάρχουν διασκορπισμένοι σε όλο το σύστημα (π.χ. MAC ετικέτες ευαισθησίας, DAC σύνολα αρχείων έγκρισης, κατάλογοι ελέγχου πρόσβασης, προφίλ χρηστών). Η αποτελεσματικότητα και η δύναμη των ελέγχων πρόσβασης εξαρτώνται από την ορθότητα των αποφάσεων ελέγχου πρόσβασης (π.χ. πως διαμορφώνονται οι κανόνες ασφαλείας) και τις δυνατότητες επιβολής τους (π.χ. ο σχεδιασμός του software και hardware ασφαλείας).

4. ***Έλεγχος αποδοχής***. Η αξία των συστημάτων εξαρτάται από τη δυνατότητά της να εξασφαλίζει ότι οι αποστολείς δε μπορούν να αρνηθούν την παροχή πληροφοριών και ότι οι δέκτες δε μπορούν να αρνηθούν τη λήψη αυτών. Ο έλεγχος αποδοχής πραγματοποιεί παράλληλα και πρόληψη και ανίχνευση. Τον τοποθετούμε στην κατηγορία πρόληψης, καθώς οι μηχανισμοί που εφαρμόζονται αποτρέπουν την επιτυχή αποκήρυξη μιας δράσης (π.χ. το ψηφιακό πιστοποιητικό που περιλαμβάνει το ιδιωτικό κλειδί του κατόχου του είναι γνωστό μόνο σε αυτόν). Κατά συνέπεια οι έλεγχοι αυτοί τυπικά εφαρμόζονται στα σημεία μετάδοσης και λήψης.

5. ***Έλεγχοι προστασίας επικοινωνιών***. Σε ένα διανεμημένο σύστημα, η δυνατότητα επιτυχίας των στόχων ασφαλείας, εξαρτάται σε μεγάλο βαθμό από την αξιοπιστία των επικοινωνιών. Ο έλεγχος προστασίας επικοινωνιών διασφαλίζει την ακεραιότητα, τη διαθεσιμότητα και την εμπιστευτικότητα των ευαίσθητων και κρίσιμων πληροφοριών κατά τη μεταφορά τους. Για την προστασία των επικοινωνιών χρησιμοποιούνται διάφοροι μέθοδοι κρυπτογράφησης των δεδομένων (π.χ. εικονικό ιδιωτικό δίκτυο, πρωτόκολλο ασφάλειας στο διαδίκτυο [IPSEC] κ.α) για

να ελαχιστοποιηθούν απειλές όπως η επανάληψη, η παρεμπόδιση, το sniffing των πακέτων ή οι υποκλοπές κάθε είδους.

6. ***Προστασία συναλλαγών***. Σε κυβερνητικά και ιδιωτικά συστήματα είναι διαρκώς αυξανόμενη η απαίτηση για διατήρηση της μυστικότητας των συναλλαγών. Οι έλεγχοι μυστικότητας των συναλλαγών (π.χ. ασφαλές στρώμα υποδοχής [Secure Socket Layer]) προστατεύουν από την απώλεια αυτής, με σεβασμό στις συναλλαγές που πραγματοποιούνται από κάθε ξεχωριστό πρόσωπο ή οργανισμό.

6.5.1.3 Τεχνικοί έλεγχοι ανίχνευσης και ανάκαμψης

Οι ανιχνευτικοί έλεγχοι προειδοποιούν για ατέλειες, δυσλειτουργίες, παραβιάσεις ή απόπειρες παραβίασης του συστήματος και περιλαμβάνουν ελέγχους όπως έλεγχοι διαδρομών στο δίκτυο, μεθόδους ανίχνευσης παρείσφρησης στο σύστημα, αλλά και ελέγχους των ιδιαίτερων συνθηκών του περιβάλλοντος όπου εγκαθίσταται το πληροφοριακό σύστημα. Τα μέτρα αποκατάστασης μπορούν να χρησιμοποιηθούν για την αποκατάσταση των χαμένων υπολογιστικών πόρων. Η χρήση τους κρίνεται επιτακτική λόγω ενδεχόμενων ατελειών των τεχνικών μέτρων υποστήριξης και πρόληψης, που θα οδηγήσουν στην υπερπήδηση αυτών από τις πιθανές απειλές. Οι έλεγχοι ανίχνευσης και αποκατάστασης περιλαμβάνουν τα εξής:

1. ***Λογιστικός έλεγχος***. Ο λογιστικός έλεγχος των σχετικών με την ασφάλεια γεγονότων και η παρακολούθηση των ανωμαλιών των συστημάτων είναι βασικά στοιχεία για την ανίχνευση και την αποκατάσταση των παραβιάσεων της ασφαλούς λειτουργίας του συστήματος.

2. ***Ανίχνευση και συγκράτηση παρείσφρησης***. Είναι απαραίτητη η ανίχνευση των παραβιάσεων της ασφάλειας (π.χ. διαρρήξεις δικτύων, ύποπτες δραστηριότητες) έτσι ώστε η αντιμετώπισή τους να είναι έγκαιρη. Επίσης έχει μικρή αξία η ανίχνευση μιας παραβίασης της ασφάλειας όταν καμία αποτελεσματική δράση δε μπορεί να εκκινήσει

για την αντιμετώπισή της. Η ανίχνευση παρείσφρησης και ο έλεγχος συγκράτησης παρέχουν αυτές τις δύο ικανότητες.

3. ***Απόδειξη πληρότητας***. Ο έλεγχος απόδειξης πληρότητας (proof-of-wholeness) αναλύει την ακεραιότητα και τις παρατυπίες των συστημάτων και προσδιορίζει το επίπεδο έκθεσης σε πιθανές απειλές. Ο έλεγχος αυτός δεν αποτρέπει τις παραβιάσεις των διαδικασιών ασφαλείας, αλλά τις ανιχνεύει και βοηθά στον καθορισμό της διορθωτικής δράσης που απαιτείται.

4. ***Αποκατάσταση ασφαλούς λειτουργίας***. Αυτή η υπηρεσία επιτρέπει σε ένα σύστημα να επιστρέψει σε μια κατάσταση ασφαλούς λειτουργίας, αφότου παρουσιαστεί μια παραβίαση της ασφάλειας.

5. ***Ανίχνευση και εξόντωση ιών***. Το λογισμικό ανίχνευσης και εξόντωσης ιών που εγκαθίσταται στους κεντρικούς υπολογιστές και τα τερματικά των χρηστών, ανιχνεύει, προσδιορίζει και αφαιρεί τους ιούς λογισμικού για να διασφαλίσει την ακεραιότητα των συστημάτων και πληροφοριών. Το λογισμικό αυτό θα πρέπει να ενημερώνεται συνεχώς, καθώς οι ιοί διαρκώς μεταβάλλονται, ενισχύονται και αυξάνονται σε πλήθος, και θα ήταν άσκοπη η χρήση τέτοιου λογισμικού, που όμως δεν έχει ενημερωθεί για τους νεοεμφανιζόμενους ιούς.

6. ***Έλεγχοι τεχνολογίας***. Οι έλεγχοι αυτοί στοχεύουν στον εντοπισμό ατελειών στη λειτουργία των, έως τότε, ολοκληρωμένων τμημάτων του έργου λογισμικού. Τέτοιες ατέλειες μπορεί να οφείλονται είτε σε ελαττωματικό εξοπλισμό είτε σε ανθρώπινο σφάλμα είτε στη μη συμβατότητα των διαφόρων τμημάτων του έργου που καλούνται να συνεργαστούν. Για το σκοπό αυτό χρησιμοποιούνται αυτοματοποιημένα συστήματα ανίχνευσης (π.χ. σύστημα χαρτογράφησης δικτύων) που εντοπίζουν τις ατέλειες για την άμεση λήψη μέτρων αντιμετώπισής των προτού οι ατέλειες αυτές δημιουργήσουν προβλήματα και στα επόμενα τμήματα του έργου.

7. ***Προστασία περιβάλλοντος***. Πολύ σημαντικοί είναι και οι έλεγχοι που πραγματοποιούνται, από ηλεκτρονικό εξοπλισμό, με σκοπό τον έλεγχο των ιδιαίτερων συνθηκών (π.χ. θερμοκρασία, υγρασία, φωτιά) που

επικρατούν στον χώρο όπου εγκαθίσταται το πληροφοριακό σύστημα. Τα συστήματα αυτά είναι συνδεδεμένα με ηλεκτρικές συσκευές (π.χ. σύστημα κλιματισμού, εξαερισμού, πυρασφάλειας) που διαμορφώνουν τις κατάλληλες συνθήκες για την ομαλότερη λειτουργία του συστήματος.

6.5.2 Διοικητικοί έλεγχοι ασφάλειας

Οι διοικητικοί έλεγχοι ασφάλειας, από κοινού με τους τεχνικούς και τους λειτουργικούς ελέγχους, εφαρμόζονται για να διαχειριστούν και να μειώσουν τον κίνδυνο απωλειών και να προστατεύσουν τους στόχους του έργου. Οι έλεγχοι αυτοί εστιάζουν στην πολιτική, τις οδηγίες και τα πρότυπα προστασίας πληροφοριών, που υλοποιούνται μέσω των λειτουργικών διαδικασιών για να εκπληρώσουν τους στόχους και την αποστολή του πληροφοριακού συστήματος. Στις επόμενες παραγράφους παρουσιάζονται οι αποτρεπτικοί, οι ανιχνευτικοί και οι έλεγχοι αποκατάστασης που εφαρμόζονται για να μειώσουν τους κινδύνους [15].

6.5.2.1 Αποτρεπτικοί διοικητικοί έλεγχοι ασφάλειας

Οι έλεγχοι αυτοί περιλαμβάνουν τα εξής:

1. Ανάθεση ευθύνης σε κατάλληλα στελέχη, παροχή επαρκούς ασφάλειας στα κρίσιμα για την υλοποίηση του έργου τμήματα.

2. Σαφής διάκριση των αρμοδιοτήτων για την αποφυγή σύγχυσης κατά τη λήψη κρίσιμων αποφάσεων.

3. Ανάπτυξη και υποστήριξη σχεδίων ασφαλείας, με βάση τους υπάρχοντες ελέγχους και τους ελέγχους που είναι υπό σχεδιασμό, για την άρτια ολοκλήρωση του πληροφοριακού έργου.

4. Εφαρμογή μέτρων ασφαλείας στο προσωπικό που θα περιλαμβάνει διαχωρισμό των καθηκόντων, καθορισμό προτεραιοτήτων και εγκατάσταση και τερματισμό πρόσβασης των χρηστών των ηλεκτρονικών υπολογιστών.

5. Καλλιέργεια συνείδησης ασφάλειας στο προσωπικό για να διασφαλίζει ότι οι χρήστες του συστήματος κατανοούν την αξία των κανόνων συμπεριφοράς και την ευθύνη τους για την προστασία του συστήματος.

6. Εκπαίδευση του προσωπικού στη χρήση των νέων τεχνολογιών για την αποφυγή λαθών και βλαβερών ενεργειών σε βάρος του πληροφοριακού συστήματος. Επίσης με τον τρόπο αυτό εξασφαλίζεται και η πλήρης αξιοποίηση των δυνατοτήτων του έργου.

7. Ολοκληρωμένες συμφωνίες με τους προμηθευτές που θα περιλαμβάνουν ποινικές ρήτρες σε περίπτωση προμήθειας ελαττωματικού εξοπλισμού.

8. Συνεργασία με αξιόπιστους προμηθευτές.

9. Σαφής καθορισμός του τρόπου χρηματοδότησης του έργου (είτε βάση του χρόνου είτε βάση της προόδου του έργου)

10. Εγγυήσεις για τις οικονομικές δυνατότητες των χρηματοδοτών και διασφάλιση ότι μπορούν να ανταποκριθούν στις οικονομικές απαιτήσεις του έργου

11. Χρήση εξοπλισμού καλής ποιότητας με αναγνώριση του αυξημένου κόστους αυτού.

6.5.2.2 Ανιχνευτικοί διοικητικοί έλεγχοι ασφάλειας

Οι ανιχνευτικοί διοικητικοί έλεγχοι είναι οι ακόλουθοι:

1. Εφαρμογή ελέγχων στο προσωπικό που να περιλαμβάνει εκκαθάριση και έρευνα του υπόβαθρου και του "πρότερου βίου" του καθενός, περιστροφή των καθηκόντων για τον εντοπισμό επαναλαμβανόμενων "συμπτώσεων" και εξέταση των δυνατοτήτων και των γνώσεων αυτών σε ότι αφορά το χειρισμό των νέων τεχνολογιών.

2. Διενέργεια περιοδικής αναθεώρησης των ελέγχων ασφαλείας για τη διασφάλιση της αποτελεσματικότητας αυτών.

3. Εκτέλεση περιοδικών και έκτακτων λογιστικών ελέγχων των συστημάτων.

4. Εφαρμογή διαρκούς διαχείρισης κινδύνου για την αποτελεσματικότερη αξιολόγηση και μετριασμό των κινδύνων.

5. Ανάθεση στο πληροφοριακό σύστημα να αποδεχτεί και να παρακολουθεί τον εναπομένων κίνδυνο, ώστε να είναι άμεση η ανίχνευση εκδήλωσης του και έγκαιρη η αντιμετώπισή του.

6.5.2.3 Διοικητικοί έλεγχοι ασφάλειας με σκοπό την αποκατάσταση

Οι έλεγχοι αυτοί περιλαμβάνουν:

1. Την παροχή συνεχούς υποστήριξης και ανάπτυξης, την εξέταση και διατήρηση της συνοχής του σχεδιασμού των διαδικασιών και τη διασφάλιση της συνέχισης των εργασιών κατά τη διάρκεια καταστάσεων ανάγκης ή καταστροφών.

2. Την καθιέρωση της ικανότητας να αναγνωρίζονται, να αναφέρονται και να αντιμετωπίζονται τα διάφορα τυχαία γεγονότα επαναφέροντας το σύστημα στην ορθή κατάσταση λειτουργίας.

3. Τήρηση μικρών αποθεμάτων για την άμεση αντικατάσταση ελαττωματικού εξοπλισμού.

4. Μεταφορά των επιπτώσεων των κινδύνων. Στους ελέγχους αποκατάστασης μπορούμε να συμπεριλάβουμε και την ασφάλιση της ακεραιότητας του έργου, καθώς με τον τρόπο αυτό δεν επιβαρυνόμαστε με το κόστος αποκατάστασης από την εκδήλωση ενός κινδύνου.

5. Κατάρτιση εναλλακτικών σχεδίων υλοποίησης όπου αυτό κρίνεται αναγκαίο και φυσικά είναι εφικτό. Με τον τρόπο αυτό τα προβλήματα αντιμετωπίζονται βάση του σχεδιασμού που πραγματοποιήθηκε στην αρχή του έργου και όχι με βεβιασμένες αποφάσεις που μπορεί να αποδειχθούν λανθασμένες.

6.5.3 Λειτουργικοί έλεγχοι ασφάλειας

Τα πρότυπα ασφαλείας πρέπει να καθορίζουν ένα σύνολο ελέγχων και οδηγιών, που θα εξασφαλίζει την ομαλή λειτουργία του πληροφοριακού συστήματος, την πλήρη εκμετάλλευση των δυνατοτήτων του αλλά και την υλοποίηση του στη βάση του αρχικού σχεδιασμού σε ότι αφορά το κόστος, το χρόνο υλοποίησης και την ποιότητά του. Τα στελέχη που διαχειρίζονται την πορεία υλοποίησης του έργου διαδραματίζουν ένα ζωτικής σημασίας ρόλο, καθώς καλούνται να επιτηρήσουν την εφαρμογή του αρχικού σχεδίου υλοποίησης, και την εξασφάλιση της εφαρμογής των κατάλληλων ελέγχων ασφαλείας.

Οι λειτουργικοί έλεγχοι ασφάλειας, που εφαρμόζονται βάση του συνόλου των απαιτήσεων προστασίας του έργου και της άσκησης ορθών πρακτικών ελέγχου, χρησιμοποιούνται για να διορθώσουν τις λειτουργικές ανεπάρκειες που θα μπορούσαν να ασκηθούν από τις πιθανές πηγές κινδύνων. Για να διασφαλιστεί η συνέπεια και η ομοιομορφία των διαδικασιών ασφαλείας, οι βαθμιαίες διαδικασίες και μέθοδοι των λειτουργικών ελέγχων θα πρέπει να καθοριστούν πλήρως, να καθιερωθούν και να διατηρηθούν έως την ολοκλήρωση του έργου. Οι έλεγχοι αυτοί παρουσιάζονται στις επόμενες παραγράφους [15].

6.5.3.1 Αποτρεπτικοί λειτουργικοί έλεγχοι

Οι αποτρεπτικοί λειτουργικοί έλεγχοι είναι οι ακόλουθοι:

1. Έλεγχος πρόσβασης και διάθεσης δεδομένων (π.χ. φυσικός έλεγχος πρόσβασης)
2. Περιορισμός της εξωτερικής διανομής δεδομένων
3. Έλεγχος ιών λογισμικού
4. Έλεγχος πρόσβασης στην εγκατάσταση (π.χ. διαδικασίες ελέγχου επισκεπτών, διαχείριση και διανομή κλειδιών και κλειδαριών κ. α)
5. Ασφάλιση καλωδίων
6. Παροχή εφεδρικής υποστήριξης (π.χ. διαδικασίες τακτικής υποστήριξης πληροφοριών και συστημάτων, σύνολα αρχείων όπου αποθηκεύονται οι αλλαγές των βάσεων δεδομένων για το ενδεχόμενο να χρησιμοποιηθούν σε μελλοντικά σενάρια αποκατάστασης)
7. Καθιέρωση off-site διαδικασιών αποθήκευσης και προστασίας
8. Προστασία laptop, προσωπικών υπολογιστών (PC) και τερματικών σταθμών

6.5.3.2 Ανιχνευτικοί λειτουργικοί έλεγχοι

Οι ανιχνευτικοί λειτουργικοί έλεγχοι είναι οι εξής:

1. Παροχή φυσικής ασφάλειας (π.χ. χρήση ανιχνευτών κίνησης, κλειστό κύκλωμα τηλεόρασης, αισθητήρες και συναγερμοί)
2. Διασφάλιση περιβάλλοντος (π.χ. ανιχνευτές φωτιάς και καπνού)

6.6 Ανάλυση οφέλους - κόστους

Για τη διάθεση των πόρων της και την εφαρμογή των οικονομικώς αποδοτικότερων ελέγχων, η ανάδοχος εταιρεία, αφού προσδιορίσει όλους τους πιθανούς ελέγχους και αξιολογήσει τις δυνατότητες και την αποτελεσματικότητά τους, θα πρέπει να διενεργήσει μια ανάλυση κόστους-οφέλους. Με βάση αυτή την ανάλυση θα είναι σε θέση να καθορίσει ποιοι έλεγχοι απαιτούνται, είναι κατάλληλοι για την περίσταση και η εφαρμογή τους είναι τελικά συμφέρουσα.

Η ανάλυση κόστους-οφέλους μπορεί να είναι είτε ποιοτική είτε ποσοτική. Σκοπός της είναι να καταδείξει ότι οι δαπάνες για τους ελέγχους μπορούν να δικαιολογηθούν από την ανάλογη μείωση του επιπέδου κινδύνου. Για παράδειγμα, οι διαχειριστές του έργου δε θα ήθελαν να ξοδέψουν 1000€ για να εφαρμόσουν έναν έλεγχο που μειώνει έναν κίνδυνο, για τον οποίο το κόστος επιπτώσεων από την εκδήλωσή του θα ήταν μόλις 200€. Φυσικά, όπως και σε κάθε πτυχή της διαδικασίας διαχείρισης κινδύνων η ορθή απόφαση εξαρτάται από τις ιδιαίτερες συνθήκες του κάθε έργου και του κάθε κινδύνου. Θα μπορούσε ο παραπάνω κίνδυνος να εκδηλωθεί περισσότερες από μία φορές ή σε περισσότερα από ένα σημεία του συστήματος οπότε το κόστος των επιπτώσεων θα ήταν το αθροιστικό κόστος όλων των επιπτώσεων.

Σημειώνουμε εδώ ότι το κόστος συνδυάζει την πιθανότητα εμφάνισης ενός κινδύνου με τις δαπάνες που απαιτούνται για την αποκατάσταση της βλάβης που προκαλεί. Αν λοιπόν ένα εξάρτημα κοστίζει 2000€ και η πιθανότητα ανάγκης αντικατάστασης του είναι 0.1 τότε το κόστος του κινδύνου καταστροφής του εξαρτήματος εκτιμάται στα 0.1 x 2000€ = 200€.

Η ανάλυση κόστους-οφέλους για τα νέα προτεινόμενα μέτρα ή για την ενίσχυση των ήδη υπαρχόντων περιλαμβάνει τα εξής [15]:

- Καθορισμός επιπτώσεων από την εφαρμογή νέων ή την αναβάθμιση των υπαρχόντων ελέγχων
- Καθορισμός επιπτώσεων από τη μη εφαρμογή νέων ή την αναβάθμιση των υπαρχόντων ελέγχων
- Υπολογισμός του κόστους εφαρμογής. Αυτός μπορεί να περιλαμβάνει, χωρίς να περιορίζονται μόνο σε αυτά, τα ακόλουθα:

- Αγορά hardware και software
- Μείωση της αποτελεσματικότητας εάν οι επιδόσεις ή η λειτουργικότητα του συστήματος μειωθεί για να αυξηθεί η ασφάλεια
- Κόστος εφαρμογής επιπρόσθετων πολιτικών και διαδικασιών
- Κόστος μίσθωσης επιπλέον προσωπικού για την εφαρμογή των προτεινόμενων πολιτικών, διαδικασιών ή υπηρεσιών
- Κόστος εκπαίδευσης
- Κόστος συντήρησης

- Αξιολόγηση του κόστους και των κερδών της εφαρμογής έναντι της κρισιμότητας του συστήματος και των δεδομένων για τον καθορισμό της αξίας για τον οργανισμό να εφαρμόσει τα νέα μέτρα, δεδομένου του κόστους τους και των λοιπών επιπτώσεών τους.

Όπως ακριβώς υπάρχει το κόστος για έναν αναγκαίο έλεγχο, υπάρχει και το κόστος από τη μη εφαρμογή του. Με το συσχετισμό του αποτελέσματος της μη εφαρμογής ενός ελέγχου με την εφαρμογή αυτού, η διοίκηση δύναται να αποφασίσει εάν είναι εφικτό να αποποιηθεί την εφαρμογή του [15].

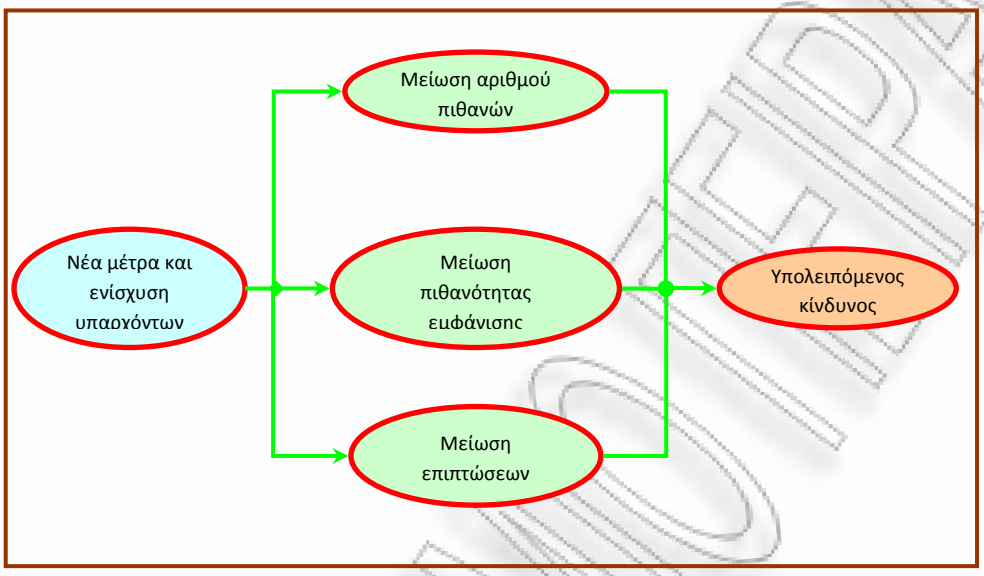
6.7 Υπολειπόμενος Κίνδυνος

Η διοίκηση μπορεί να αναλύσει το μέγεθος της μείωσης του κινδύνου που θα επιτευχθεί από την εισαγωγή των νέων μέτρων ή την αναβάθμιση των παλαιών, μέσω της μείωσης της πιθανότητας εμφάνισης ενός κινδύνου ή των επιπτώσεων του, δύο παραμέτρους που καθορίζουν το επίπεδο μετριασμού.

Η εφαρμογή νέων μεθόδων ή η αναβάθμιση των παλαιών μπορούν να μετριάσουν τον κίνδυνο [15]:

- Μειώνοντας τις αδυναμίες του αρχικού σχεδιασμού και του ίδιου του συστήματος, μειώνοντας έτσι τους κινδύνους που δύνανται να εκδηλωθούν.
- Να προσθέσουν συγκεκριμένους ελέγχους που θα μειώσουν τις δυνατότητες εκδήλωσης των ενδεχόμενων κινδύνων.
- Να προσθέσουν συγκεκριμένους ελέγχους που θα μειώσουν το μέγεθος των επιπτώσεων τους εφόσον αυτοί εκδηλωθούν.

Τα παραπάνω παρουσιάζονται στο Σχήμα 39, παρουσιάζοντας τους στόχους της κάθε ενέργειας και το τελικό αποτέλεσμα, που δεν είναι άλλο από τον κίνδυνο που τελικά απομένει.



Σχήμα 39: Αποτέλεσμα διαδικασίας μετριασμού κινδύνων

Πρακτικά κανένα πληροφοριακό έργο δεν είναι πλήρως απαλλαγμένο από κινδύνους και καμία εφαρμογή ελέγχου δε μπορεί να εγγυηθεί τη μείωση του επιπέδου του κινδύνου στο μηδέν.

Τα πρόσωπα που επιμελούνται του σχεδιασμού υλοποίησης του έργου και διαχειρίζονται τα κονδύλια που πρόκειται να διατεθούν, στο σημείο αυτό θα πρέπει να λάβουν την απόφαση εάν ο κίνδυνος που υπάρχει ακόμα είναι σε επίπεδο που μπορεί να γίνει αποδεκτός και επιτρέπει τη συνέχιση υλοποίησης του έργου. Φυσικά η διοίκηση θα πρέπει να συντάξει μια έκθεση, με την οποία θα περιγράφει το τελικό επίπεδο κινδύνου και τους λόγους για τους οποίους το επίπεδο αυτό είναι ικανοποιητικό και δεν απαιτούνται περαιτέρω ενέργειες για το μετριασμό του. Σε διαφορετική περίπτωση ο κύκλος της διαδικασίας διαχείρισης κινδύνων θα πρέπει να επαναληφθεί για να αυξηθεί το επίπεδο ασφάλειας του έργου, εάν υπάρχει η δυνατότητα για κάτι τέτοιο και εάν είναι συμφέρουσα μια τέτοια ενέργεια. Διαφορετικά υπάρχει πάντα και το ενδεχόμενο ματαίωσης της υλοποίησης του πληροφοριακού έργου [15].

Κεφάλαιο 7: Παρακολούθηση Κινδύνων

7.1 Εισαγωγή

Αν και η παρακολούθηση των κινδύνων μοιάζει να είναι το τελευταίο στάδιο του κύκλου της τυπικής διαδικασίας διαχείρισης κινδύνων, στην πράξη είναι το στάδιο που μπορεί να επανεκκινήσει τον κύκλο. Σκοπός της διαδικασίας παρακολούθησης κινδύνων είναι η παρακολούθηση των εντοπισθέντων, εναπομεινάντων και δευτερευόντων κινδύνων, ο εντοπισμός νέων κινδύνων, η αναθεώρηση των σχεδίων αντιμετώπισης, ο έλεγχος της εκτέλεσης των ενεργειών αντιμετώπισης και η εξέταση της αποτελεσματικότητας αυτών.

Η παρακολούθηση των κινδύνων και των ελέγχων που εφαρμόζονται για την αντιμετώπιση αυτών είναι μία διαρκής διαδικασία που λαμβάνει χώρα καθ' όλη τη διάρκεια υλοποίησης του έργου και ενδεχομένως να είναι απαραίτητη, σε ορισμένα σκέλη της και μετά την ολοκλήρωση της εγκατάστασης του πληροφοριακού συστήματος, υπό την ευθύνη του οργανισμού πλέον που κατέχει την κυριότητα και την εκμετάλλευσή του.

Σκοπός λοιπόν του τελευταίου σταδίου είναι να καθορίσει εάν τα μέτρα ενάντια στους κινδύνους εφαρμόζονται βάση του αρχικού σχεδιασμού κι εάν αποδίδουν τα αναμενόμενα ή αν απαιτείται η εφαρμογή νέων μέτρων. Επίσης, αξιολογεί αν η έκθεση στους κινδύνους έχει αλλάξει από την αρχική της κατάσταση και αναλύονται οι σχετικές τάσεις. Επίσης, αξιολογείται αν κάποιος από τους αναμενόμενους κινδύνους έχει εκδηλωθεί και αξιολογείται η αντιμετώπισή του. Τέλος, ελέγχεται κατά πόσο κάποιο κίνδυνοι συνεχίζουν να υφίστανται και αν η αντιμετώπισή τους κρίνεται ακόμα αναγκαία και ελέγχονται οι νέοι κίνδυνοι και οι τρόποι αντιμετώπισής τους.

Στις επόμενες παραγράφους περιγράφονται οι βασικές λειτουργίες, τα απαιτούμενα στοιχεία και οι μέθοδοι που χρησιμοποιούνται για την παρακολούθηση των κινδύνων και τα αποτελέσματα αυτού.

7.2 Βασικές λειτουργίες Παρακολούθησης Κινδύνων

Οι βασικές λειτουργίες που περιλαμβάνονται στο στάδιο της παρακολούθησης είναι οι εξής [11]:

- Παρακολούθηση της υλοποίησης των ενεργειών αντιμετώπισης των κινδύνων
- Παρακολούθηση για την εμφάνιση προπομπών κινδύνων. Ο προπομπός του κινδύνου πρακτικά προμηνύει ότι ο κίνδυνος θα εμφανιστεί σχεδόν σίγουρα.
- Διαχείριση και επικαιροποίηση του σχεδίου αντιμετώπισης κινδύνων λόγω της μεταβλητότητας των κινδύνων
- Εντοπισμός νέων κινδύνων
- Διαχείριση μη εντοπισθέντων κινδύνων
- Παρακολούθηση των «πράσινων» κινδύνων. Πρακτικά οι πράσινοι κίνδυνοι είναι οι κίνδυνοι χαμηλής έκθεσης, που δεν ενοχλεί (απειλή) ή δεν ενθουσιάζει (ευκαιρία) η ύπαρξή τους. Σε κάθε περίπτωση, επιβάλλεται η παρακολούθησή τους έτσι ώστε να διαπιστώνεται ότι παραμένουν «πράσινοι» και η έκθεσή τους δε μεταβάλλεται.
- Κοινοποίηση των αναφορών σχετικά με την εξέλιξη της διαχείρισης των κινδύνων στους ενδιαφερόμενους του έργου.

7.3 Χρήσιμα Στοιχεία για την Επόπτευση των Κινδύνων

Πληροφορίες που απαιτούνται για την επόπτευση των κινδύνων κατά τη διάρκεια υλοποίησης του πληροφοριακού συστήματος είναι οι εξής [22]:

- Σχέδιο διαχείρισης κινδύνων
- Σχέδιο αντιμετώπισης κινδύνων
- Αναφορές λειτουργίας του έργου (π. χ λίστες δράσης-αντικειμένου, προειδοποιήσεις κινδύνων, αναφορές προόδου, αναφορές ποιότητας λειτουργίας κ. α).
- Επιπρόσθετη αναγνώριση και ανάλυση κινδύνων για κινδύνους που αναγνωρίστηκαν ή εκδηλώθηκαν στην πορεία υλοποίησης του έργου και

για τους οποίους επαναλαμβάνονται οι διαδικασίες διαχείρισης κινδύνων.

- Αλλαγές στις απαιτήσεις του έργου, όπως για παράδειγμα προσθήκη νέων λειτουργιών στα συστήματα που ενδεχομένως να αντιμετωπίζουν απειλές που δεν εμφανίζονται στον αρχικό σχεδιασμό.

7.4 Μέθοδοι Παρακολούθησης Κινδύνων

Οι μέθοδοι που χρησιμοποιούνται για την παρακολούθηση των κινδύνων είναι οι ακόλουθοι [22]:

- **Έλεγχοι αντιμετώπισης κινδύνων.** Οι έλεγχοι αυτοί εξετάζουν και καταγράφουν την αποτελεσματικότητα της αντιμετώπισης των κινδύνων σε ότι αφορά την αποφυγή, τη μεταφορά ή το μετριασμό αυτών. Οι έλεγχοι αυτοί πραγματοποιούνται καθ ' όλη τη διάρκεια υλοποίησης του έργου.
- **Περιοδική ανασκόπηση των κινδύνων που απειλούν το έργο.** Τέτοιου είδους αναφορές θα πρέπει να ακολουθούν τακτικό προγραμματισμό. Θα πρέπει να τηρείται ένα ημερολόγιο κινδύνων. Αυτό χρειάζεται καθώς ο βαθμός κινδύνου και οι προτεραιότητες, ενδεχομένως να μεταβάλλονται στην πορεία υλοποίησης του έργου και οι αλλαγές αυτές μπορεί να απαιτούν εκ νέου ποιοτική και ποσοτική ανάλυση. Παράλληλα θα υποδεικνύουν και τις απειλές που δε μπορούν πλέον να βλάψουν το πληροφοριακό σύστημα και τις διαδικασίες υλοποίησής του και θα προτείνουν τους ελέγχους που μπορούν πλέον να “απενεργοποιηθούν”.
- **Ανάλυση κεκτημένης αξίας.** Η ανάλυση αυτή χρησιμοποιείται για την παρακολούθηση της πορείας του έργου βάση του αρχικού σχεδιασμού. Τα αποτελέσματα της ανάλυσης αυτής μπορεί να προβλέψουν πιθανή απόκλιση από το αρχικώς προβλεπόμενο κόστος και τον προγραμματισμένο χρόνο υλοποίησης. Όταν ένα έργο αποκλίνει ξεκάθαρα και σε αξιοσημείωτο βαθμό από το αρχικό πλάνο, τότε απαιτείται εκτέλεση εκ νέου διαχείρισης κινδύνων, για να εντοπιστούν και να αντιμετωπιστούν τα αίτια και οι επιπτώσεις αυτής της απόκλισης.

- **Τεχνική αξιολόγηση επιδόσεων.** Με την αξιολόγηση αυτή συγκρίνονται οι δυνατότητες και οι επιδόσεις του συστήματος με αυτές οι οποίες είχαν τεθεί ως στόχος κατά το σχεδιασμό του έργου. Εάν το σύστημα δεν αποδίδει τα αναμενόμενα, σημαίνει ότι διορθωτικές κινήσεις θα πρέπει να εκτελεστούν. Η αξιολόγηση αυτή θα πρέπει να γίνεται σε κάθε τμήμα του έργου που ολοκληρώνεται, λαμβάνοντας υπόψη και τις απαιτήσεις των συστημάτων που πρόκειται να εγκατασταθούν, έτσι ώστε να μειωθεί η έκταση των επιπτώσεων και η πολυπλοκότητα των επιδιορθώσεων για την επίτευξη του αρχικού στόχου.
- **Επιπρόσθετος σχεδιασμός αντιμετώπισης κινδύνων**. Ο σχεδιασμός αυτός είναι απαραίτητος όταν παρουσιαστεί ένας κίνδυνος που δεν είχε αρχικά προβλεφθεί, όταν διαπιστωθεί ότι οι επιπτώσεις ενός κινδύνου είναι μεγαλύτερες από τις αναμενόμενες ή όταν η σχεδιασμένη αντίδραση έναντι ενός κινδύνου αποδειχθεί ανεπαρκής.

7.5 Αποτελέσματα Παρακολούθησης Κινδύνων

Στην ενότητα αυτή παρουσιάζονται οι έξοδοι της διαδικασίας παρακολούθησης κινδύνων και οι οποίες αναλύονται παρακάτω [22]:

- **Δράση εκτός αρχικού σχεδιασμού.** Αναφερόμαστε για ενέργειες που πραγματοποιούνται για κινδύνους που εκδηλώνονται και αιφνιδιάζουν με την εμφάνισή τους καθώς δεν είχαν προβλεφθεί και απαιτούν την άμεση λήψη δράσης για την αντιμετώπισή τους.
- **Διορθωτικές ενέργειες.** Είναι ενέργειες που πραγματοποιούνται για να διορθώσουν παραλείψεις και προχειρότητες του αρχικού σχεδιασμού. Επίσης χρησιμοποιούνται και για την αλλαγή ορισμένων διαδικασιών καθώς στην πράξη αναδείχθηκαν κάποιες πιο αποτελεσματικές εφαρμογές.
- **Αλλαγές των απαιτήσεων του έργου.** Οι διορθωτικές ενέργειες στον αρχικό σχεδιασμό καθώς και οι εντελώς νέοι έλεγχοι που πιθανώς να απαιτηθούν μπορεί να μεταβάλλουν σημαντικά κάποιες πτυχές του

έργου και να κριθεί αναγκαία η επανεκτίμηση όχι μόνο του σχεδίου αντιμετώπισης κινδύνων, αλλά και του σχεδίου υλοποίησης του έργου.

- **Ενημέρωση βάση των εξελίξεων του σχεδίου αντιμετώπισης κινδύνων**. Οι κίνδυνοι μπορεί να εκδηλωθούν ή όχι. Κατά την διάρκεια ενός έργου οι κίνδυνοι που εκδηλώνονται καταγράφονται και αξιολογούνται. Το σχέδιο αντιμετώπισης κινδύνων μπορεί να βελτιώνεται και να ενισχύεται βάση των νέων στοιχείων. Οι κίνδυνοι που τελικά δεν εκδηλώθηκαν πρέπει επίσης να καταγράφονται και να τίθενται εκτός σχεδιασμού (εξοικονόμηση κονδυλίων, μείωση πολυπλοκότητας, μείωση προσωπικού).
- **Τήρηση αρχείων με στοιχεία κινδύνων.** Τα αρχεία αυτά θα βοηθήσουν στην καλύτερη προστασία του σχεδίου υλοποίησης του έργου, στην καλύτερη λειτουργία του, αλλά και θα αποτελέσουν πολύτιμη βάση δεδομένων για έργα που θα υλοποιηθούν στο μέλλον.

7.6 Φύλλα Κινδύνων

Ο τρόπος αναφοράς των κινδύνων βασίζεται, ως επί το πλείστον, στα φύλλα κινδύνων. Το φύλλο κινδύνου είναι ουσιαστικά η ταυτότητα του κινδύνου. Δημιουργείται κατά τον εντοπισμό του κινδύνου και αρχειοθετείται για λόγους διαχείρισης γνώσης, όταν ο κίνδυνος είτε εκλείψει είτε επέλθει. Το φύλλο κινδύνου περιλαμβάνει γενικά στοιχεία του κινδύνου, στοιχεία από την ανάλυση του κινδύνου, στοιχεία για την αντιμετώπιση των κινδύνων και κάποιες παρατηρήσεις. Ανάλογα με το υπό μελέτη έργο και την ωριμότητα των στελεχών σε σχέση με τη διαχείριση των κινδύνων, μπορεί να τροποποιείται ανάλογα [11].

Φύλλο Κινδύνου Νο 1					
Γενικά Στοιχεία					
Όνομα Κινδύνου	Ανεπάρκεια χρόνου για έλεγχο και επανέλεγχο νέων και διορθωμένων υπομονάδων (module) αντίστοιχα (π. χ προγραμματισμός πόρων, υπολογισμός στατιστικών κ. α)				
Σύντομη Περιγραφή	Αν και η επίσημη δοκιμή ολοκλήρωσης έχει περατωθεί, υπάρχουν στοιχεία που είτε δεν περιλαμβάνονται στον αρχικό προγραμματισμό ή έχουν διορθωθεί ή τροποποιηθεί σε σχέση με την πρώτη φορά. Τέτοια στοιχεία είναι η αναφορά αποθεμάτων, ο συγκριτικός πίνακας προμηθειών, ο προγραμματισμός πόρων κ. α.				
Ημερομηνία Αναγνώρισης	11/6/2012				
Μητρικός Κίνδυνος	Η αντιμετώπιση τεχνικής πολυπλοκότητας προκαλεί καθυστερήσεις. Τα τεχνικά προβλήματα είναι αξεπέραστα.				
Κατηγορία Κινδύνου	Επιχείρηση				
Δραστηριότητα Έργου	Προετοιμασία, έλεγχος & τελικές ρυθμίσεις τεχν. Εξοπλισμού παραγωγικού συστήματος.				
Ανάλυση					
Πιθανότητα (Π)	***Έκθεση= Π*Σ***				
0,9 Πολύ Υψηλή	0,05	0,09	0,18	0,36	0,72
0,7 Υψηλή	0,04	0,07	0,14	0,28	0,56
0,5 Μέση	0,03	0,05	0,10	0,20	0,40
0,3 Χαμηλή	0,02	0,03	0,06	0,12	0,24
0,1 Πολύ Χαμηλή	0,01	0,01	0,02	0,04	0,08
	0,05 Πολύ Χαμηλή	0,10 Χαμηλή	0,20 Μέση	0,40 Υψηλή	0,80 Πολύ Υψηλή
	Συνέπεια (Σ)				
Αντιμετώπιση					
Α/Α	***Περιγραφή***	***Ημ/νία***	***Ημ/νία***	***Ημ/νία***	

	ενέργειας	***Καταγραφής***	***Έναρξης***	***Ολοκλήρωσης***
1	Επίσπευση ανάπτυξης υπολοίπων εφαρμογών και διόρθωσης υπαρχόντων	11/06/2012		
Παρατηρήσεις				
Υπεύθυνος	Δημητρακάκη Μαρία			
Εγκρίθηκε από	Μαλαματένιου Φλώρα			
Παρακολούθηση				
Αρχική Έκθεση	Αρχική Πιθανότητα	Αρχική Συνέπεια	Ημερομηνία	
0,12	0,3	0,4	11/06/2012	
Τρέχουσα Έκθεση	Τρέχουσα Πιθανότητα	Τρέχουσα Συνέπεια		

Σχήμα 40: Μοντέλο φύλλου διαχείρισης κινδύνων σε Πληροφοριακό Σύστημα

Κεφάλαιο 8: Μελέτη Περίπτωσης

8.1 Εισαγωγή

Στο κεφάλαιο αυτό πραγματοποιείται εφαρμογή των διαδικασιών της διαχείρισης κινδύνων, για το έργο: **«*Ολοκληρωμένο Πληροφοριακό Σύστημα (ΟΠΣ) Δήμου Αθηναίων*»** [25]. Ουσιαστικά, στις πρώτες ενότητες παρουσιάζεται το προς μελέτη έργο, και στην ενότητα 8.5 διενεργείται μια παρουσίαση όλων των διαδικασιών διαχείρισης κινδύνων με βάση τις απαιτήσεις και τα ζητούμενα του έργου αυτού.

8.2 Ολοκληρωμένο Πληροφοριακό Σύστημα (ΟΠΣ) Δήμου Αθηναίων

Το έργο αυτό αφορά την ανάπτυξη ολοκληρωμένου πληροφοριακού συστήματος για την παροχή ηλεκτρονικών διαδικτυακών υπηρεσιών για το Δήμο Αθηναίων. Ο σκοπός της ανάπτυξης του συστήματος αφορά την αναβάθμιση της ποιότητας των παρεχομένων υπηρεσιών ενημέρωσης και εξυπηρέτησης του Δήμου Αθηναίων προς τους δημότες του, τις επιχειρήσεις, αλλά και όλους τους Έλληνες πολίτες, με τις κάτωθι ηλεκτρονικά παρεχόμενες υπηρεσίες που παρέχονταν μόνο μερικώς ή καθόλου σε ηλεκτρονικό επίπεδο [25]:

- Διεκπεραίωση υπηρεσιών και ηλεκτρονική έκδοση πιστοποιητικών
- Ηλεκτρονική υποστήριξη της "Γραμμής του Δημότη - 1595"
- Ηλεκτρονικές πληρωμές προς το Δήμο (τέλη, πρόστιμα, παράβολα αιτήσεων κ.λ.π.)
- Ηλεκτρονική παρακολούθηση προόδου αιτημάτων/διεργασιών
- Πλαίσιο ταυτοποίησης των πολιτών (με βάση την ηλεκτρονική υπογραφή)
- Σύστημα διασύνδεσης για την απασχόληση

- Νέοι τρόποι εξυπηρέτησης του πολίτη (υποδομή Voice Portal, Infokiosks)
- Νέες ηλεκτρονικά παρεχόμενες υπηρεσίες για ΑΜΕΑ, ανέργους και ενίσχυση επιχειρηματικότητας
- Ηλεκτρονική πολεοδομία, κατηγορία οικοδομικών αδειών και ηλεκτρονική υποβολή σχεδίων
- Εξαγωγή στατιστικών αναφορών και συμπερασμάτων ανά δημοτικό διαμέρισμα με βάση GIS
- Κεντρική εξαγωγή δεικτών απόδοσης, ταχύτητας επίλυσης προβλημάτων, δεικτών αποδοτικότητας τμημάτων και όγκου ζήτησης
- Διαχείριση λογαριασμού οφειλών και εκκαθάριση πληρωμών για τους πολίτες και τις επιχειρήσεις

Το έργο επιμερίζεται σε δύο υποέργα [25]:

Υποέργο 1: ***Ανάπτυξη Εφαρμογών***, το οποίο περιλαμβάνει την οργάνωση εφαρμογών πληροφορικής σ΄ ένα «Ολοκληρωμένο Πληροφοριακό Σύστημα» του Δήμου Αθηναίων, η οποία θα οργανώνει το πληροφοριακό υλικό και τις υπηρεσίες προς τους πολίτες, τους χρήστες των υπηρεσιών του Δήμου και των ΚΕΠ, τις επιχειρήσεις και τις υπόλοιπες δημόσιες υπηρεσίες. Τα συστήματα που θα περιλαμβάνει εμφανίζονται παρακάτω:

1. Σύστημα Διαχείρισης Ενημέρωσης και Περιεχομένου (ΣΔΕΠ)
2. Σύστημα Διαχείρισης Ροών Εργασιών (ΣΔΡΕ)
3. Σύστημα Διαχείρισης Εγγράφων (ΣΔΕ)
4. Υποσύστημα Πρωτοκόλλου
5. Υποσύστημα Διαχείρισης Χρηστών
6. Υποσύστημα Διαχείρισης Ψηφιακής Υπογραφής
7. Σύστημα Διασύνδεσης Απασχόλησης
8. Ηλεκτρονική Διεκπεραίωση (Εκκαθάριση Συναλλαγών)

Υποέργο 2: ***Προμήθεια Εξοπλισμού***, το οποίο περιλαμβάνει την προμήθεια και εγκατάσταση συστημάτων πληροφορικής (π. χ ηλεκτρονικούς υπολογιστές, server, εκτυπωτές, περιφερειακές συσκευές, λειτουργικά συστήματα, προγράμματα κ. α)

και ανήκει στο συνολικό έργο της υποστήριξης και λειτουργίας του Ολοκληρωμένου Πληροφοριακού Συστήματος του Δήμου Αθηναίων.

Ο συνολικός προϋπολογισμός του έργου ανέρχεται στα ***3.708.800,00€*** (συμπεριλαμβανομένου ΦΠΑ 19%). Ουσιαστικά, ο προϋπολογισμός του Υποέργου 1 ανέρχεται στο ποσό των 1.476.800,00€ και το Υποέργο 2 στα 223.200,00€ [25].

8.2.1 Συστήματα και Εφαρμογές του Υποέργου 1

Τα διάφορα συστήματα που θα αναλυθούν παρακάτω αποτελούν τμήματα του Ολοκληρωμένου Πληροφοριακού Συστήματος του Δήμου Αθηναίων και είναι τα ακόλουθα [26]:

- **Σύστημα Διαχείρισης Ενημέρωσης και Περιεχομένου (ΣΔΕΠ)**

Το σύστημα διαχείρισης του περιεχομένου είναι υπεύθυνο για την διαχείριση του περιεχομένου όπως επίσης και των ενοτήτων του site, ενώ στην πύλη εφαρμογών (Application Portal) δημιουργείται η μορφή και η παρουσίαση των σελίδων για να την εμφάνισή τους.

- **Σύστημα Διαχείρισης Ροών Εργασίας (ΣΔΡΕ)**

Η κάλυψη της απαίτησης για την ολοκληρωμένη αντιμετώπιση του πολίτη ξεκινά με τη δυνατότητα διαχείρισης σαφώς προδιαγεγραμμένων αιτημάτων με βάση προεπιλεγμένες και απόλυτα καταγεγραμμένες διαδικασίες. Απαιτείται συνεπώς η παρακολούθηση της εξέλιξης των αιτημάτων από όλα τα εμπλεκόμενα μέρη, δηλαδή από τον πολίτη, ο οποίος παρακολουθεί την εξέλιξη του ή των αιτημάτων του, τους υπαλλήλους του δήμου που είναι και οι χειριστές του αιτήματος ή του προσωπικού των ΚΕΠ. Οι παραπάνω δυνατότητες εξασφαλίζονται από την ύπαρξη Συστήματος Διαχείρισης Ροών Εργασίας (Workflow Management System) - ΣΔΡΕ, το οποίο επιτρέπει τη διαχείριση των επιχειρησιακών ροών εργασίας - διαδικασιών του Δήμου, αλλά και την ad-hoc δρομολόγηση των πληροφοριών και εργασιών στους χρήστες του. Το σύστημα θα βασίζεται σε κάποια

από τις εμπορικά διαθέσιμες λύσεις της αγοράς. Οι λειτουργικές προδιαγραφές και η σύνθεση του συστήματος αναφέρονται σε μεγαλύτερη λεπτομέρεια ακολούθως.

- **Σύστημα Διαχείρισης Εγγράφων (ΣΔΕ)**

Η λειτουργία του ολοκληρωμένου περιβάλλοντος εξυπηρέτησης του πολίτη, θα απαιτήσει τη διακίνηση και παρακολούθηση μεγάλου όγκου πληροφοριών / εγγράφων. Κρίνεται σκόπιμη και κρίσιμη η εγκατάσταση στο Δήμο Αθηναίων ενός ολοκληρωμένου Συστήματος Διαχείρισης (ηλεκτρονικών) Εγγράφων (Document Management System). Το Σύστημα Διαχείρισης Εγγράφων (ΣΔΕ) συγκεντρώνει όλες τις λειτουργίες που απαιτούνται για την εύκολη, αυτοματοποιημένη και αποδοτική διαχείριση της επιχειρησιακής πληροφορίας, η οποία σήμερα διατίθεται σε διάφορες μορφές (έντυπη- ηλεκτρονική) και διακινείται δια μέσου διαφορετικών μέσων (e-mail, fax, κλπ). Η διαχείριση εγγράφων αποτελεί οριζόντια εφαρμογή η οποία εκτιμάται ότι θα δρα ως το κεντρικό σημείο διασύνδεσης και πρόσβασης όλων των επιμέρους υποσυστημάτων με τα πρωτογενή δεδομένα του Δήμου.

- **Υποσύστημα Πρωτοκόλλου**

Το Υποσύστημα Πρωτοκόλλου αποβλέπει στην αυτοματοποίηση της διαδικασίας χειρισμού της επίσημης Εισερχόμενης, Εξερχόμενης και Εσωτερικής Αλληλογραφίας. Δεδομένου ότι οι εργασίες του υποσυστήματος πρωτοκόλλου αφορούν σε διαχείριση εγγράφων και δρομολόγηση αντίστοιχων διεργασιών, η πλειονότητα αυτών δύναται να καλύπτεται πλήρως ή στον μεγαλύτερο βαθμό από τα ΣΔΕ και ΣΔΡΕ, όπως αναφέρεται και ακολούθως στη σχετική ενότητα.

- **Υποσύστημα Διαχείρισης Χρηστών**

Το Υποσύστημα Διαχείρισης Χρηστών παρέχει ένα ολοκληρωμένο περιβάλλον διαχείρισης των εντεταλμένων χειριστών που έχουν πρόσβαση στα επιμέρους συστήματα (ΣΔΕΠ, ΣΔΡΕ, ΣΔΕ, Πρωτοκόλλου). Επιπλέον παρέχει ένα μηχανισμό ενιαίας πρόσβασης (σύμφωνα με τη διεθνή πρακτική, τα συστήματα αυτά αναφέρονται ως “Single Sign On”) των χρηστών με βάση το όνομα (username) και τον κωδικό (password). Χωρίς το σύστημα αυτό οι χρήστες (υπάλληλοι Δήμου,

υπάλληλοι ΚΕΠ, λοιπός Δημόσιος Τομέας) θα έπρεπε να αποστηθίζουν ισάριθμα ονόματα και κωδικούς με τα συστήματα τα οποία χειρίζονται, ενώ και οι διαχειριστές ασφάλειας θα έπρεπε να ζητούν κάθε φορά από τον ίδιο το χρήστη τα στοιχεία του, προκειμένου να τον εξουσιοδοτήσουν ξεχωριστά για κάθε εφαρμογή.

- **Υποσύστημα Διαχείρισης Ψηφιακής Υπογραφής**

Εξετάζοντας το εύρος των υπηρεσιών που παρέχει ο Δήμος Αθηναίων ως προς τις ανάγκες πιστοποίησης, παρατηρούμε πως σήμερα για την ολοκλήρωση υπηρεσιών όπως έκδοση πιστοποιητικών, πληρωμή προστίμων κλπ, απαιτείται η φυσική παρουσία των δημοτών σε κάποια υπηρεσία του δήμου. Με το προτεινόμενο **σύστημα πιστοποίησης** με χρήση **ηλεκτρονικής υπογραφής**, το οποίο αναλύεται στη σχετική ενότητα που ακολουθεί, η παρουσία των δημοτών απαιτείται μόνο την πρώτη φορά την οποία θα χρειαστούν κάποια υπηρεσία, ενώ ταυτόχρονα γίνεται πλήρης εκμετάλλευση του διαδικτύου. Επιπλέον χάρη στη δυνατότητα αναγνώρισης της ταυτότητας των χρηστών, επιτρέπεται η πρόσβαση σε προσωποποιημένες υπηρεσίες, όπως για παράδειγμα στη δημοτική βιβλιοθήκη, από όπου οι δημότες που έχουν προχωρήσει σε εγγραφή τους στο σύστημα, μπορούν να αναζητούν και να δεσμεύουν προς δανεισμό βιβλία του ενδιαφέροντός τους. Με αντίστοιχο τρόπο ευνοούνται και άλλες δράσεις πολιτισμού, on-line κρατήσεις εισιτηρίων για εκδηλώσεις του δήμου (δημοτικά θέατρα κτλ) και πολιτιστικές εκδηλώσεις.

- **Σύστημα Διασύνδεσης Απασχόλησης**

Θα δημιουργηθεί η απαραίτητη υποδομή για τη διαχείριση της προσφοράς και της ζήτησης εργασίας σε τοπικό επίπεδο. Η δημιουργούμενη υποδομή θα είναι πλήρως επεκτάσιμη και θα μπορεί να διασυνδεθεί με αντίστοιχα συστήματα για την απασχόληση, που υφίστανται ή θα δημιουργηθούν μελλοντικά σε κεντρικό ή περιφερειακό επίπεδο.

- **Ηλεκτρονική Διεκπεραίωση (Εκκαθάριση) Συναλλαγών**

Η ολοκλήρωση με σύστημα ηλεκτρονικής διεκπεραίωσης συναλλαγών θα λειτουργήσει πολλαπλασιαστικά για το πλήθος των συναλλαγών που αφορούν σε πληρωμές του δημότη ή της επιχείρησης.

8.2.1.1 Αλληλεξαρτήσεις Υποσυστημάτων και Εφαρμογών

Η Ηλεκτρονική Πύλη αποτελεί το κεντρικό σημείο πρόσβασης προς όλες τις υπηρεσίες και τις σχετικές διαδικασίες. Η λειτουργία της Ηλεκτρονικής Πύλης (Portal) βασίζεται στο υπάρχον *Σύστημα Διαχείρισης Εγγράφων και Περιεχομένου*. Η λειτουργία της Ηλεκτρονικής Πύλης παρέχει με τρόπο διαφανή για τους τελικούς χρήστες, σύνδεση με τα επιμέρους συστήματα και υποσυστήματα. Η Πύλη παρέχει πρόσβαση και στο Σύστημα Διασύνδεσης για την Απασχόληση.

Το *Σύστημα Διαχείρισης Ροής Εργασιών* θα φροντίζει για την οργάνωση, την αυτοματοποίηση και το συντονισμό των διαδικασιών που αφορούν στην εξυπηρέτηση των πολιτών. Το σύστημα διασυνδέεται με τα περισσότερα από τα επιμέρους συστήματα και υποσυστήματα για την ολοκλήρωση της λειτουργικότητας με στόχο την εξυπηρέτηση των τυποποιημένων διαδικασιών.

Το *Σύστημα Διαχείρισης των Εγγράφων* βρίσκεται στη βάση των περισσότερων διαδικασιών αφού οι περισσότερες διαδικασίες σχετίζονται με πληροφορία αυτόνομη και ομαδοποιημένη σε έγγραφα τα οποία συμβατικά αναφέρονται ως «αιτήσεις», «πιστοποιητικά», «βεβαιώσεις», «δηλώσεις», κ.ο.κ. Το ΣΔΕ θα πρέπει να ολοκληρώνεται αρμονικά με το σύστημα ΣΔΡΕ. Επίσης καθώς κάποιες διαδικασίες απαιτούν την επίδειξη της ταυτότητας του χρήστη για την ολοκλήρωσή τους, προβλέπεται η σύνδεση του ΣΔΡΕ με το Υποσύστημα Διαχείρισης Ψηφιακής Υπογραφής (Πολιτών).

Το *Υποσύστημα Διαχείρισης Χρηστών* θα επιτρέπει την οργάνωση των χρηστών σε ομάδες με συγκεκριμένα δικαιώματα για κάθε εφαρμογή (σύστημα και υποσύστημα) αλλά και στα δεδομένα.

8.2.1.2 Χρήστες Συστήματος

Μέσω του Πληροφοριακού Συστήματος και της λειτουργικότητας που αυτό θα παρέχει θα υποστηριχθούν (α) οι εσωτερικές λειτουργίες των υπαλλήλων του Δήμου Αθηναίων, (β) οι διαδικασίες συναλλαγών με τους πολίτες και τις επιχειρήσεις και (γ) η διαλειτουργικότητα με άλλα συστήματα της Δημόσιας Διοίκησης Ως εκ τούτου, το Πληροφοριακό Σύστημα θα πρέπει να καλύπτει τις ανάγκες διαφορετικών ομάδων χρηστών. Η κάθε ομάδα έχει διαφορετικές απαιτήσεις από το σύστημα, αλλά και διαφορετικές δυνατότητες πρόσβασης στα συστήματα/υποσυστήματα. Αναλυτικότερα αναφέρονται τα εξής [26]:

- **Ενδιαφερόμενοι (Πολίτες, Επιχειρήσεις κλπ)**

Οι πολίτες και οι επιχειρήσεις θα μπορούν να έχουν έγκαιρη και επικαιροποιημένη πληροφόρηση σχετικά με τις λειτουργικές περιοχές που τους αφορούν. Ο ενδιαφερόμενος πολίτης θα πρέπει να μπορεί να αντλήσει πληροφορίες για τα δικαιολογητικά που απαιτούνται για τη διεκπεραίωση της υπόθεσής του, καθώς και να διεκπεραιώσει ηλεκτρονικές συναλλαγές με τις Υπηρεσίες του Δήμου, με ηλεκτρονική υποβολή αιτημάτων, ηλεκτρονική αποστολή πιστοποιητικών, ηλεκτρονική παρακολούθηση της προόδου διεκπεραίωσης των υποθέσεών τους, ηλεκτρονική πληρωμή τελών και προστίμων κλπ.

- **Προσωπικό Διευθύνσεων του Δήμου Αθηναίων**

Η πρώτη ομάδα χρηστών αποτελείται από τους εργαζόμενους στο Δήμο Αθηναίων και στις Διευθύνσεις αυτού. Το προσωπικό αυτών των υπηρεσιών αποτελεί τους βασικούς χρήστες του Πληροφοριακού Συστήματος, μέσω του οποίου θα έχουν τη δυνατότητα να εκτελούν τις εργασίες τους με μεγαλύτερη ευκολία, ταχύτητα και ασφάλεια. Το σύστημα θα πρέπει να καλύπτει τις ανάγκες αυτών των χρηστών για:

  - Ευκολότερη παρακολούθηση της κίνησης των εισερχόμενων και εξερχόμενων εγγράφων,

- Ευέλικτη διαχείριση της καταχωρημένης πληροφορίας σε επίπεδο αναζήτησης και ενημέρωσης των πολιτών μέσω της Πύλης,
- Βελτίωση στην επικοινωνία με τους συναλλασσόμενους πολίτες και οργανισμούς.

Το προσωπικό που θα χρησιμοποιεί το σύστημα διακρίνεται στις ακόλουθες κατηγορίες:

- **Τοπικοί Διαχειριστές** εφαρμογών του πληροφοριακού συστήματος. Αποστολή τους είναι η διασφάλιση της επικοινωνίας για τεχνικά θέματα με τους κεντρικούς διαχειριστές, η παραμετροποίηση υποσυστημάτων διαχείρισης ροής εργασιών και ηλεκτρονικού πρωτοκόλλου και η παροχή βοήθειας στους απλούς χρήστες. Οι τοπικοί διαχειριστές θα είναι στελέχη του Δήμου Αθηναίων.

- **Χρήστες εφαρμογών**, οι οποίοι διακρίνονται σε δύο κατηγορίες:

  - **Απλοί χρήστες**, με πρόσβαση στο λειτουργικό τμήμα της εφαρμογής που αφορά στην εξυπηρέτηση των πολιτών.
  - **Προϊστάμενοι υπηρεσιών**, με δυνατότητα πρόσβασης και στο λειτουργικό τμήμα της εφαρμογής που αφορά στη διοικητική παρακολούθηση κάθε Διεύθυνσης του Δήμου Αθηναίων, μέσω τυποποιημένων αναφορών, στατιστικών στοιχείων και αναλύσεων.

- **Λοιποί φορείς**

Η τρίτη ομάδα χρηστών του πληροφοριακού συστήματος αποτελείται από τους λοιπούς Εξυπηρέτησης Πολιτών (ΚΕΠ) του Δήμου Αθηναίων και της υπόλοιπης χώρας. Το πληροφοριακό σύστημα πρέπει να καλύπτει τις ανάγκες για ασφαλή επικοινωνία και συναλλαγή με τους λοιπούς φορείς με σκοπό τη μείωση του χρόνου διεκπεραίωσης των υποθέσεων τους. Ο τρόπος λειτουργίας του πληροφοριακού συστήματος, σε σχέση με αυτή την ομάδα χρηστών, συνοψίζεται στα ακόλουθα:

- Συμπλήρωση, διαχείριση (τροποποίηση, διαγραφή) και εκτύπωση ηλεκτρονικής φόρμας αιτήσεων από διαπιστευμένους χρήστες με την εξασφάλιση ασφαλούς σύνδεσης
- Αποστολή ηλεκτρονικής φόρμας πιστοποιητικού και ενημέρωση μέσω της κεντρικής βάσης δεδομένων του πληροφοριακού συστήματος
- Αξιοποίηση των διαδικτυακών υπηρεσιών που θα υλοποιηθούν στο πλαίσιο του έργου με σκοπό την ενσωμάτωση τους σε υφιστάμενα συστήματα των συνεργαζόμενων φορέων

Το προσωπικό που θα χρησιμοποιεί το σύστημα αποτελείται από τους **Χρήστες εφαρμογών** διασύνδεσης του Δήμου Αθηναίων με τρίτους φορείς.

8.2.2 Απαιτούμενος Εξοπλισμός του Υποέργου 2

Εξυπηρετητής Διαδικτύου (Web Server): Πρόκειται για τον εξυπηρετητή στον οποίο αποκτούν πρόσβαση οι χρήστες από το διαδίκτυο. Ο εξυπηρετητής αυτός υποστηρίζει την επεξεργασία της πληροφορίας για την παρουσίαση της μέσω του πρωτοκόλλου HTTP. Οι εξυπηρετητές αυτοί θα τοποθετηθούν εκτός του τοπικού δικτύου του Δ.Α. σε ειδικά προστατευμένη περιοχή («αποστρατικοποιημένη ζώνη» - DMZ) αφού δεν πρέπει να συνδέονται άμεσα με τα εσωτερικά στοιχεία του συστήματος.

Εξυπηρετητές Εφαρμογών (Application Server): Πρόκειται για τους εξυπηρετητές που αναλαμβάνουν την υποστήριξη της λειτουργικότητας των εφαρμογών (Application Logic), δηλαδή των συστημάτων και υποσυστημάτων. Η διαφοροποίηση σε σχέση με τον παραπάνω εξυπηρετητή είναι ακριβώς στο σκοπό τον οποίο εξυπηρετούν, δηλαδή οι εξυπηρετητές διαδικτύου αφορούν στην υποστήριξη των εξωτερικών χρηστών, σε αντίθεση με τους εξυπηρετητές εφαρμογών που αφορούν την υποστήριξη του προσωπικού του Δ.Α., καθώς και τη δημιουργία περιεχομένου για την υποστήριξη του Εξυπηρετητή Διαδικτύου.

Διαχειριστής Εξυπηρετητής Βάσεων Δεδομένων (Database Server):

Περιλαμβάνει όλα τα απαραίτητα στοιχεία λογισμικού τα οποία αναλαμβάνουν την διαχείριση (αποθήκευση, οργάνωση, δεικτοδότηση, αναζήτηση, εντοπισμός και

ανάκτηση) των δεδομένων του συστήματος, όπως επίσης και την επικοινωνία και διαχείριση συνθετότερων συστημάτων αποθήκευσης δεδομένων.

Εξυπηρετητής Τηλεομοιοτυπίας και Ηλεκτρονικού Ταχυδρομείου (Fax/Email Server): Ενσωματώνει όλες τις λειτουργίες ολοκληρωμένης διαχείρισης εισερχόμενης, εξερχόμενης τηλεομοιοτυπίας καθώς επίσης και ηλεκτρονικού ταχυδρομείου.

Εξυπηρετητής Λήψης Εφεδρικών Αντιγράφων (Back Up Server) σύμφωνα και με τους πίνακες συμμόρφωσης. Όπως ήδη αναφέρθηκε, είναι δυνατό να υιοθετηθούν εναλλακτικές αρχιτεκτονικές, οι οποίες συνδυάζουν-συγχωνεύουν ή διαχωρίζουν τα προηγούμενα στοιχεία, αναθέτοντας ελαφρώς διαφορετικούς ρόλους. Ωστόσο, το σύνολο των ρόλων που θα εμφανίζονται από τους υποψήφιους Αναδόχους σε κάθε προτεινόμενο σύστημα θα πρέπει κατ' ελάχιστο να καλύπτουν τα όσα αναφέρονται στα προηγούμενα.

8.2.2.1 Διαστασιολόγηση ΟΠΣ

Ως εκτιμώμενα μεγέθη του ΟΠΣ και των Υποσυστημάτων αναφέρονται τα επόμενα [26]:

- Δυνατότητα υποστήριξης αριθμού ταυτόχρονων εσωτερικών χρηστών (Concurrent Intranet and Extranet Users) ≥ 150
- Δυνατότητα υποστήριξης αριθμού ταυτόχρονων πιστοποιημένων εξωτερικών

8.2.2.2 Εγγύηση Καλής Λειτουργίας

Ο Ανάδοχος θα πρέπει να προσφέρει υπηρεσίες εγγύησης για όλο τον εξοπλισμό που θα προσφέρει. Με την οριστική παραλαβή του έργου θα αρχίσει η περίοδος εγγύησης καλής λειτουργίας (παροχή δωρεάν συντήρησης). Ο εξοπλισμός που προσφέρεται πρέπει να καλύπτεται απαραίτητα από δύο (2) χρόνια εγγύησης καλής λειτουργίας. Ο χρόνος εγγύησης καλής λειτουργίας υπολογίζεται από την ημερομηνία οριστικής παραλαβής του εξοπλισμού.

Σε περίπτωση που ο Ανάδοχος προσφέρει επιπλέον από τον ζητούμενο χρόνο εγγύησης αυτός θα πρέπει (α) να αφορά ακέραιο αριθμό ετών και (β) να καλύπτει το σύνολο της προσφερόμενης λύσης.

Οι υποχρεώσεις του Αναδόχου στο πλαίσιο εγγύησης καλής λειτουργίας, είναι οι ακόλουθες [26]:

- Αποκατάσταση των βλαβών και ανωμαλιών λειτουργίας του εξοπλισμού.
- Η αποκατάσταση των βλαβών θα γίνεται στον τόπο που είναι εγκατεστημένος ο εξοπλισμός. Σε εξαιρετικές περιπτώσεις, μετά από έγκριση της Αναθέτουσας Αρχής, η επισκευή θα μπορεί να γίνει σε χώρους του Αναδόχου.
- Παράδοση αντιτύπων όλων των εγχειριδίων του εξοπλισμού και των απαραίτητων μέσων (πχ. CD) που συνοδεύουν τα προϊόντα.
- Διενέργεια προληπτικής συντήρησης του εξοπλισμού τουλάχιστον μία (1) φορά τον χρόνο ή όσες φορές το θεωρεί απαραίτητο ο Ανάδοχος. Οποιαδήποτε εργασία προληπτικής συντήρησης ή διαχείρισης που προϋποθέτει τη μη διαθεσιμότητα του συστήματος, θα εκτελείται εκτός ωραρίου εργασίας.
- Υπηρεσία Άμεσης Βοήθειας (Help-Desk).

8.3 Υλοποίηση Έργου

Ο χρόνος υλοποίησης του Έργου είναι εντός τριών (3) μηνών από την ημερομηνία υπογραφής της σύμβασης. Ο Ανάδοχος υποχρεούται εντός δύο (2) μηνών από την ημερομηνία υπογραφής της σύμβασης, να έχει ολοκληρώσει την παράδοση του εξοπλισμού, μέχρι και την περίοδο πιλοτικής λειτουργίας. Η περίοδος παραγωγικής λειτουργίας προσδιορίζεται στον ένα (1) μήνα κατ ΄ ελάχιστο μετά την ολοκλήρωση της περιόδου πιλοτικής λειτουργίας.

8.4 Στόχοι του Έργου

1. Ο εκσυγχρονισμός του υφιστάμενου Δικτυακού Τόπου του Δήμου Αθηναίων και των συνδεόμενων με αυτή λειτουργιών, με σύγχρονες Τεχνολογίες Πληροφορικής και Επικοινωνιών (ΤΠΕ), οι οποίες θα συμβάλλουν άμεσα στην υποστήριξη των θεσμικών και οργανωτικών παρεμβάσεων και μεταρρυθμίσεων και έμμεσα στην αναβάθμιση της ποιότητας των υπηρεσιών και στην αναδιοργάνωση των εσωτερικών

διαδικασιών, με εμφανές τελικά αντίκτυπο στην καλύτερη διοικητική εξυπηρέτηση του πολίτη.

2. Η αποτελεσματικότερη οργάνωση αλλά και η επακόλουθη εκλογίκευση και απλούστευση των εσωτερικών διαδικασιών και εργασιών του ΔΑ με άμεσο αντίκτυπο στην καλύτερη εξυπηρέτηση του πολίτη.

3. Η βελτίωση της ποιότητας ζωής των πολιτών μέσω της διαμόρφωσης κατάλληλων και τεκμηριωμένων πολιτικών στο τομέα των μεταφορών (οδική ασφάλεια, προστασία περιβάλλοντος κλπ).

4. Η παροχή πληροφορικού υλικού και εύληπτης πληροφορίας με διαλογικό τρόπο, σε επιχειρήσεις και στο ευρύ κοινό.

5. Η παροχή διεπαφής (interface) για τη λειτουργική διασύνδεση πληροφοριακών συστημάτων άλλων φορέων με το ΔΑ με σκοπό είτε τη συστηματοποιημένη είτε την ad-hoc ανταλλαγή δεδομένων καθώς και την on line ενημέρωση.

6. Η παροχή προς το ΔΑ και τους φορείς με τους οποίους παρουσιάζει ισχυρές συνέργιες (ΚΕΠ Δήμου και λοιπές δημόσιες υπηρεσίες) της δυνατότητας ανταλλαγής δεδομένων και υπηρεσιών που κρίνονται απαραίτητα για την αποτελεσματική εκτέλεση των λειτουργιών τους.

7. Η ανάπτυξη του ανθρώπινου δυναμικού

8.5 Ολοκληρωμένο Πληροφοριακό Σύστημα (ΟΠΣ) Δήμου Αθηναίων και Διαχείριση Κινδύνων

Στην ενότητα αυτή πραγματοποιείται ανάλυση σχετικά με τις διαδικασίες διαχείρισης κινδύνων για το ΟΠΣ του Δήμου Αθηναίων.

8.5.1 Χαρακτηρισμός σχετικά με το έργο και την Αναθέτουσα Αρχή

Η πρώτη διαδικασία της διαχείρισης κινδύνων είναι η διαδικασία συλλογής πληροφοριών σχετικά με την αναθέτουσα αρχή και το ίδιο το έργο. Η πληροφορίες που απαιτούνται είναι:

Για την αναθέτουσα Αρχή:

- Πληροφορίες σχετικά με το έργο και τους σκοπούς του ΟΠΣ Δήμου Αθηναίων.
- Η αξία του νέου πληροφοριακού συστήματος για τη λειτουργία και την ανάπτυξη του ΟΠΣ.

<u>Σχετικά με το περιβάλλον όπου θα εγκατασταθεί το πληροφοριακό σύστημα:</u>

- Υπάρχοντα πληροφοριακά συστήματα στον οργανισμό.
- Έλεγχος των χώρων όπου θα εγκατασταθεί το υλικό του νέου πληροφοριακού συστήματος.
- Συστήματα ασφαλείας για την προστασία από φυσικές και μη καταστροφές. Δηλαδή συστήματα ανίχνευσης και ελέγχου καπνού, φωτιάς, υγρασίας, θερμοκρασίας που υπάρχουν στις εγκαταστάσεις.
- Φύλαξη των εγκαταστάσεων από προσωπικό ασφαλείας.
- Ιστορικό φυσικών καταστροφών της περιοχής (πλημμύρες, σεισμοί).
- Επίπεδο γνώσεων και εκπαίδευσης του προσωπικού που θα χειριστεί το πληροφοριακό σύστημα.
- Τρόπος αντιμετώπισης της χρήσης του νέου συστήματος από το προσωπικό.
- Πλήρης γνώση των πληροφοριών που θα διαχειριστεί το νέο σύστημα.
- Μέγεθος των επιπτώσεων από την απώλεια ή την κοινοποίηση των πληροφοριών που θα διαχειρίζεται το νέο πληροφοριακό έργο.
- Το νομικό πλαίσιο που επικρατεί για τη διαχείριση τις πληροφορίας και τη μετάδοση αυτής.
- Το δίκτυο διασύνδεσης των διαφόρων τερματικών σταθμών.
- Αναμενόμενες τεχνολογικές εξελίξεις

<u>Πληροφορίες σχετικά με το υλοποιούμενο πληροφοριακό σύστημα</u>

- Στόχος υλοποίησης του νέου πληροφοριακού συστήματος.
- Τρόπος υλοποίησης των λειτουργιών που θα κλιθεί να επιτελέσει το νέο πληροφοριακό σύστημα πριν από την εισαγωγή του.
- Πλήρης περιγραφή του τρόπου χρηματοδότησης και των φορέων που την έχουν αναλάβει.

- Επιστημονικές αναφορές για την τεχνολογία που πρόκειται να εισαχθεί.
- Επιστημονικές αναφορές για την εγκατάσταση συστημάτων ασφαλείας.
- Πρότερη πείρα από την υλοποίηση παρόμοιων έργων.
- Εσωτερικές και εξωτερικές διασυνδέσεις που πρέπει να υλοποιηθούν (πληροφορίες για την υπάρχουσα υποδομή).

8.5.2 Εντοπισμός Πιθανών Κινδύνων

Παρακάτω παρουσιάζονται πιθανοί κίνδυνοι που μπορεί να επηρεάσουν την υλοποίηση του έργου:

Α. Φυσικές καταστροφές

- Κίνδυνος σεισμού (Α.1)
- Κίνδυνος πλημμύρας (Α.2)

Β. Φυσικό και θεσμικό περιβάλλον του έργου

- Κίνδυνος εκδήλωσης πυρκαγιάς στο χώρο της εγκατάστασης (Β.1)
- Κίνδυνος εκδήλωσης πυρκαγιάς σε γειτονικές εγκαταστάσεις (Β.2)
- Κίνδυνος διαρροής υδάτων λόγω παλαιότητας ή κακής κατασκευής του δικτύου υδροδότησης (Β.3)
- Κίνδυνος αδυναμίας ηλεκτροδότησης του συστήματος λόγω ελλείψεων στην ηλεκτρολογική εγκατάσταση (Β.4)
- Κίνδυνος παραβίασης του νομικού πλαισίου που διέπει τις διαδικασίες μετάδοσης πληροφορίας και τήρησης αρχείων προσωπικών δεδομένων (Β.5)
- Κίνδυνος αδυναμίας υποστήριξης των ταχυτήτων του συστήματος από το παρεχόμενο από το κράτος δίκτυο μετάδοσης πληροφορίας (Β.6)

Γ. Ανθρώπινος παράγοντας

- Κίνδυνος αλλοίωσης, υποκλοπής ή καταστροφής μεταδιδόμενων πληροφοριών (Γ.1)
- Κίνδυνος πρόσβασης σε απόρρητες βάσεις δεδομένων και κοινοποίηση του περιεχομένου τους ή παραποίηση αυτού (Γ.2)

- Κίνδυνος προσβολής του συστήματος από την επιδρομή hacker (Γ.3)
- Κίνδυνος δολιοφθορών από δυσαρεστημένο προσωπικό(Γ.4)

Δ. Κίνδυνοι τεχνολογίας

- Κίνδυνος χρησιμοποίησης νέων τεχνολογιών που θα αποδειχθούν μη λειτουργικές στο μέλλον (Δ.1)
- Κίνδυνος χρησιμοποίησης τεχνολογίας που θα καταστεί απαρχαιωμένη στο άμεσο μέλλον (Δ.2)
- Αδυναμία διασύνδεσης τμημάτων του έργου (Δ.3)
- Αδυναμία διασύνδεσης υπάρχοντος εξοπλισμού με το νέας τεχνολογίας εγκαθιστάμενο σύστημα (Δ.4)
- Κίνδυνος ελαττωματικού εξοπλισμού (Δ.5)
- Κίνδυνος μη αξιολόγησης των τεχνολογικών απαιτήσεων του έργου και αν είναι εφικτή η εγκατάσταση στον οργανισμό (Δ.6)

Ε. Επιχειρησιακοί κίνδυνοι

- Κίνδυνος αδυναμίας χρήσης του συστήματος λόγω έλλειψης ειδικών γνώσεων από το διοικητικό προσωπικό(Ε.1)
- Κίνδυνος καταστροφής υλικού ή λογισμικού από τους χειριστές του συστήματος λόγω κακής χρήσης του (Ε.2)
- Κίνδυνος απροθυμίας προσαρμογής του προσωπικού στα νέα δεδομένα του εργασιακού τους περιβάλλοντος (Ε.3)
- Ατελείς έλεγχοι από το προσωπικό ασφαλείας που δεν αντιλαμβάνεται την αξία της σωστής εκτέλεσης των καθηκόντων του (Ε.4)
- Κίνδυνος εσφαλμένης εγκατάστασης υλικού και λογισμικού από το προσωπικό της ανάδοχου εταιρείας, λόγω έλλειψης τεχνικών γνώσεων ή εξαιτίας απλού ανθρώπινου σφάλματος (Ε.5)
- Κίνδυνος μη ρεαλιστικών προσδοκιών από τα ενδιαφερόμενα μέρη (Ε.6)
- Κίνδυνος μη συμμετοχής των χρηστών στο project και μη κατανόησης των στόχων του έργου (Ε.7)
- Κίνδυνος λανθασμένης υποστήριξης του manager από την ανάδοχο εταιρία (Ε.8)

- Κίνδυνος αδυναμίας μέτρησης της ζημιάς που θα προκληθεί σε περίπτωση ύπαρξης των κινδύνων (Ε.8)

<u>ΣΤ. Κίνδυνοι οργάνωσης του έργου</u>

- Κίνδυνος κακού αρχικού σχεδιασμού υλοποίησης του έργου (ΣΤ.1)
- Κίνδυνος μη ρεαλιστικού χρονοδιαγράμματος και ανάλυσης κόστους του έργου (ΣΤ.2)
- Κίνδυνος μεταβολής των απαιτήσεων από το σύστημα λόγω ασαφούς αρχικού πλάνου απαιτήσεων (ΣΤ.3)
- Κίνδυνος κακής αρχικής συμφωνίας για το χρόνο διάθεσης κονδυλίων από τους χρηματοδότες του έργου (ΣΤ.4)
- Κίνδυνος αναξιόπιστων προμηθευτών εξοπλισμού, ως προς την τήρηση των χρονοδιαγραμμάτων και την προμήθεια του συμφωνηθέντος εξοπλισμού σε ποιότητα και ποσότητα (ΣΤ.5)
- Έλλειψη εμπειρίας και τεχνογνωσίας των προσώπων που αναλαμβάνουν την παρακολούθηση υλοποίησης του έργου και θα κλιθούν να λάβουν σημαντικές αποφάσεις σε στενά χρονικά περιθώρια (ΣΤ.6)
- Κίνδυνος κακής συνεργασίας μεταξύ ανάδοχων εταιρειών σε περίπτωση κοινοπραξίας (ΣΤ.7)
- Κίνδυνος καθυστερημένων αλλαγών λόγω αύξησης των απαιτήσεων του έργου (ΣΤ.8)

8.5.3 Ποιοτική ανάλυση & Δράσεις Αντιμετώπισης Κινδύνων

Στον Σχήμα 41 παρουσιάζεται η πιθανότητα εμφάνισης καθενός από τους παραπάνω κινδύνους και πραγματοποιούνται κάποιες παρατηρήσεις όπου κρίνεται απαραίτητο. Η ανάλυση που γίνεται για την αξιολόγηση των κινδύνων είναι ποιοτική και στοχεύει στον εντοπισμό των κινδύνων εκείνων που απαιτούν την άμεση επέμβαση της διοίκησης, για την προστασία του έργου. Ο κάθε κίνδυνος αντιπροσωπεύεται από έναν κωδικό, όπως παρουσιάστηκε στην προηγούμενη ενότητα κατά τη διαδικασία αναγνώρισης των κινδύνων.

Πιθανοί Κίνδυνοι	Πιθανότητα Εμφάνισης					Παρατηρήσεις
	Πολύ Χαμηλή	Χαμηλή	Μέτρια	Υψηλή	Πολύ Υψηλή	
Α. Φυσικές καταστροφές						
Α.1	✓					Μικρή δυνατότητα πρόβλεψης
Α.2	✓					Συνήθως τα συστήματα τοποθετούνται σε όροφο
Β. Φυσικό και θεσμικό περιβάλλον του έργου						
Β.1		✓				-
Β.2		✓				Υπάρχουν κολλητά στην εγκατάσταση γειτονικά κτίρια
Β.3	✓					Μικρή δυνατότητα πρόβλεψης
Β.4			✓			-
Β.5		✓				Κρατικό έργο άρα θα πληροί και τις νομικές διατάξεις που το κράτος έχει καθορίσει
Β.6		✓				-
Γ. Ανθρώπινος παράγοντας						

Γ.1			✓			Μέτριος κίνδυνος καθώς δεν υπάρχει ισχυρό κίνητρο
Γ.2			✓			Μέτριος κίνδυνος καθώς δεν υπάρχει ισχυρό κίνητρο
Γ.3		✓				Χαμηλός κίνδυνος καθώς δεν υπάρχει ισχυρό κίνητρο
Γ.4		✓				Δύσκολα θα έχουν τέτοια πρόσωπα πρόσβαση για πρόκληση φθορών
Δ. Κίνδυνοι τεχνολογίας						
Δ.1			✓			Αλληλένδετος με τον επόμενο κίνδυνο
Δ.2		✓				Αλληλένδετος με τον προηγούμενο κίνδυνο
Δ.3			✓			-
Δ.4				✓		-
Δ.5		✓				Οι προμηθευτές τέτοιου εξοπλισμού είναι αξιόπιστοι αλλά ποτέ δεν αποκλείεται η εμφάνιση ελαττωματικού υλικού

Δ.6			✓			Μέτριος κίνδυνος καθώς είναι εφικτό να μη πραγματοποιηθεί σωστή αξιολόγηση των τεχνολογικών απαιτήσεων
Ε. Επιχειρησιακοί κίνδυνοι						
Ε.1				✓		Πιθανός να ζητηθεί η εκπαίδευση του προσωπικού από την ανάδοχο εταιρεία
Ε.2			✓			-
Ε.3			✓			Στα πλαίσια της εκπαίδευσης είναι και η εμφύσηση της αξίας του συστήματος
Ε.4			✓			Στα πλαίσια της εκπαίδευσης είναι και η εμφύσηση της αξίας του συστήματος
Ε.5		✓				-
Ε.6			✓			Αρχικές υπογραφές για τις απαιτήσεις του συστήματος
Ε.7			✓			Πιθανός να ζητηθεί η συμμετοχή των χρηστών στο project

Ε.8			✓			Εάν ο project manager αρνείται τη συμμετοχή των χρηστών στο project, ή προσπαθεί να οργανώσει το χρονοδιάγραμμα του έργου μόνος του, τότε υπάρχει σοβαρός κίνδυνος για το έργο
Ε.9			✓			-
ΣΤ. Κίνδυνοι οργάνωσης του έργου						
ΣΤ.1		✓				-
ΣΤ.2			✓			-
ΣΤ.3		✓				-
ΣΤ.4		✓				Μικρός κίνδυνος λόγω αξιοπιστίας των χρηματοδοτών
ΣΤ.5		✓				-
ΣΤ.6		✓				-
ΣΤ.7			✓			-
ΣΤ.8			✓			Κίνδυνος που επηρεάζει το χρονοδιάγραμμα και το κόστους υλοποίησης του έργου

Σχήμα 41: Πιθανότητα εμφάνισης κινδύνων(ποιοτική προσέγγιση)

Στο Σχήμα 42 παρουσιάζεται το επίπεδο των επιπτώσεων από την εκδήλωση καθενός από τους παραπάνω κινδύνους. Στα σχόλια που γίνονται δικαιολογείται το επίπεδο αυτό και αναγνωρίζεται ο τομέας υλοποίησης του έργου που θα πληγεί

από την εκδήλωση των κινδύνων (π.χ. κόστος, χρόνος υλοποίησης, ποιότητα, αξιοπιστία). Το επίπεδο των επιπτώσεων σε πολλούς από τους παραπάνω κινδύνους εξαρτάται από τον τομέα στον οποίο εκδηλώνεται ο κάθε κίνδυνος. Για παράδειγμα εξαρτάται από το είδος των πληροφοριών που θα χαθούν, αλλοιωθούν ή κοινοποιηθούν ή από το τμήμα του εξοπλισμού που καταστρέφεται σε κάθε περίπτωση.

Πιθανοί Κίνδυνοι	**Επίπεδο Επιπτώσεων**					**Παρατηρήσεις και στοιχεία του έργου που επιβαρύνονται**
	Πολύ Χαμηλό	**Χαμηλό**	**Μέτριο**	**Υψηλό**	**Πολύ Υψηλό**	
Α. Φυσικές καταστροφές						
Α.1				✓		Ενδιαφέρουν σεισμοί που θα καταστρέψουν όλη την εγκατάσταση
Α.2				✓		Ενδιαφέρουν πλημμύρες που θα καταστρέψουν όλη την εγκατάσταση
Β. Φυσικό και θεσμικό περιβάλλον του έργου						
Β.1				✓		Ενδιαφέρουν πυρκαγιές που θα καταστρέψουν όλη την εγκατάσταση
Β.2				✓		Ενδιαφέρουν πυρκαγιές που θα καταστρέψουν όλη την εγκατάσταση
Β.3				✓		Ενδιαφέρουν πλημμύρες που θα καταστρέψουν όλη την εγκατάσταση

Β.4		✓				Αύξηση του χρόνου υλοποίησης αλλά ενδεχομένως το επιπλέον κόστος να επιβαρύνει την αναθέτουσα αρχή
Β.5		✓				Επιβάρυνση του κόστους και του χρόνου υλοποίησης για τη διενέργεια διορθωτικών κινήσεων
Β.6		✓				Ενδεχόμενη αύξηση του κόστους και του χρόνου υλοποίησης και μείωση της ποιότητας λειτουργίας αλλά χαμηλού επιπέδου κίνδυνος καθώς δεν είναι στην ευθύνη της ανάδοχου εταιρείας
Γ. Ανθρώπινος παράγοντας						
Γ.1			✓			Πλήττεται η αξιοπιστία του συστήματος αλλά και επιβαρύνεται το κόστος και ο χρόνος υλοποίησης για την προσθήκη επιπλέον συστημάτων ασφαλείας που δεν υπήρχαν στον αρχικό σχεδιασμό

Γ.2			✓			Πλήττεται η αξιοπιστία του συστήματος αλλά και επιβαρύνεται το κόστος και ο χρόνος υλοποίησης για την προσθήκη επιπλέον συστημάτων ασφαλείας που δεν υπήρχαν στον αρχικό σχεδιασμό
Γ.3				✓		Υψηλός κίνδυνος που θα επιφέρει καταστροφή λογισμικού και απώλεια δεδομένων, πιθανώς αναντικατάστατων (εξαρτάται και από τον τομέα του συστήματος που πλήττεται)
Γ.4				✓		Εξαρτάται και από τον τομέα του συστήματος που πλήττεται
Δ. Κίνδυνοι τεχνολογίας						
Δ.1				✓		Κίνδυνος να καταστεί το σύστημα μη λειτουργικό
Δ.2			✓			Κίνδυνος να μην έχει το σύστημα την αναμενόμενη αξία στο άμεσο μέλλον
Δ.3		✓				Επιβάρυνση του χρόνου υλοποίησης
Δ.4			✓			Επιβάρυνση του χρόνου υλοποίησης και του κόστους που όμως δε θα επιβαρύνει λογικά την ανάδοχο εταιρεία

Δ.5		✓				Επιβάρυνση του χρόνου υλοποίησης και πιθανή καταστροφή και μέρους του υγιούς εξοπλισμού
Δ.6				✓		Επιβάρυνση του χρόνου και του κόστους υλοποίησης
Ε. Επιχειρησιακοί κίνδυνοι						
Ε.1		✓				Εκπαίδευση του προσωπικού των νοσοκομείων που θα χειρίζεται το νέο σύστημα
Ε.2				✓		Επιβαρύνει κόστος και χρόνο υλοποίησης για τη διόρθωση των απωλειών και η σοβαρότητα των επιπτώσεών του εξαρτάται από το τμήμα του συστήματος που καταστρέφεται
Ε.3		✓				Μικρό το επίπεδο των επιπτώσεων καθώς οι υπάλληλοι θα συμμορφωθούν τελικά στις νέες εξελίξεις και απαιτήσεις της εργασίας τους
Ε.4		✓				Μικρό το επίπεδο των επιπτώσεων καθώς οι περισσότεροι έλεγχοι ασφαλείας είναι αυτοματοποιημένοι

Ε.5			✓			Οι επιπτώσεις του κινδύνου στο κόστος και στο χρόνο υλοποίησης του έργου εξαρτώνται από το τμήμα του έργου που πλήττεται
Ε.6			✓			Μέτριο το επίπεδο των επιπτώσεων καθώς θα συμμορφωθούν και τα δύο μέρη σε κάποια ενδιάμεση λύση
Ε.7		✓				Εάν οι χρήστες δεν εμπλέκονται στον προγραμματισμό του έργου, μπορεί να πραγματοποιήσουν καθυστερημένες αλλαγές, και αυτό με τη σειρά του μπορεί να προκαλέσει σημαντικές αυξήσεις στο κόστος του έργου.
Ε.8			✓			Πιθανή επίπτωση στην υλοποίηση των στόχων του έργου.
Ε.9			✓			Επίπτωση στο κόστος, εάν οι ενδιαφερόμενοι δεν γνωρίζουν το μέγεθος της ζημιάς, σημαίνει ότι δε μπορούν να υποστηρίξουν τη διαδικασία διαχείρισης κινδύνων για το πληροφοριακό έργο που τους έχει ανατεθεί
ΣΤ. Κίνδυνοι οργάνωσης του έργου						

ΣΤ.1					✓	Ενδεχομένως να έχει καταστροφικές επιπτώσεις και ίσως και την εγκατάλειψη υλοποίησης του έργου, ανάλογα με τη φύση των λαθών στον αρχικό σχεδιασμό
ΣΤ.2					✓	Ενδεχομένως να έχει καταστροφικές επιπτώσεις και ίσως και την εγκατάλειψη υλοποίησης του έργου, ανάλογα με τη φύση των λαθών στον αρχικό σχεδιασμό
ΣΤ.3		✓				Επιβαρύνεται το κόστος και ο χρόνος υλοποίησης του έργου, ίσως όμως να μην επιβαρυνθεί η ανάδοχος εταιρεία εάν κριθεί ότι δε φέρει ευθύνη για τα σφάλματα
ΣΤ.4			✓			Κίνδυνος καθυστέρησης υλοποίησης του έργου αλλά και ίσως επιβάρυνσης του κόστους του
ΣΤ.5		✓				Καθυστέρηση υλοποίησης του έργου

ΣΤ.6			✓			Εάν παρουσιαστούν σημαντικά θέματα προς επίλυση τότε οι συνέπειες μπορεί να είναι πολύ σημαντικές και να επιβαρύνουν κόστος, χρόνο, αξιοπιστία και ποιότητα
ΣΤ.7			✓			Κίνδυνος καθυστέρησης υλοποίησης του έργου λόγω έλλειψης συνεργασίας
ΣΤ.8			✓			Καθυστέρηση υλοποίησης του έργου

Σχήμα 42: Επίπεδο επιπτώσεων κάθε κινδύνου

Στο Σχήμα 43 παρουσιάζεται το συνολικό επίπεδο έκθεσης στον κάθε κίνδυνο, συνυπολογίζοντας την πιθανότητα εμφάνισης και τη σοβαρότητα των επιπτώσεων. Παράλληλα δίνονται και προτεινόμενες δράσεις αντιμετώπισης των κινδύνων αυτών.

Πιθανοί Κίνδυνοι	**Συνολικό Επίπεδο Έκθεσης σε κάθε Κίνδυνο**				**Παρατηρήσεις και προτεινόμενη δράση αντιμετώπισης**
	Αμελητέο	**Χαμηλό**	**Μέτριο**	**Υψηλό**	
Α. Φυσικές καταστροφές					
Α.1	✓				Καμία δράση
Α.2		✓			Τοποθέτηση συστημάτων σε όροφο, έλεγχος κουφωμάτων, ασφάλιση
Β. Φυσικό και θεσμικό περιβάλλον του έργου					

B.1			✓		Σύστημα ανίχνευσης πυρκαγιάς, συστήματα πυρόσβεσης, τήρηση κανόνων ασφαλείας από το προσωπικό, ασφάλιση
B.2	✓				Η δράση για την αντιμετώπιση του Β.1 κινδύνου καλύπτει και τη δράση γι αυτόν το σχεδόν απίθανο κίνδυνο
B.3		✓			Έλεγχος του δωματίου όπου θα εγκατασταθεί το σύστημα (μικρής σημασίας έλεγχος)
B.4		✓			Έλεγχος των εγκαταστάσεων, ενημέρωση της αναθέτουσας αρχής για τις επιπλέον απαιτήσεις του έργου και εισαγωγή αυτών στον αρχικό σχεδιασμό υλοποίησης του έργου
B.5		✓			Μελέτη του νομικού πλαισίου που διέπει τη μετάδοση πληροφορίας και την τήρηση αρχείων προσωπικών δεδομένων και συμμόρφωση του σχεδιασμού υλοποίησης του έργου με αυτό (αναζήτηση της γνώμης ειδικών, πληροφόρηση για επικείμενες αλλαγές της νομοθεσίας)

Β.6		✓			Πληροφόρηση για τις δυνατότητες του τρέχοντος δικτύου και για επικείμενη αναβάθμιση αυτού, υλοποίηση του έργου με βάση τις τρέχουσες δυνατότητες αυτού και παροχή της δυνατότητας εύκολης αναβάθμισης των συστημάτων
Γ. Ανθρώπινος παράγοντας					
Γ.1		✓			Κρυπτογράφηση μεταδιδόμενων πληροφοριών και γενικά εφαρμογή συνήθων μεθόδων ασφαλούς μετάδοσης πληροφορίας
Γ.2		✓			Έλεγχος πρόσβασης με τεχνικά μέσα αλλά και με προσωπικό ασφαλείας (όχι υπερβολικά μέτρα)
Γ.3		✓			Σύνηθες λογισμικό ασφάλειας δικτύων
Γ.4		✓			Έλεγχος πρόσβασης σε υλικό, λογισμικό και βάσεις δεδομένων
Δ. Κίνδυνοι τεχνολογίας					
Δ.1				✓	Προσεκτική και τεκμηριωμένη επιλογή του επιπέδου τεχνολογίας που θα χρησιμοποιηθεί
Δ.2		✓			Προσεκτική και τεκμηριωμένη επιλογή του επιπέδου τεχνολογίας που θα χρησιμοποιηθεί

Δ.3		✓			Πλήρης αρχικός σχεδιασμός που θα προβλέπει τη δυνατότητα συνδεσιμότητας των τμημάτων του έργου
Δ.4			✓		Ενημέρωση αναθέτουσας αρχής για τροποποιήσεις στον υπάρχον εξοπλισμό, εισαγωγή αυτών στον αρχικό σχεδιασμό υλοποίησης του έργου
Δ.5		✓			Δυνατότητα άμεσης αντικατάστασης ελαττωματικού εξοπλισμού, πρόβλεψη τέτοιου είδους καθυστερήσεων στον αρχικό σχεδιασμό, τακτικός έλεγχος εξοπλισμού για πρόληψη καταστροφής και άλλων τμημάτων του έργου από τη χρήση μη ασφαλούς υλικού και λογισμικού
Δ.6			✓		Πλήρης αρχικός σχεδιασμός που θα αξιολογεί αν υπάρχει η δυνατότητα να υλοποιηθεί το έργο, πόσο οικείο είναι στο περιβάλλον, πόση εμπειρία υπάρχει στο λογισμικό, στο δίκτυο που απαιτείται και στις διεπαφές με τους χρήστες.
Ε. Επιχειρησιακοί κίνδυνοι					
Ε.1		✓			Εκπαίδευση του προσωπικού που θα χειρίζεται το νέο σύστημα

E.2			✓		Έλεγχος δυνατοτήτων προσωπικού, έλεγχος πρόσβασης προσωπικού σε ευπαθείς και υψηλού κόστους αποκατάστασης ζημιών τομείς του έργου
E.3	✓				Θέσπιση κανόνων και ίσως ένα σεμινάριο παρουσίασης της αξίας του πληροφοριακού συστήματος
E.4	✓				Θέσπιση κανόνων, έλεγχος άρτιας εκτέλεσης των καθηκόντων τους και ίσως ένα σεμινάριο παρουσίασης της αξίας του πληροφοριακού συστήματος
E.5		✓			Έλεγχος γνώσεων του προσωπικού της αναδόχου εταιρείας (ενδεχομένως η ενέργεια αυτή να είναι περιττή καθώς κάθε εταιρία οφείλει πάντα να γνωρίζει τις ικανότητες του προσωπικού της)
E.6		✓			Αρχική συμφωνία και υπογραφές από τα ενδιαφερόμενα μέρη για τις απαιτήσεις του συστήματος και δοκιμή του συστήματος σε κάθε φάση του κύκλου ζωής του έργου

Ε.7			✓		Όσο πιο νωρίς είναι εφικτό να συμμετέχει ο χρήστης στο έργο και να υπάρχει συνεχής ενημέρωση στο χρήστη για τυχόν αλλαγές κατά τη διάρκεια υλοποίησης του έργου.
Ε.8			✓		Ο project manager πρέπει να στηρίζει την πρόοδο του έργου, να επιλύει άμεσα οποιοδήποτε πρόβλημα προκύπτει, να αποφεύγει να σπαταλάει πολύ χρόνο εστιάζοντας σε μια πτυχή του έργου, να έρχεται σε συνεχή επικοινωνία με τον χορηγό του έργου και τα ενδιαφερόμενα μέρη.
Ε.9			✓		Πρέπει να είναι σαφής η ζημιά που προκύπτει σε περίπτωση που προκύψει κάποιος κίνδυνος.
ΣΤ. Κίνδυνοι οργάνωσης του έργου					
ΣΤ.1			✓		Επιμελής, ορθολογικός, διορατικός και τεκμηριωμένος σχεδιασμός υλοποίησης του έργου
ΣΤ.2				✓	Ορθολογική, ρεαλιστική και επιμελώς καταρτισμένη προσφορά ανάληψης του έργου

ΣΤ.3		✓			Δεν απαιτείται ιδιαίτερη δράση καθώς η προκήρυξη αποσαφηνίζει κάθε πτυχή του έργου. Όμως πάντα η ανάδοχος εταιρεία οφείλει να τη μελετήσει προσεκτικά και να διασφαλίσει εξ αρχής τις απαιτήσεις του έργου
ΣΤ.4	✓				Καμία δράση. Η χρηματοδότηση του έργου καλύπτεται πλήρως νομικά
ΣΤ.5	✓				Διασφάλιση της προμήθειας του εξοπλισμού με την εισαγωγή ρητρών στις συμφωνίες
ΣΤ.6		✓			Προσεκτική επιλογή των προσώπων που διαχειρίζονται την πορεία υλοποίησης του έργου
ΣΤ.7			✓		Σαφής διαχωρισμός των καθηκόντων κατά τη φάση σχεδιασμού του έργου
ΣΤ.8			✓		Πρέπει να υπάρχει έλεγχος και σωστή διαχείριση των αλλαγών γιατί αποτυχημένες και βεβιασμένες αλλαγές μπορεί να φέρουν σε αποτυχία το πληροφοριακό έργο. Επίσης, κατά την πραγματοποίηση των αλλαγών πρέπει να είναι γνωστός ο χρόνος και το κόστος που θα απαιτηθεί

Σχήμα 43: Συνολικό επίπεδο έκθεσης στον κάθε κίνδυνο και προτεινόμενες δράσεις

Συμπεράσματα

Στην παρούσα εργασία έγινε σαφές ότι ένα έργο πληροφορικής μεγάλου μεγέθους και πολυπλοκότητας εμπεριέχει ποικίλους κινδύνους που απειλούν την επιτυχία της εφαρμογής του. Όσο μεγαλύτερο είναι το κόστος των έργων αυτών, η πολυπλοκότητά τους και η αξία τους για τη λειτουργία του οργανισμού τόσο σημαντικότερο εργαλείο για την εξασφάλιση της επιτυχημένης υλοποίησης τους αποτελεί η διαχείριση κινδύνων. Μέσα από αυτή μπορούν να προβλεφθούν τα προβλήματα που ενδέχεται να εμφανιστούν κατά την πορεία υλοποίησης του έργου και να προκαλέσουν σημαντικές απώλειες είτε από πλευράς κόστους, είτε από πλευράς χρόνου ολοκλήρωσης των εργασιών, είτε στην ποιότητα και την αξιοπιστία του. Η ευθύνη της διαχείρισης κινδύνων δεν τελειώνει εδώ καθώς καλείται να παρουσιάσει και τον τρόπο με τον οποίο θα μειωθεί η έκθεση του έργου στον κάθε κίνδυνο, να παρακολουθεί την εφαρμογή των μέτρων που συνέστησε αλλά και τον κίνδυνο που απομένει και μετά την εφαρμογή των μέτρων αυτών.

Η διαχείριση κινδύνων είναι μια αυστηρά δομημένη διαδικασία της οποίας τα βήματα θα πρέπει να εκτελούνται με επιμέλεια και σύνεση, καθώς μόνο έτσι θα καταφέρει να επιτύχει τους στόχους της. Και ουσιαστικά στόχος της διαδικασίας διαχείρισης κινδύνων είναι η άρτια υλοποίηση του αρχικού σχεδιασμού εγκατάστασης του πληροφοριακού έργου, χωρίς να επηρεαστεί αυτή από

απρόοπτα γεγονότα. Όλα τα στάδια της διαδικασίας διαχείρισης κινδύνων είναι εξίσου σημαντικά και έχουν τη δική τους ξεχωριστή συμβολή για την επίτευξη των στόχων της διαδικασίας.

Η μεθοδολογία διαχείρισης κινδύνων που περιγράφηκε μπορεί να αποτελέσει χρήσιμο εργαλείο για τη διεξαγωγή μελετών διαχείρισης κινδύνων και συμβάλει στον άρτιο σχεδιασμό και την επιτυχημένη υλοποίηση μεγάλων πληροφοριακών έργων. Η γενικότητα της μεθοδολογίας έγκειται στο γεγονός ότι περιγράφονται αναλυτικά όλα τα βήματα που ακολουθούνται για τη διαχείριση κινδύνων και οι κίνδυνοι που περιγράφονται αφορούν όλα τα είδη πληροφοριακών έργων.

Στην παρούσα εργασία εξετάστηκε επίσης, η εφαρμογή της διαδικασίας διαχείρισης κινδύνων στο έργο: «Ολοκληρωμένο Πληροφοριακό Σύστημα (ΟΠΣ) του Δήμου Αθηναίων». Αφού πραγματοποιήθηκε η ανάλυση του έργου και ποιοι είναι οι στόχοι του, εισήχθησαν οι κίνδυνοι που μπορεί να επηρεάσουν την ποιότητα, την αξιοπιστία, το κόστος και το χρονοδιάγραμμα του έργου. Εκ των υστέρων, πραγματοποιήθηκε ποιοτική ανάλυση των κινδύνων αυτών και παρουσιάστηκαν κάποιες μετρήσεις όσον αφορά την πιθανότητα εμφάνισής των κινδύνων, το επίπεδο των επιπτώσεων τους και το συνολικό επίπεδο έκθεσης σε κάθε κίνδυνο. Από τα αποτελέσματα που εξήχθησαν έγινε αντιληπτό ποιοι κίνδυνοι μπορεί να επηρεάσουν το συγκεκριμένο έργο και αναγνωρίζεται ο τομέας υλοποίησης του έργου που θα πληγεί από την εκδήλωση των κινδύνων. Γι αυτό το λόγο, προτάθηκαν και τρόποι αντιμετώπισης αυτών των κινδύνων.

Συνοψίζοντας, το πόρισμα που εμφανίζεται στην παρούσα εργασία είναι ότι ο υπεύθυνος του έργου με τη χρήση της διαδικασίας διαχείρισης κινδύνων, αισθάνεται μεγαλύτερη σιγουριά ότι δε θα βγει εκτός χρονοδιαγράμματος και προϋπολογισμού του έργου. Επίσης, γίνεται αντιληπτό ότι είναι πολλοί οι κίνδυνοι που μπορούν να εισέλθουν σε ένα έργο και να ανατρέψουν τα δεδομένα. Η καταγραφή όμως και η επίγνωση των κινδύνων βοηθούν στην αποτελεσματική διαδικασία λήψης αποφάσεων με το μικρότερο δυνατό ρίσκο.

Βιβλιογραφία

1. Mouratidis H., Giorgini P., Manson G., 2005
2. Βικιεπιστήμιο, http://el.wikiversity.org
3. Ψηφιακό Σχολείο, http://digitalschool.minedu.gov.gr
4. Martin Fowler. Patterns of Enterprise Application Architecture, Addison-Wesley, Boston, 2003
5. DeLONE, W. H. & E. R. McLEAN, Information Systems Success Revisited. IEEE (Institute of Electrical and Electronics Engineers) Computer Society, 2002, http://csdl.computer.org/comp/proceedings/hicss/2002/1435/08/14350238.pdf
6. Γεωργόπουλου Β. Νικολάου – Οικονόμου Σ. Γεωργίου, 'Πληροφοριακά Συστήματα για τη Διοίκηση Επιχειρήσεων, τόμος Α'', εκδόσεις Ευγενίου Μπένου, 1995
7. Βικιπαιδεία, http://el.wikipedia.org
8. Paul C. Dinsmore et al, 'The right projects done right!', John Wiley and Sons, 2005
9. Οδηγός βέλτιστων πρακτικών για τη σύναψη και εκτέλεση δημοσίων συμβάσεων,http://www.publicprocurementguides.treasury.gov.cy/OHS-GR/HTML/index.html?1_3_project_lifecycle.htm
10. PMI, A Guide to the Project Management Body Of Knowledge, Project Management Institute, USA, 2004

11. Κηρυττόπουλος Κ., 'Εγχειρίδιο Διαχείρισης Κινδύνων', εκδόσεις Κλειδάριθμος, 2006

12. Kleim R. & Ludin I., Reducing Project Risk, Gower Publishing Ltd, Uk, Hampshire, 1997

13. James A. Ward, PMP, 'KEEP IT SIMPLE TO ENHANCE PROJECT SUCCESS', 2000

14. Kerzner H., Project Management, 'A Systems Approach to Planning, Scheduling and Controlling, John Wiley & Sons, 2003

15. Gary Stoneburner, Alice Goguen, Alexis Feringa, "Risk Management Guide for Information Technology Systems", NIST, 2001

16. Beatty R., 'The Five – Minute Interview: A job Hunter's Guide to a Successful Interview', John Wiley & Sonw, Chichester, UK, 2002

17. Barker A. '30 minutes … to Brainstorm Great Ideas', Kogan Page, UK, 1997

18. Hilson D., 'Using a Risk Breakdown Structure in Project Management', Journal of Facilities Management, 2003

19. QuickMBA.com, 'Strategy section Swot Analysis', 2005
http://www.quickmba.com/strategy/swot

20. Chapman R., 'The effectiveness of working group risk identification and assessment techniques', International Journal of Project Management, 1998

21. Vicky Haney, 'Top IT Project Risks and What to do about them', VBH Consulting, 2009

22. Project Management Institute, "A Guide to the Project Management Body of Knowledge (PMBOK Guide)", Four Campus Boulevard, 2000

23. Vose D., 'Risk Analysis: A Quantitative Guide', John Wiley, Chichester, UK, 2000

24. Saltelli A., Chan K. and Scott E., 'Sensitive Analysis', Wiley, New Jersey, 2000

25. Κοινωνία της Πληροφορίας, http://www.cityofathens.gr/koinonia-tis-pliroforias-0#5

26. Δήμος Αθηναίων,
http://old.cityofathens.gr/files/13_12_2007_%20exoplismos_opsda_analytiko.pdf

27. Alan J. Laubsch, "Risk Management: A Practical Guide", RiskMetrics Group, 1999

28. Alfredo del Cano, M. Pilar de la Cruz, “Integrated Methodology for Project Risk Management**”,** Journal of Construction Engineering and Management, 2002

29. Paul S.Royer, “Proceedings of the Project Management Institute Annual Seminars & Symposium”, Houston, 2000

30. An interview with Max Wideman, “Software Project Risk Management, Success and Training”, Projects & Profits, 2002

31. Karl E. Wiegers, “Know Your Enemy: Software Risk Management”, Software Development, 1998

32. Ian Hawkins, “Risk Analysis Techniques”, GARP FRM Exam Review Class Notes (http://www.EuclidResearch.com/current.htm), 1998